GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security and Emergency Management Agency

Performance Oversight Pre-Hearing Responses

Dr. Christopher Rodriguez

Submission to

Committee on the Judiciary and Public Safety
Chairperson Charles Allen
Council Member, Ward 6

January 30, 2020

Committee on the Judiciary and Public Safety
John A. Wilson Building
1350 Pennsylvania Ave., NW, Suite 123
Washington, DC 20004

General Questions

1. Please provide a current organizational chart for the agency, including the number of vacant, frozen, and filled positions in each division or subdivision. Include the names and titles of all senior personnel, and note the date that the information was collected on the chart.

Please see attachment "Q1 HSEMA" for the current organizational chart.

a. Please provide an explanation of the roles and responsibilities of each division and subdivision.

Director's Office:
Provides executive leadership and administrative authority over HSEMA.

Chief of Staff:
Drives the Director's strategic priorities. Develops and standardizes processes and procedures across HSEMA.

Office of Public Affairs:
Manages internal and external communications for HSEMA. Spearheads outreach to District residents and visitors.

Office of Legal Affairs:
Provides legal counsel and policy advice to the HSEMA director. Supports the work of the Homeland Security Commission.

Administration Division:
Manages HSEMA's day-to-day enterprise activities. Key personnel and functions include:

- Chief Administrative Officer: Manages HSEMA's day-to-day administrative functions.
- Grants Management Bureau: Manages the federal homeland security grant programs awarded to the District and the National Capital Region.
- Finance Bureau: Manages HSEMA's finances in accordance with District policies and priorities.
- Information Technology (IT) Bureau: Manages, in coordination with OCTO, HSEMA's IT systems and other technology needs.
- Human Resources Bureau: Manages, in coordination with DCHR, the recruitment and hiring of new HSEMA staff and contractors. Manages personnel issues across the agency.

Preparedness Division:
Manages HSEMA's emergency preparedness activities. Key personnel and elements include:

- Chief of Homeland Security and Preparedness: Oversees the daily activities of the Homeland Security and Preparedness Division.
- Planning, Training, and Exercise Bureau: Provides training and exercise opportunities to the District. Develops the District's corrective action program. Creates planning products to meet the needs of HSEMA and key stakeholders within the District.
- Long-Term Risk Reduction Bureau: Manages the District's long-term recovery program. Administers and oversees the District's Hazard Mitigation Program. Within this Bureau, the Disability Integration Coordinator ensures the District's emergency management program effectively meets the needs of people with disabilities and those with access and functional needs.
- Regional Technical Assistance Bureau: Provides regional and sub-regional expertise to enhance preparedness capabilities, programs and initiatives in the National Capital Region (NCR).
- Strategic Partnership Bureau: Coordinates preparedness activities with non-governmental organizations such as the private sector and faith-based organizations.

National Capital Region Threat Intelligence Consortium:

Manages HSEMA's homeland security and intelligence activities. Key Personnel and elements include:

- Cyber Security Bureau: Collects, analyzes, responds to, and disseminates timely cyber threat information to and among the federal, state, local, and private sector agencies within the National Capital Region (NCR).
- NCR Watch/IC3 Bureau: Provides around-the-clock alert notifications and develops a common operating picture supporting coordination and collaboration on emerging incidents across the NCR.
- Public Safety Bureau: Focuses on unclassified production related to terrorism, crime, and public health for the public.
- National Security Bureau: Focuses on maintaining the baseline capabilities of the fusion center and providing support to law enforcement, first responder, and critical infrastructure partners.

Operations Division:

Manages HSEMA's steady-state and emergency operations activities. Key personnel and elements include:

- Chief of Operations: Oversees the Operation Division's daily activities.
- Emergency Operations Center (EOC) Bureau: Manages the District's Emergency Operation Center, oversees the District's Qualifications System, and processes EMAC requests.
- Joint All Hazards Operation Center (JAHOC) Bureau: As the District's watch center, the JAHOC maintains 24/7 coverage of the District.

Provides situational awareness of and coordinates resource requests for security and other incidents within DC.

- Facility and Security Bureau: Manages building and personnel security, access to Agency facilities, HSEMA's vehicle fleet, and the Agency's warehouse.

b. Please provide a narrative explanation of any changes to the organizational chart made during the previous year.

A proposed change to the organizational chart is currently in the final stages of review. The proposed change will elevate the National Capital Region Threat Intelligence Consortium to the division level.

2. Please provide a current Schedule A for the agency which identifies each position by program and activity, with the employee's title/position, salary, fringe benefits, and length of time with the agency.

Please note the date that the information was collected. The Schedule A should also indicate if the position is continuing/term/temporary/contract or if it is vacant or frozen. Please separate salary and fringe and indicate whether the position must be filled to comply with federal or local law.

Please see attachment "Q2 HSEMA" for Schedule A. Information was compiled on January 14, 2020.

3. Please list all employees detailed to or from your agency during FY19 and FY20, to date. For each employee identified, please provide the name of the agency the employee is detailed to or from, the reason for the detail, the date of the detail, and the employee's projected date of return.

During FY19 HSEMA had four employees detailed to or from other agencies. Timothy Spriggs was detailed to the Department of Public Works from September 24, 2018 through April 1, 2019. Jennifer Del Toro was on a detail to the Office of the Deputy Mayor for Public Safety and Justice (DMPSJ) from September 24, 2018 through April 26, 2019. Timothy Spriggs and Jennifer Del Toro have since separated from the Agency. In addition, John Mein was detailed to HSEMA from the Office of Neighborhood Safety and Engagement (ONSE) from January 28, 2019 to April 1, 2019. He has since joined HSEMA as a full-time employee. HSEMA has one employee currently detailed to another agency. Nicole Peckumn was detailed to the Mayor's Office of Public Affairs starting on February 11, 2019. Nicole Peckumn remains on detail. All details to and from the agency were done for the good of the District, to improve performance, and to help meet the immediate needs of the District government.

4. Please provide the Committee with:

a. A list of all vehicles owned, leased, or otherwise used by the agency and to whom the vehicle is assigned, as well as a description of all vehicle collisions involving the agency's vehicles in FY19 and FY20, to date; and

Included below is a current vehicle and accident list as of January 14, 2020.

Vehicle	Tag	Acquisition	Assignment	Accident Date
Chevy Tahoe 2017	G62-0841U	Leased	Chris Rodriguez	09/26/2019
Chevy Tahoe 2018	G62 3993S	Leased	Rashad Young	None
Ford Explorer 2014	G62-3599N	Leased	Chris White	None
Dodge Durango 2014	G62-2532P	Leased	Donte Lucas	06/21/2019
Chevy Suburban 2016	G62-1294S	Leased	Robert Sneed	None
Chevy Tahoe 2018	G62 1664V	Leased	Clint Osborn	None
Ford Expedition 2014	G62-2542P	Leased	EOM	None
Freightliner Columbia 2007	DC-8362	Owned	DC-12 MCC (Ops Division)	None
Kenworth T370 2019	DC-13238	Owned	DC-13 MCC (Ops Division)	None
Ford Flex 2019	G61-1279W	Leased	Fleet	None
Dodge Durango 2016	G62-0057S	Leased	Fleet	None
Dodge Durango 2014	G62-0760P	Leased	Fleet	None
Ford Explorer 2013	G42-2184W	Leased	Fleet	None
Mercedes-Benz Sprinter 2010	DC-7901	Leased	Fleet	None
Quality Generator 1999	DC-1004	Owned	Generator	None
Whisperwatt DCA-70SSJU 2004	603380	Owned	Generator	None
Whisperwatt DCA-70SSJU 2008	603541	Owned	Generator	None
DOOSAN 608950 6KW PORTABLE LIGHT TOWER 2016	DC-8950	Owned	Light Tower	None
DOOSAN 608949 6KW PORTABLE LIGHT TOWER 2016	DC-8949	Owned	Light Tower	None
Aisle Master 33NF 2019	45285	Owned	Logistics	None

Chevy Silverado 2018	G63-0971V	Leased	Logistics	None
Dodge Durango 2016	G62-2285R	Leased	Maintenance	None
Chevy Suburban 2014	G62-1071N	Leased	Maintenance	None
Chevy Tahoe 2019	G62-1851W	Leased	Reserved	None
Utility Trailer CargoMate 2000	None	Owned	Utility Vehicles	None
Pace America Utility Trailer OutBack 2000	DC-7968	Owned	Utility Vehicles	None
Pace America Utility Trailer Paceamerica 2000	DC-7241	Owned	Utility Vehicles	None

The accidents in FY19 and FY20, to date, involved the following:

- 6/21/2019 – A District vehicle was hit by another vehicle while parked. The driver left the scene. The District employee didn't notice minor damage to the vehicle until later that day.
- 9/26/2019 – The District vehicle was parked. The vehicle was struck by another vehicle and the striking vehicle left the scene.

b. A list of travel expenses, arranged by employee for FY19 and FY20, to date, including the justification for travel.

FY 2019

Name	Destination	Justification	Travel Period	Expense
Adams, Nikelle	San Diego, CA	2019 ESRI User Conference	7/7/2019 - 7/13/2019	$2,365.80
Akasa, Annah	Chicago, Il	Assoc. of Unmanned Vehicle Systems	4/28/2019 - 5/3/2019	$3,966.88
Alexander, Daniel	Savannah, GA	IAEM Conference	11/15/2019 - 11/21/2019	$2,901.22
Alsop, Vermecia	Philadelphia, PA	L0212 HMA Developing Quality Applications Elements	10/14/2018 - 10/18/2018	$1,350.20
Alsop, Vermecia	Broomfield, CO	44th Annual Natural Hazards Research and Application Workshop	7/13/2019 - 7/18/2019	$2,280.71
Alsop, Vermecia	Bellefonte, PA	NFIP/ SHMO Meeting	11/19/2019 - 11/21/2019	$376.72
Bernet, Courtney	Newport News, VA	Virginia Symposium Emergency	3/24/2019 - 3/26/2019	$552.18
Bernet, Courtney	Phoenix, AZ	2019 National Homeland Security Conference	6/16/2019- 6/21/2019	$2,176.43

Name	Destination	Justification	Travel Period	Expense
Bernet, Courtney	Redlands, CA	BCEM Emerging Leaders	9/9/2019 - 9/13/2019	$1,285.56
Bradley, Nickea	Philadelphia, PA	FEMA Region III, L0212	10/15/2018 - 10/16/2018	$383.15
Bradley, Nickea	Davis, WV	State Hazard Mitigation Officers Meeting	11/12/2018 - 11/16/2018	$499.96
Bradley, Nickea	Broomfield, Co	2019 Natural Hazards Workshop	7/13/2019 - 7/17/2019	$1,635.78
C., Evan	National Harbor, MD	Analysts Annual Training Conference	8/19/2019- 8/21/2019	$788.44
Coleman, Bettina	Grand Rapids, MI	IAEM 66th Annual Conference	10/19/2018 - 10/25/2018	$1,678.21
Coleman, Bettina	San Antonio, TX	2019 Texas Emergency Management	4/16/2019 - 4/19/2019	$1,581.45
Crawford, Elijah	New Orleans, LA	Administrative Professional Conference	9/21/2019 - 9/26/2019	$4,367.15
Crawley, Lorien	Las Vegas, NV	Society for Human Resource Management 2019 Annual Conference	6/22/2019 - 6/27/2019	$3,989.27
Cruz, Joiner	Washington, DC	Mayors Disability & Diversity Expo Outreach Program and Public Speaking Seminar;	2/1/2019	$45.90
Cruz, Joiner	Washington, DC	2 Day Business Writing Skills Workshop	3/11/2019 and 3/19/2019	$73.00
D., Rachel	Chicago, IL	Forum & 4th Annual Analyst RoundTable Seminar	6/24/2019- 6/28/2019	$2,292.24
D., Rachel	San Antonio, TX	Basic Intelligence and Threat Analysis Training	9/8/2019 - 9/21/2019	$3,114.51
D., Jesse	Las Vegas, NV	DEFCON 2019 Conference	8/7/2019 - 8/11/2019	$1,393.98
D., Jesse	El Paso, TX	Department of Homeland Security Seminar	8/26/2019 - 8/31/2019	$1,723.70
D., Jesse	Alexandria, VA	National Fusion Center Association	11/4/2019 - 11/7/2019	$161.40
E., Sarah	St. Louis, MO	2019 Preparedness Summit	3/25/2019 - 3/30/2019	$1,797.67
E., Sarah	San Antonio, TX	Basic Intelligence and Threat Analysis Training	9/8/2019 - 9/21/2019	$3,160.35
F., Kelli	Hanover, MD	Mid-Atlantic Regional Gang Investigators Network 13th Annual Conference	3/4/2019 - 3/6/2019	$250.70
F., Kelli	Ewing, NJ	Basic Intelligence and Threat Analysis Training	3/31/2019 - 4/12/2019	$2,766.74
F., Kelli	Richmond, CA	Open-source intelligence Training	5/13/2019 - 5/16/2019	$730.26

Name	Destination	Justification	Travel Period	Expense
F., Kelli	Quantico, VA	Joint Regional Intelligence Center (JRIC) Tactical Analysis Course	7/8/2019 - 7/11/2019	$157.76
G., Margaret	Ocean City, MD	Maryland Human Trafficking Professionals Seminar	10/28/2018 - 10/30/2018	$436.56
G., Margaret	Ridgeland, MS	2019 Fusion Center 4th Annual Human Trafficking Analyst Training	2/25/2019 - 3/1/2019	$820.22
G., Margaret	Richmond, VA	DHS Open Source Intelligence Training	5/14/2019 - 5/16/2019	$498.64
G., Travis	Trenton, NJ	Basic Intelligence Threat Analysis Course (BITAC) Training	3/31/2019 - 4/13/2019	$1,220.80
G., Travis	Chicago, IL	AIRIP's 2nd Annual Global Intelligence Forum & 4th Annual Analyst RoundTable	6/24/2019 - 6/28/2019	$2,359.75
G., Travis	Redlands, CA	Big City Emergency Management Emerging Leaders Program	9/9/2019 - 9/13/2019	$1,581.92
G., Charles	Scott Valley, CA	Augmented Intelligence Summit - Scott Valley, CA	3/27/2019 - 3/31/2019	$2,379.74
G., Charles	Baltimore, MD	4th Annual FAA UAS Symposium - Baltimore Convention Center	6/3/2019 - 6/5/2019	$161.55
G., Charles	Chicago, IL	Global Security Exchange	9/8/2019 - 9/11/2019	$1,998.81
Harley, Stephanie	Redlands, CA	Big City Emerging Leaders Program	12/9/2018 - 12/14/2018	$1,473.04
Harley, Stephanie	Boston, MA	Big City Emergency Managers Meeting	3/24/2019 - 3/26/2019	$1,135.28
Harris, Robert	Redlands, CA	Big City Emerging Leaders Program	9/9/2019 - 9/13/2019	$1,685.57
H., Leslie	Phoenix, AZ	2019 National Homeland Security Conference	6/16/2019 - 6/21/2019	$2,607.11
H., Leslie	Hanover, VA	FEMA Region 3 IMT/NIMS Workshop	8/26/2019 - 8/28/2019	$468.82
H., Donell	Cambridge, MA	Urban Humanitarian Emergencies Course	7/15/2019 - 7/19/2019	$498.70
H., Donell	Rapid City, SD	Governors Homeland Security Advisors Conference	9/3/2019 - 9/7/2019	$498.70
H., Steven	Trenton, NJ	Basic Intelligence and Threat Analysis Course (BITAC) Training	3/31/2019 - 4/12/2019	$2,753.98
Huggins, Briana	Philadelphia, PA	L0212 HMA Developing Quality Applications	10/14/2018 - 10/18/2018	$1,256.91

Name	Destination	Justification	Travel Period	Expense
Huggins, Briana	Chicago, IL	2018 Grants Professional Association (GPA) Conference	11/6/2018 - 11/11/2018	$1,412.04
Jones, Cynthia	Los Angeles, CA	Americans with Disabilities Act (ADA) Update Conferences	9/11/2019 - 9/14/2019	$1,718.84
Jones, Gelinda	New Orleans, LA	WebEOC Conference	5/6/2019 - 5/10/2019	$614.04
Jones, Gelinda	Burlington, WI	Final MCV Inspection	7/8/2019 - 7/10/2019	$188.50
Lampson, Alexandria	Newport News, VA	Virginia Symposium Emergency Management	3/24/2019 - 3/26/2019	$554.73
Lescure, William	San Diego, CA	2019 ESRI Public Safety Conference	7/5/2019 - 7/10/2019	$1,134.24
Lucas, Donte	New Orleans, LA	Exchange 2019 User Conference	5/7/2019 - 5/10/2019	$1,202.96
Marcenelle, M	Huntsville, AL	Advanced writing Course for Fusion Centers	6/17/2019- 6/21/2019	$273.00
M., Krista	Clark County, NV	DEFCON 2019 Conference	8/7/2019 - 8/11/2019	$2,236.22
Mcdermott, Nicole	Hanover, VA	Region III IMT/NIMS workshop	8/26/2019 - 8/28/2019	$350.50
M., Sonia	Oklahoma City, OK	2018 Homeland Security Information Network Intelligence Seminar	12/11/2018 - 12/13/2018	$1,563.43
M., Sonia	Columbus, OH	DHS Office of Intelligence Analysis -2019 Specialized Seminar Series	7/29/2019 - 7/31/2019	$894.12
M., Sonia	Atlanta, GA	Open Source Intelligence Analysis Course-Mandatory by Department of Homeland Security	8/5/2019 - 8/8/2019	$902.01
M., Sonia	San Antonio, TX	Basic Intelligence and Threat Analysis	9/8/2019 - 9/21/2019	$3,119.13
Mitchell, Tanya	Atlanta, GA	2019 Atlanta Streets ALIVE - Atlanta, GA	4/6/2019 - 4/8/2019	$678.29
Nichting, Claire	New Orleans, LA	Real Time Crime Center Event - New	3/3/2019 - 3/6/2019	$1,958.84
Osborne, Clint	New York City, NY	Big City Emergency Managers 2018 Fall	10/15/2018 - 10/19/2018	$1,586.15
Osborne, Clint	Denver, CO	Pioneer Shield Exercise	12/5/2018 - 12/9/2018	$1,024.80
Osborne, Clint	Atlanta, GA	HSEMA Support to the 2019 Super Bowl	1/30/2019 - 2/5/2019	$893.34
Osborne, Clint	Chicago, IL	2019 Big City Emergency Managers'	9/17/2019 - 9/19/2019	$1,413.31
P., David	Clark County, NV	DEFCON 2019 Conference	8/7/2019 - 8/11/2019	$1,862.54

Name	Destination	Justification	Travel Period	Expense
Quarrelles, Jamie	Phoenix, AZ	2019 National Homeland Security	6/16/2019 - 6/21/2019	$1,721.66
R., Shannon	New Brunswick, NJ	Rutgers Center for Critical Intelligence	6/4/2019 - 6/6/2019	$606.82
R., Shannon	Golden, CO	Basic Intelligence and Threat analysis	8/18/2019 - 8/31/2019	$4,541.02
Reed, Tristan F.	Chicago, IL	Grants Professionals Association Annual Conference	11/7/2018 - 11/10/2018	$1,992.39
Rodriguez, Christopher	Boston, MA	Big City Emergency Managers (BCEM) Spring 2019 Meeting	3/25/2019 - 3/27/2019	$1,195.16
Rodriguez, Christopher	Chicago, IL	2019 Big City Emergency Managers' Meeting	9/16/2019 - 9/17/2019	$411.20
Rodriguez, Christopher	Sacramento, CA	California OES/Fusion Center Meetings	9/17/2019 - 9/20/2019	$2,033.99
R., Sheila	Ewing, NJ	Basic Intelligence and Threat Analysis	3/31/2019 - 4/12/2019	$2,767.90
R., Cembrye	Phoenix, AZ	2019 National Homeland Security Conference	6/16/2019 - 6/21/2019	$2,248.28
Ruesch, Emily	Newport News, VA	Emergency Management Accreditation Program training	3/24/2019 - 3/26/2019	$468.08
Ruesch, Emily	Phoenix, AZ	National homeland Security Association Conference	6/16/2019 - 6/21/2019	$2,166.07
S., Paige	Brunswick, NJ	Rutgers Intelligence Seminar	6/4/2019 - 6/6/2019	$607.98
Scott, Delores Lynn	Rapids, MI	IAEM 66th Annual Conference - Grand	10/21/2018 - 10/24/2018	$789.07
Scott, Delores Lynn	San Antonio, TX	Texas Emergency Management	4/16/2019 - 4/17/2019	$1,109.90
Scott, Mark	Reisterstown, MD	State Mitigation Planning Workshop	11/1/2018 - 11/2/2018	$91.50
Scott, Mark	New York City, NY	Critical Infrastructure Supply Chain Security Forum	4/23/2019 - 4/24/2019	$671.38
Scott, Mark	Nicholasville, KY	Comprehensive Security Specialist Training	8/18/2019 - 8/30/2019	$6,140.77
Scott, Mark	New York City, NY	DHS Corporate Security Seminar	9/16/2019 - 9/17/2019	$690.30
Shackelford, Jerica	Grand Rapids, MI	International Association of Emergency Managers 66th Annual Conference	10/21/2018 - 10/25/2018	$1,138.38
Shackelford, Jerica	Chicago, IL	2018 Grants Professional Association	11/6/2018 - 11/11/2018	$2,602.66
Shackelford, Jerica	Washington, DC	CPM Class and Meeting - Parking and Ground Transportation	1/9/2019 - 2/9/2019	$140.25

Name	Destination	Justification	Travel Period	Expense
Shackelford, Jerica	Washington, DC	CPM classes, meetings and workshops	3/6/2019 - 3/27/2019	$136.24
Shackelford, Jerica	Washington, DC	CPM Sessions and Meetings	4/12/2019 - 6/13/2019	$102.75
Shackelford, Jerica	Washington, DC	July CPM Classes	7/11/2019 - 7/13/2019	$39.00
Shackelford, Jerica	Aptos, CA	Prosci Change management certification	8/5/2019 - 8/8/2019	$913.30
Speranza, Carrie	Grand Rapids, MI	2018 International Association of Emergency Managers Annual	10/19/2018 - 10/25/2018	$2,560.00
Speranza, Carrie	Alexandria, VA	Policy and Leadership Mid-Year Forum	3/30/2019- 4/1/2019	$66.00
Speranza, Carrie	Chicago, IL	2019 Big City Emergency Managers' Meeting	9/17/2019 - 9/19/2019	$1,543.26
Stewart, Jonathan	New York City, NY	Big City Emergency Managers 2018 Fall Meeting	10/15/2018 - 10/19/2018	$1,822.06
Stewart, Jonathan	Boston, MA	Big City Emergency Managers (BCEM) Spring 2019 Meeting	3/25/2019 - 3/29/2019	$1,963.42
Stewart, Jonathan	Phoenix, AZ	2019 National Homeland Security Conference	6/17/2019 - 6/21/2019	$1,750.54
Tamm, Erik	New Orleans, LA	Real Time Crime Center Event	3/3/2019 - 3/6/2019	$227.20
T., Alexandria	San Antonio, TX	Basic Intelligence and Threat Analysis	9/8/2019 - 9/20/2019	$2,085.25
Terry, Andre	Las Vegas, NV	Society for Human Resource Management 2019 Annual Conference	6/22/2019 - 6/27/2019	$3,491.38
White, Christopher	New York City, NY	Big City Emergency Managers Fall 2018	10/15/2018 - 10/19/2018	$1,967.50
White, Christopher	San Francisco, CA	Northern California Fusion Center Meetings	2/10/2019 - 2/12/2019	$1,108.50
White, Christopher	Boston, MA	Big City Emergency Managers (BCEM) Spring 2019 Meeting - Boston, MA	3/25/2019 - 3/28/2019	$673.93
Wilson, Larae	Redlands, CA	Big City Emerging Leaders Program	12/9/2018 - 12/14/2018	$1,530.55
Wilson, Larae	Boston, MA	Big City Emergency Managers Meeting	3/24/2019 - 3/26/2019	$1,199.96
W., Rachel	Phoenix, AZ	2019 National Homeland Security Conference	6/16/2019 - 6/21/2019	$2,288.85
Worrell, Andrew	Nicholasville, KY	Comprehensive Security Specialist Training	8/18/2019 - 8/30/2019	$5,324.00

FY 2020, to date (as of 1/27/2020)

Name	Destination	Justification	Travel Period	Expense
Bradley, Nickea	State College, PA	State NFIP Coordinator/State Hazard	11/19/2019 - 11/21/2019	$348.00
D., Jesse	Alexandria, VA	National Fusion Center Association	11/4/2019 - 11/7/2019	$161.40
G., Matthew	Houston, TX	World Series Deployment	10/21/2019 - 10/24/2019	$1,900.82
H., Donell	Houston, TX	World Series Deployment	10/22/2019 - 10/24/2019	$434.50
Huggins, Briana	Philadelphia, PA	FEMA Workshop	12/3/2019 - 12/5/2019	$716.30
M., Krista	Sacramento, CA	State Threat Assessment Fusion Center	10/2/2019 - 10/4/2019	$863.21
M., Krista	Houston, TX	World Series Deployment	10/21/2019 - 10/24/2019	$2,418.03
M., Krista	Alexandria, VA	NFCA Conference	11/4/2019 - 11/7/2019	$157.96
Mudambo, Mildred	Philadelphia, PA	2019 FEMA Region III Grants recipient	12/2/2019 - 12/4/2019	$722.70
Partridge, Nathanial	Savannah, GA	IAEM Conference	11/16/2019 - 11/21/2019	$1,909.03
Peckumn, Nicole	Nashville, TN	MGT 404- Sports/Event Incident	11/4/2019 - 11/6/2019	$1,445.32
Quarrelles, Jamie	Savannah, GA	2019 International Association of Emergency Managers Conference	11/15/2019 - 11/21/2019	$3,234.46
Rodriguez, Christopher	Sacramento, CA	CSTAC Meeting	10/2/2019 - 10/4/2019	$1,404.63
Rodriguez, Christopher	Milan, Italy	Critical Infrastructure Protection and Resilience Expo	10/14/2019 - 10/16/2019	$3,782.83
Scott, Mark	Savannah, GA	IAEM Conference	11/17/2019 - 11/20/2019	$1,288.68
Shackelford, Jerica	Savannah, GA	International Association of Emergency Managers (IAEM) 2019 Conference	11/17/2019 - 11/21/2019	$1,909.85
Speranza, Carrie	Savannah, GA	IAEM Annual Conference 2019	11/15/2019 - 11/21/2019	$2,090.35
Sumbeida, Muniru	Philadelphia, PA	2019 FEMA Region III Grants Recipient	12/2/2019 - 12/4/2019	$549.52
Valentine, Amanda	Philadelphia, PA	FEMA Region 3 Grant Recipient Workshop	12/2/2019 - 12/5/2019	$909.63

5. Please list all memoranda of understanding ("MOU") entered into by the agency during FY19 and FY20, to date, as well as any MOU currently in force. For each, indicate the date on which the MOU was entered and the termination date.

Please see the below chart for information related to Urban Areas Security Initiative (UASI) and State Homeland Security Program (SHSP) Memorandums of Agreement for FY19 and FY20, to date (January 24, 2020).

Agency	Purpose	Date Entered	Date Terminated
DC Health	Patient Tracking	October 23, 2019	September 30, 2020
DC Health	Medical Reserve Corps	October 23, 2019	May 31, 2021
District of Columbia Department of Human Services	Mass Care Program Development	October 23, 2019	September 30, 2020
District of Columbia Fire and Emergency Medical Services	CBRNE Detection	October 9, 2019	September 30, 2020
District of Columbia Fire and Emergency Medical Services	Terrorism Liaison Officer Program, Planning, Training, and Exercise Support	October 9, 2019	September 30, 2020
District of Columbia Metropolitan Police Department	License Plate Reader Program	October 9, 2019	September 30, 2021
District of Columbia Office of the Chief Medical Examiner	Fatality Management Continuity of Operations (COOP)	October 4, 2019	September 30, 2021
District of Columbia Office of Unified Communications	Radio Cache (NCRCIG)	October 9, 2019	September 30, 2021
District of Columbia Office of Unified Communications	CAD Information Sharing and Interoperability	October 4, 2019	September 30, 2021
District of Columbia Office of Unified Communications	Interoperable Communications Planning, Training, and Exercises	October 4, 2019	September 30, 2020
District of Columbia Office of Unified Communications	9-1-1 Wireless Call Routing Analytics	October 4, 2019	May 31, 2021
Serve DC	Volunteers and Donations Management	October 23, 2019	September 30, 2020
DC Health	Medical Supplies and Equipment Cache	October 23, 2019	September 30, 2020
District of Columbia Department of Energy and Environment	Hazardous Materials Emergency Response Enhancement	October 9, 2019	September 30, 2020
District of Columbia Fire and Emergency Medical Services	Chemical Protective Equipment	October 9, 2019	September 30, 2020
District of Columbia Fire and Emergency Medical Services	NIMS Typed Team Training	October 23, 2019	September 30, 2020

Agency	Purpose	Date Entered	Date Terminated
District of Columbia Fire and Emergency Medical Services	Triage Equipment	December 18, 2019	September 30, 2020
District of Columbia Metropolitan Police Department	Law Enforcement Information Systems	October 4, 2019	September 30, 2020
District of Columbia Metropolitan Police Department	Personal Protection Equipment and CBRN Response	December 27, 2019	September 30, 2020
District of Columbia Metropolitan Police Department	Virtual Terrorism Response Training	October 23, 2019	September 30, 2020
District of Columbia Metropolitan Police Department	Crisis Negotiation Squad Response Vehicle	December 27, 2019	September 30, 2020
District of Columbia Public Schools	Emergency Response Information Portal (ERIP)	December 18, 2019	September 30, 2020
Serve DC	Citizen Preparedness and Volunteer Management	October 9, 2019	September 30, 2020
District of Columbia Office of Unified Communications	CAD Information Sharing and Interoperability (Continuation)	October 16, 2018	September 30, 2020
District of Columbia Fire and Emergency Medical Services	Tactical Medical Casualty Care (TECC) Train the Trainer (CCA)	June 11, 2019	March 31, 2020
DC Health	Medical Reserve Corps (Continuation) (DCERS)	September 27, 2018	May 31, 2020
District of Columbia Metropolitan Police Department	License Plate Reader Program (Continuation)	September 27, 2018	September 30, 2020
District of Columbia Office of Unified Communications	Radio Cache - District of Columbia (Continuation)	September 27, 2018	September 30, 2020
District of Columbia Metropolitan Police Department	Law Enforcement Homeland Security Capabilities (Continuation)	September 27, 2018	January 31, 2020

Please also see attachment "Q5 HSEMA" for the listing of MOUs to other agencies issued in FY19 and FY20, or that are still active in FY20.

6. Please list the ways, other than MOU, in which the agency collaborated with analogous agencies in other jurisdictions, with federal agencies, or with non-governmental organizations in FY19 and FY20, to date.

The mission of the National Capital Region Threat Intelligence Consortium (NTIC) as the District's fusion center network, is to share information among federal, state, and local entities to maximize the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity. The NTIC collaborates with local and federal

entities daily through assigned liaisons. This includes joint productions related to threat targeting to the District or in anticipation of large special events (for example July 4, State of the Union Address, etc.).

Additionally, HSEMA hosts or participates in several different working groups that bring together federal and local entities including the School Safety Alliance, DC's Human Trafficking Task Force, and the Interfaith Preparedness and Advisory Group (IPAG). In response to mass shooting incidents around the globe, in 2019 HSEMA partnered with the Mayor's Office of Religious Affairs (MORA) and the Metropolitan Police Department (MPD) to form the IPAG. This partnership provides support and solidarity to the District's places of worship prior to an emergency. The IPAG was provided emergency preparedness trainings and technical support with applications for federal funding to enhance security for their facilities.

HSEMA's Long-Term Risk Reduction (LTRR) Bureau, Mitigation Unit collaborated with other District agencies, most notably, Department of Energy and the Environment (DOEE), District of Columbia Public Schools (DCPS), and the Department of General Services (DGS) Protective Services Division (PSD). With DOEE, HSEMA provided technical assistance with floodplain and flood inundation mapping. The collaboration focused on project development for Climate ReadyDC, resiliency hubs, a hospital microgrid pilot and building surveys of facilities in Watts Branch. With DCPS, HSEMA collaborated on the Safety Through Resiliency Assessment Planning (STRAP) Pilot Assessments, River Terrace Education Campus (RTEC) emergency evacuation exercise, the Redbook Playbook, which provided a quick guide to the larger Redbook, and School Safety Alliance migration to a more collaborative format. Also, with DGS-PSD, HSEMA collaborated for building assessments.

HSEMA's Planning, Training, and Exercise Bureau (PTEB), conducted plan reviews for DC Energy Assurance Plan (DOEE), FEMA DC Programmatic Agreement 2019 (FEMA/OP SHPO), DC Comp Plan (OP), NPS DC Flood Plan (NPS), Disaster Recovery Reform Act (FEMA), and DC Interagency Flood Plan (DOEE).

Nationally, HSEMA is a member of the National Emergency Management Association (NEMA), allowing the agency to work directly with the analogous homeland security and emergency management agencies from every state and US territory. This allows the District to share resources during emergencies through the Emergency Management Assistance Compact (EMAC). It also allows the District to review and provide feedback on federal policy for disaster management and advocate for ongoing grant funding through NEMA's written comments and white papers. In 2019, HSEMA LTRR Mitigation collaborated with NEMA for the Hazard Mitigation Chapter Update and the NEMA Annual Report. Written comments from HSEMA were given on the Disaster Recovery Reform Act (DRRA) and Streamlining Disaster Recovery.

Nationally, HSEMA is a member of the National Governors Homeland Security Advisor Council (GHSAC). Like NEMA, GHSAC provides the agency with a forum to work with our homeland security and intelligence agency partners across the nation. It also allows the District to review and provide feedback on federal policy for homeland security and advocate for ongoing grant funding.

Nationally, HSEMA is a member of the Big City Emergency Managers (BCEM), which is a network of the most progressive emergency management agencies from the largest metropolitan areas around the country. Along with providing the District with another forum to formally advocate for disaster policy and funding, BCEM provides HSEMA with a method to collect and share best practices from peer agencies. The agency, especially our Division of Operations, regularly shares and receives plans, policies, and procedures from our counterparts to fill gaps in our doctrine. This saves the District staff time and funding.

Nationally, HSEMA is a member of Silver Jackets Program supported by United States Army Corps of Engineers (USACE). Silver Jackets teams bring together multiple states, federal, and sometimes tribal and local agencies to learn from one another in reducing flood risk and other natural disasters. Shared knowledge is used to enhance response and recovery efforts when such events do occur. HSEMA LTRR Mitigation collaborated with Silver Jackets on the DC Levee Outreach, flood risk management planning, and Watts Branch flood risk study.

Regionally, the agency also participates as the state representative on various Federal Emergency Management Agency (FEMA) committees and working groups, such as the Modeling and Data Working Group. HSEMA also participates in regular emergency response and recovery exercises across the region with our analogous local, state, and federal partners.

HSEMA administers the Statewide Interoperability Executive Council (SIEC), the mechanism through which the District manages public safety and emergency communications interoperability enhancement efforts. Under the District Statewide Communications Interoperability Plan, the SIEC provides policy-level direction to District and regional partners on the development and maintenance of interoperable emergency communications. The SIEC oversees the Interoperable Communications Committee (ICC), a board made up of representatives from key SIEC agencies and other interested District, federal, and regional agencies. The Statewide Interoperability Coordinator serves as the liaison between the SIEC and ICC, while also coordinating and overseeing interoperability policy and procedures.

HSEMA is represented on all of the National Capital Region Regional Emergency Support Function (RESF) committees of the Metropolitan Washington Council of Governments (MWCOG), as well as the Homeland Security Executive Committee (HSEC), the HSEC Advisory Council, HSEC Cyber Working Group, HSEC Fusion Center Working Group, the Complex Coordinated Attack (CCA) Working Group, and the Interoperability Working Group. HSEMA also participates on or co-chairs

several subcommittees for the National Special Security Events (NSSE) planning team. HSEMA regularly attends and participates at the meetings of the following associations: Hotel Association of Washington DC – Security Directors, Apartment Office Building Association – Emergency Preparedness Committee, the Consortium of University Police Chiefs, National Fusion Center Association Cyber Intelligence Network, Railway Alert Network, Amtrak Rail and Information Sharing Group, the Association of Metropolitan Water Agencies, Mid- Atlantic First Financial Sector, U.S. Department of Homeland Security – Sector Specific - Food and Agriculture Subcommittee, Maryland Center for School Safety Statewide School Safety Weekly Conference Call, the DC Venue Group, the Washington Nationals Security, and the Capital One Center Security. HSEMA also serves as a member of InfraGuard, the Washington-Baltimore High Intensity Drug Trafficking Area Program, and the Joint Force Headquarters-National Capital Region Joint Operations Information Group.

In accordance with Mayor's Order 2018-084 dated October 22, 2018, HSEMA is the chair and coordinating agency for the Mayor's Unmanned Aerial Systems (UAS) working group, which is tasked with evaluating and making recommendations for a comprehensive program to incorporate UAS in the District's airspace. In addition to representatives from District agencies, the working group also consists of airspace managers from various analogous local, regional, and federal partners.

Finally, HSEMA partners daily with the American Red Cross (ARC) for emergency response. The ARC's National Capital Region Chapter operates under the ARC national charter and provides direct assistance to residents that require housing and incidental expenses following residential fires. HSEMA serves as the ARC's primary point of contact within the District.

7. **For FY19 and FY20, to date, please list all intra-District transfers to or from the agency, and include a narrative description of the purpose of each transfer.** There were no intra-District transfers to HSEMA in FY19 or FY20. Intra-District transfers from HSEMA to other agencies are listed below.

FY 2019

FROM	SELLING AGENCY	DESCRIPTION OF SERVICES PROVIDED	AMOUNT
HSEMA	DC Human Resources	Compliance Services	$39,917
HSEMA	Office of Disability Rights	Sign Language Services	$2,475
HSEMA	Office of Finance Resource Management	Agency Purchase Cards	$281,367
HSEMA	OFOS	Single Audit	$85,975
HSEMA	Office of Finance Resource Management	RTS	$2,847
HSEMA	OCTO	FY19 IT ASSESSMENTS	$111,313
HSEMA	Office of the Secretary	Records Retention	$22,743

HSEMA	DPW	Fleet	$31,304
HSEMA	OUC	Radio Services	$10,647

FY 2020, to date (01/24/2020)

FROM	SELLING AGENCY	DESCRIPTION OF SERVICES PROVIDED	AMOUNT
HSEMA	Office of Finance Resource Management	RTS Cost	$10,000
HSEMA	DPW	Fleet Maintenance	$35,000
HSEMA	OCTO	IT Assessment	$119,956
HSEMA	DGS	EOC Assessment	$292,500
HSEMA	DC Human Resources	Compliance Services	$12,500
HSEMA	Office of Finance Resource Management	Agency Purchase Cards	$75,000

8. For FY19 and FY20, to date, please identify any special purpose revenue funds maintained by, used by, or available for use by the agency. For each fund identified, provide:

a. The revenue source name and code;
b. The source of funding;
c. A description of the program that generates the funds;
d. The amount of funds generated by each source or program;
e. Expenditures of funds, including the purpose of each expenditure;
f. Whether expenditures from the fund are regulated by statute or policy; and
g. The current fund balance.

HSEMA does not maintain, use, or have available for use, any special purpose revenue funds.

9. For FY19 and FY20, to date, please list all purchase card spending by the agency, the employee making each expenditure, and the general purpose of each expenditure.

See attachment "Q9 HSEMA". The data for FY20 goes through January 24, 2020.

10. Please list all capital projects in the financial plan for the agency or under the agency's purview in FY19 and FY20, to date, and provide an update on each project, including the amount budgeted, actual dollars spent, and any remaining balances. In addition, please provide:

a. An update on all capital projects begun, in progress, or concluded in FY18, FY19, and FY20, to date, including the amount budgeted, actual dollars spent, and any remaining balances;
b. An update on all capital projects planned for the four-year financial plan;

c. A description of whether the capital projects begun, in progress, or concluded in FY18, FY19, and FY20, to date, had an impact on the operating budget of the agency. If so, please provide an accounting of such impact; and

d. A description and the fund balance for each existing allotment in each capital project under the agency's purview.

HSEMA received and was allotted $4.25M in FY20 capital funding to accomplish one project: the renovation of the District's Emergency Operations Center. To date, HSEMA has worked with the Department of General Services (DGS) to select a vendor to provide architectural/engineering services (A/E) for the design and construction of the EOC. In January 2020, HSEMA held a kick-off meeting with the design firm, commencing the renovation. The anticipated completion date is 24 months.

11. Please provide a list of all budget enhancement requests (including capital improvement needs) for FY19 and FY20, to date. For each, include a description of the need and the amount of funding requested.

HSEMA works in close collaboration with the Mayor's Office of Budget and Performance Management and the Deputy Mayor for Public Safety and Justice to develop our budget. The FY19 and FY20 agency budgets submitted as part of the Mayor's budget submissions reflect those efforts.

12. Please list, in chronological order, each reprogramming in FY19 and FY20, to date, that impacted the agency, including those that moved funds into the agency, out of the agency, or within the agency. Include known, anticipated reprogrammings, as well as the revised, final budget for your agency after the reprogrammings. For each reprogramming, list the date, amount, rationale, and reprogramming number.

Please see "Q12 HSEMA".

13. Please list each grant or sub-grant <u>received by</u> your agency in FY19 and FY20, to date. List the date, amount, source, purpose of the grant or sub-grant received, and amount expended.

Grant Program	Date	Amount	Expended to date	Source	Purpose
Emergency Management Performance Grant (EMPG)	9/17/2019	$3,071,016	$2,219,641	DHS-FEMA	The purpose of the FY 2019 EMPG Program is to give grants to assist state, local, tribal, and territorial governments in preparing for all hazards, as authorized by the Robert T. Stafford Disaster Relief and

Grant Program	Date	Amount	Expended to date	Source	Purpose
					Emergency Assistance Act (42 U.S.C. 5121 et seq.).
Homeland Security Grant Program (HSGP) - includes the State Homeland Security Program (SHSP) and Urban Areas Security Initiative (UASI)	08/26/2019	Total: $58,500,000 UASI: $52,750,000 SHSP: $5,750,000	Total: $1,311,299 UASI: $1,18,190 SHSP: $193,109	DHS-FEMA	The FY 2019 HSGP provides funding for planning, organization, equipment, training, and exercise needs of states and high-threat, high-density urban areas, and assists them in building an enhanced and sustainable capacity to prevent, protect against, respond to, and recover from acts of terrorism. It is composed of the UASI and SHSP.
Nonprofit Security Grant Program (NSGP)	9/09/2019	$4,449,845	$14,646	DHS-FEMA	NSGP provides funding support for target hardening activities to nonprofit organizations that are at high risk of a terrorist attack and located within one of the UASI-eligible urban areas. DC had 47 successful applicants in FY2019.
Regional Catastrophic Preparedness Grant Program (RCPGP)	9/13/2019	$1,138,790	$0	DHS-FEMA	The FY 2019 RCPGP provides funding to close known capability gaps and encourage innovative regional solutions to issues related to catastrophic incidents, specifically targeting capabilities for food, water, and sheltering.
Pre-Disaster Mitigation Grant Program	3/28/2019	$1,339,073.25	$0	DHS-FEMA	The pre disaster mitigation grant program funds a range of activities to support a sustained pre-disaster natural hazard mitigation program aimed at reducing the overall risk to the population and structures from future hazard events. This project will support the installation of Supervisory Control And Data

Grant Program	Date	Amount	Expended to date	Source	Purpose
					Acquisition (SCADA) systems at 13 stormwater pumping stations.
Pre-Disaster Mitigation Grant Program	7/3/2019	$818,079	$0	DHS-FEMA	The pre disaster mitigation grant program funds a range of activities to support a sustained pre-disaster natural hazard mitigation program aimed at reducing the overall risk to the population and structures from future hazard events. This project will support the replacement of the 12th Street and Main Avenue pump station.

a. How many FTEs are dependent on grant funding? What are the terms of this funding? If it is set to expire, what plans, if any, are in place to continue funding the FTEs?

All of HSEMA's FTEs are either fully or partially dependent on grant funding (total of 142 FTEs). Grant-funded employees work in support of the federal grant programs' goals, which are emergency preparedness and response, building homeland security capabilities, and reducing or eliminating long-term risk to people and property from natural hazards.

The current grant programs are multi-year and will not expire this fiscal year. Continued funding is dependent on Congress appropriating FY2020 grants. HSEMA is currently working with DC Office of Federal and Regional Affairs (OFRA) as well as our partners in the federal agencies, Federal Emergency Management Agency (FEMA) and Department of Homeland Security (DHS), to ensure that the District continues to receive the homeland security grant funding necessary to further our mission.

14. Please list each grant or sub-grant <u>granted by</u> your agency in FY19 and FY20, to date. List the date, amount, source, and purpose of the grant or sub-grant granted.

Please see attachment "Q14 HSEMA". Note: FY20 data is through 01/24/2020.

15. Please list each contract, procurement, and lease, entered into or extended and option years exercised by your agency during FY19 and FY20, to date. For each contract, procurement, or lease, please provide the following information, where applicable:

a. The name of the party;

b. The nature of the contract, procurement, or lease, including the end product or service;
c. The dollar amount of the contract, procurement, or lease, including amount budgeted and amount actually spent;
d. The term of the contract, procurement, or lease;
e. Whether it was competitively bid;
f. The name of the agency's contract monitor(s) and the results of any monitoring activity; and
g. The funding source.

Please see attachment "Q15 HSEMA". Note: FY20 data is current through 01/24/2020.

16. Please list all pending lawsuits that name the agency as a party. Identify which cases on the list are lawsuits that potentially expose the District to significant financial liability or will result in a change in agency practices and describe the current status of the litigation. Please provide the extent of each claim, regardless of its likelihood of success. For those identified, please include an explanation about the issues involved in each case.

The agency is not a named party in any pending lawsuits.

17. Please list all settlements entered into by the agency or by the District on behalf of the agency in FY19 or FY20, to date, and provide the parties' names, the date the settlement was entered into, the amount of the settlement, and if related to litigation, the case name, docket number, and a brief description of the case. If unrelated to litigation, please describe the underlying issue or reason for the settlement (e.g. administrative complaint, excessive use of force, etc.).

The agency has not entered into any settlements in FY19 and FY20, to date.

18. Please list the administrative complaints or grievances that the agency received in FY19 and FY20, to date, broken down by source. Please describe the process utilized to respond to any complaints and grievances received and any changes to agency policies or procedures that have resulted from complaints or grievances received. For any complaints or grievances that were resolved in FY19 or FY20, to date, describe the resolution.

The agency received seven administrative complaints/grievances in FY19 and FY 20, to date. The agency follows the grievance policies and procedures established in §§ 1626 through 1635 in the District Personnel Manual (DPM) for non-union employees. Union employees have the option to follow the grievance/arbitration procedures established in Article 24 of the Collective Bargaining Agreement (CBA) or the grievance policies and procedures established in §§ 1626 through 1635 in the DPM. The agency resolved three complaints/grievances to date: one complaint/grievance through OAG, two complaints/grievances through the EEO process, and one complaint/grievance through a mediation facilitated by DCHR. The agency has not made any changes to policies or procedures as a result of these complaints/grievances. The current CBA between HSEMA and the National Association of Government Employees Local R3-08,

originally effective October 1, 2014 through September 20, 2017, has expired. The agreement remains in force until either party to agreement states the desire to renegotiate. For reference, please see CBA article 34 section D the current CBA, attached as in attachment "Q32 HSEMA".

19. Please describe the agency's procedures for investigating allegations of sexual harassment, sexual misconduct, or discrimination committed by or against agency employees. List and describe any allegations relating to the agency or its employees in FY19 and FY20, to date, and whether and how those allegations were resolved (e.g. a specific disciplinary action, such as re-training, employee transfer, suspension, or termination).

a. Please also identify whether the agency became aware of any similar matters in FY19 or FY20, to date, through means other than an allegation, and if so, how the matter was resolved (e.g. sexual harassment was reported to the agency, but not by the victim).

The agency has not received any complaints or allegations of sexual harassment or other forms of sexual misconduct in FY19 or FY20, to date.

HSEMA's procedures for investigating allegations of sexual harassment, sexual misconduct, or discrimination committed by or against agency employees are in line with DCHR's sexual harassment issuance effective December 2019. The procedures are as follows:

1. Planning the investigation
2. Gathering the facts in a fair, objective manner
3. Conducting interviews
    - Complainant
    - Alleged harasser
    - Others with relevant information
4. Assessing credibility
5. Obtaining other needed evidence
6. Preparing a report

20. Please provide the Committee with a list of the total workers' compensation payments paid by the agency or on the agency's behalf in FY19 and FY20, to date, including the number of employees who received workers' compensation payments, in what amounts, and for what reasons.

The agency did not process any workers' compensation payments in FY19 or FY20, to date.

21. Please list and describe any ongoing investigations, audits, or reports on the agency or any employee of the agency, or any investigations, studies, audits, or reports on the agency or any employee of the agency that were completed during FY19 and FY20, to date.

During FY19, HSEMA participated in the FY18 DC Single Audit of Federal Awards Programs, which resulted in no findings.

During FY19 HSEMA closed out findings from the FY17 DC Single Audit that resulted in a refund of $86,988.66 to FEMA for the Snowstorm Jonas Public Assistance Grant. All findings from that audit were fully closed out in FY19.

The Federal Emergency Management Agency (FEMA) performed a desk-based monitoring of HSEMA's management of FEMA grant programs. Responses to questions and requested files were exchanged between July and September 2019. FEMA provided its findings on November 26, 2019 and assigned 2 follow-up actions due by January 31, 2020.

22. Please describe any spending pressures the agency experienced in FY19 and any anticipated spending pressures for the remainder of FY20. Include a description of the pressure and the estimated amount. If the spending pressure was in FY19, describe how it was resolved, and if the spending pressure is in FY20, describe any proposed solutions.

The agency did not experience any spending pressures in FY19 and does not anticipate any spending pressures in FY20.

23. Please provide a copy of the agency's FY19 performance plan. Please explain which performance plan objectives were completed in FY19, and whether they were completed on time and within budget. If they were not, please provide an explanation.

HSEMA fully met all but three of its key performance indicator (KPI) targets in FY19.

- The first of these measures, "Percent of employees with activation responsibilities certified in their EOC activation role" was not met with only 36% of applicable employees certified. HSEMA was unable to fully meet this KPI due to changes in FEMA's guidelines for EOC credentialing in FY18 that necessitated changes to our credentialing program. These new requirements are currently being incorporated into our program through restructuring of the EOC teams, training development and delivery, and establishment of credentialing standards. HSEMA anticipates that we will be able to meet this KPI for FY20.
- Secondly, the agency did not fully meet its KPI goal of 10% for "Percent of distributable analytic products co-authored with one or more federal, state or local partners." While the NTIC collaborated with partners for many of its analytic projects, it formally co-authored a much smaller number. The formal process for co-authoring is used less frequently because it can significantly increase the amount of time it takes to finalize and distribute these products.
- Finally, the agency did not meet its target of 95% for "Percent of employees funded through the FEMA Emergency Management Performance Grants (EMPG) program that have completed the EMPG training requirements." This KPI was nearly met with a final measure of 92.6%. Staff turnover, specifically on the training and exercise support team, resulted in incomplete

training records for EMPG-funded staff. During FY19, HSEMA hired a dedicated state training officer who is implanting the processes necessary to address this shortfall, and the agency anticipates that this target will be met in FY20.

HSEMA also completed all but one of our strategic initiatives. The agency's "Enhance Emergency Operations Center Operations" initiative was not completed because funding for the agency's planned renovation did not become available until August 2019.

In addition, please see FY19 Performance Accountability Report as attachment "Q23 HSEMA".

24. Please provide a copy of your agency's FY20 performance plan as submitted to the Office of the City Administrator.

Please see attachment "Q24 HSEMA".

25. Please describe any regulations promulgated by the agency in FY19 or FY20, to date, and the status of each.

The agency did not promulgate any regulations in FY19 or FY20, to date. However, there is an upcoming hearing before DC Council on February 6, 2020 for the "District of Columbia Government Continuity of Operations Plans Amendment Act of 2019." The purpose of this legislation is to amend HSEMA's enabling statute to require both subordinate and independent agencies of the District of Columbia to work with the Homeland Security and Emergency Management Agency to develop, update, and regularly exercise Continuity of Operations Plans. We anticipate, pending approval from Council, that this will be in enacted in 2020.

26. Please provide the number of FOIA requests for FY19 and FY20, to date, that were submitted to your agency. Include the number granted, partially granted, denied, and pending. In addition, please provide the average response time, the estimated number of FTEs required to process requests, the estimated number of hours spent responding to these requests, and the cost of compliance.

FOIA Requests	**FY19**	**FY20, to date (01/24/2020)**
Total # of Requests Received	130	23
Total granted in full	38	7
Total partially granted	16	0
Total denied	1	0
Total pending	0	3
Average Response Time (Days)	3.6	4.9
# of FTEs Processing Requests	2	1
# of Hours Processing Requests	164	30
Cost of Compliance	$8,465.68	$1,548.60

27. Please provide a list of all studies, research papers, reports, and analyses that the agency prepared or contracted for during FY19 and FY20, to date. Please state the status and purpose of each. Please submit a hard copy to the Committee if the study, research paper, report, or analysis is complete.

HSEMA has contracted through MWCOG with Tetra Tech to develop a Field Safety Manual and training materials that will guide HSEMA's response to and support of incidents when staff have deployed outside of the office setting. We expect that this will be completed by FY20 Q4.

Due to the sensitive nature of HSEMA's non-public documents, only UNCLASSIFIED Intelligence Bulletins, posted online at https://www.ncrintel.org/intelligence-products are available for Council review. In addition, please see attachment "Q27 HSEMA" for the list of distributed cyber threat bulletins in FY19 and FY20, to date (January 24, 2020).

Lastly, the District Hazard Mitigation Plan (DHMP) provides critical information, situation assessments, risk assessments, and operational tactics based on best practices to aid multi-agency efforts in mitigation District hazards, and establishes a base for thorough identification of hazards, risk analysis, efficient hazard management, and implementation of hazard reduction and avoidance measures. The DHMP was adopted on December 18, 2018, requalifying the District to be eligible for these grants and continued use of currently awarded funding. The latest version is currently in draft and is therefore not available to include for attachment.

28. Please list in descending order the top 25 overtime earners in your agency in FY19 and FY20, to date, if applicable. For each, state the employee's name, position number, position title, program, activity, salary, fringe, and the aggregate amount of overtime pay earned. Please describe the process the agency uses to determine which employees are granted overtime.

Please see attachment "Q28 HSEMA". Please note, FY20 data is through January 24, 2020.

HSEMA follows the District Personnel Manual Chapter 11 and 12 and the Collective Bargaining Agreement (CBA) when administering overtime for our employees. Also, overtime is managed at the agency bureau level. Bureau managers approve employees for overtime if there is an operational need. Please see the current CBA, attachment "Q32 HSEMA".

29. For FY19 and FY20, to date, please provide a list of employee bonuses or special pay granted that identifies the employee receiving the bonus or special pay, the amount received, and the reason for the bonus or special pay.

Fiscal Year	Employee Name	Position Title	Bonus Pay	Special Award	Reason
20	Steven Benefield	Communications Management Specialist	$25,000	N/A	Retirement

30. For FY19 and FY20, to date, please list each employee separated from the agency with separation pay. State the amount and number of weeks of pay. Also, for each, state the reason for the separation.

In FY19 and FY20, to date, the agency has had no separated employees who received separation pay.

31. Please provide the name of each employee who was or is on administrative leave in FY19 and FY20, to date. In addition, for each employee identified, please provide: (1) their position; (2) a brief description of the reason they were placed on leave; (3) the dates they were/are on administrative leave; (4) whether the leave was/is paid or unpaid; and (5) their current status.

Name	Title	Reason	Time Frame	Paid/ Unpaid	Current Status
Frederick Goldsmith	Deputy Chief of Operations	Operations pending final decision on corrective or adverse action per DPM § 1619.1.	10/10/19-Present	Paid	Admin Leave

32. Please provide each collective bargaining agreement that is currently in effect for agency employees. Please include the bargaining unit and the duration of each agreement. Please note if the agency is currently in bargaining and its anticipated completion.

The current Collective Bargaining Agreement (CBA), originally effective October 1, 2014 through September 20, 2017, remains in effect until September 30, 2020. Please see the current CBA, attached as "Q32 HSEMA".

33. If there are any boards, commissions, or task forces associated with your agency, please provide a chart listing the names, number of years served, agency affiliation, and attendance of each member. Include any vacancies. Please also attach agendas and minutes of each board, commission, or task force meeting in FY19 or FY20, to date, if minutes were prepared. Please inform the Committee if the board, commission, or task force did not convene during any month.

Information for the Local Emergency Planning Council (LEPC) membership is included in the chart below:

Agency/ Organization	Meeting #1 10/15/2019	Meeting #2 1/21/2020	Additional info
DC HSEMA	Lisa White	Lisa White	Core Agency

Agency/ Organization	Meeting #1 10/15/2019	Meeting #2 1/21/2020	Additional info
	Ali Lampson Donell Harvin Travis Cryan Jon Stewart Nickea Bradley Jason Rubinstein NTIC Representative	Ali Lampson Donell Harvin Travis Cryan Dion Black Natalie Hix Jason Rubinstein Madison Mattingly	
DOEE	Jayne Deichmeister	Jayne Deichmeister	Core Agency
FEMS	Chief Falwell	LT. John Barnes	Core Agency
MD/VA Local Agencies	Mike Grierson		NCR Partner
DC Health	Marc Barbiere	Julia Rich	
Dept. of Defense	Darryl Hart		Federal Partner
DCRA			
DHS	Justin Brown		
DDOT			
DPW		Wanda Ellis	
MPD	Capt. Caren	Capt. Caren	
Red Cross			
CSX			
WMATA			
DC Hospital Association			

Agency/ Organization	Meeting #1 10/15/2019	Meeting #2 1/21/2020	Additional info
Georgetown Hospital			
GW Hospital			
Howard Hospital			
Children's National Hospital			
DC Water			
Washington Gas Company			
EPA			
PEPCO			

**Please note we have had two official LEPC meetings. The first few groups were kept small by design. More partners were invited for the later meetings. This is a comprehensive list of who has either attended, who will attend, or who we would like to attend in order to build up the District's ability to integrate, coordinate, and partner with local, federal, and regional partners. In addition, all LEPC members are within their first year of service.*

Please see attachment "Q33a HSEMA Part 1" for the 10/15/19 Meeting Agenda, attachment "Q33a HSEMA Part 2" for the 10/15/19 Meeting Minutes, attachment "Q33a HSEMA Part 3" for the January 21, 2020 Meeting Agenda, and attachment "Q33a HSEMA Part 4" for the January 21, 2020 meeting minutes.

The Homeland Security Commission currently has one vacancy. The most recent meeting was held in May 2019. Additional information for the Homeland Security Commission is included in the table below:

Commissioner	Confirmation Date/Term Beginning	Term End	Residence	Attendance
David Heyman (HSC Chair)	May 22, 2017	February 22, 2019 (Mr. Heyman served in a hold-over capacity through August 2019)	Ward 4	December 8, 2017; April 20, 2018; June 21, 2018; August 20, 2018; November 16, 2018, March 1, 2019; April 12, 2019; May 20, 2019
Philip McNamara	July 11, 2017	February 22, 2022 (Reappointment approved by DC Council in January 2020)	Ward 1	December 8, 2017; April 20, 2018; November 16, 2018, March 1, 2019; April 12, 2019; May 20, 2019
Meloyde Batten-Mickens	December 8, 2017	February 22, 2020	Fort Washingt on, MD	December 8, 2017; June 21, 2018; August 20, 2018; November 16, 2018; January 17, 2019; April 12, 2019; May 20, 2019
Brad Belzak	December 8, 2017	February 22, 2022 (Reappointment approved by DC Council in January 2020)	Ward 2	December 8, 2017; April 20, 2018; June 21, 2018; August 20, 2018; November 16, 2018; January 17, 2019; March 1, 2019; April 12, 2019; May 20, 2019
Edward Pearson	December 18, 2018	February 22, 2022	Ward 7	January 17, 2019; March 1, 2019; April 12, 2019; May 20, 2019
Joanna Turner	December 18, 2018	February 22, 2022	Ward 6	January 17, 2019; March 1, 2019; April 12, 2019
Brian Baker	December 18, 2018	February 22, 2022	Ward 6	January 17, 2019; March 1, 2019; April 12, 2019; May 20, 2019

Please see attachment "Q33b HSEMA Part 1" for the FY19 and FY20, to date meeting agendas and attachment "Q33b HSEMA Part 2" for the open meeting minutes. Please note, there were two meetings held in November 2018 and none held in December 2018 and February 2019.

Please see the following Unmanned Aircraft System (UAS) Working Group member information:

TIGER TEAM

Name	Affiliation

Rick Owen	Office of Contracting and Procurement (OCP)
Jeffery Carroll	Metropolitan Police Dept (MPD)
Travis Gross	Homeland Security and Emergency Management Agency (HSEMA)
Erika Satterlee	Executive Officer of the Mayor (EOM)
Robert Bozarth	Fire and Emergency Medical Services Dept (FEMS)
Michelle Caron	Metropolitan Police Dept (MPD)
Helen McClure	Office of the Deputy Mayor for Public Safety and Justice (DMPSJ)
Jane Waters	Office of Risk Management (ORM)
Matt Crossett	Office of the Chief Technology Officer (OCTO)
Turna Lewis	Office of the Chief Technology Officer (OCTO)

UAS TIGER TEAM MEMBERS

Name	Affiliation
Mark Adamchik	US Park Police (USPP)
Mark Aitken	Akin Gump
Jim Anderson	Insurance Carrier
Robert Bozarth	Fire and Emergency Medical Services Dept (FEMS)
Robert Campbell	US Capitol Police (USCP)
Linda Canfield	United States Secret Service (USSS)
Sarah Case-Herron	Homeland Security and Emergency Management Agency (HSEMA)
Suneel Cherukui	Office of the Chief Technology Officer (OCTO)
Rudy Chounoune	Fire and Emergency Medical Services Dept (FEMS)
Conan Bruce	Dept of General Services (DGS)
Terry D. Couch	Metropolitan Police Dept (MPD)
Steven Cronberry	Metropolitan Washington Airports Authority (MWAA)
Matthew Crossett	Office of the Chief Technology Officer (OCTO)
Kimberly Dickerson	Metropolitan Police Dept (MPD)
Paul Duray	DC Health
Jayne Deichmeister	Dept of Energy & Environment (DOEE)
Wanda Ellis	Department of Public Works (DPW)
Lynn Enos	US Dept of Homeland Security (DHS)
Benjamin Falls	Federal Bureau of Investigation-Washington Field Office (FBI-WFO)
William (Bill) Farr	Metropolitan Police Dept (MPD)
Aidan Garcia	Federal Bureau of Investigation-Washington Field Office (FBI-WFO)
Roger Gatton	Office of Risk Management (ORM)
Richard Gaylord	Federal Bureau of Investigation-Washington Field Office (FBI-WFO)

Elliot Grollman	FPS (Federal Protective Service)
Jestelle Hanrahan	Homeland Security and Emergency Management Agency (HSEMA)
Ronald Harris	Metropolitan Police Dept (MPD)
Adam Jachimowicz	Homeland Security and Emergency Management Agency (HSEMA)
Sarah Jacob	US Dept of Homeland Security (US DHS)
Kent Jefferies	Transportation Security Administration (TSA)
Shani Jones	Office of United Communications (OUC)
Robert Kelley	Office of Risk Management (ORM)
James Kelly	Metropolitan Police Dept (MPD)
Barney Krucoff	Office of the Chief Technology Officer (OCTO)
Kenneth Liebowitz	Office of the City Administrator (OCA)
Nina Liggett	Office of the Chief Technology Officer (OCTO)
Jason Litowitz	National Counter Terrorism Center (NCTC)
Mark McDonald	Federal Aviation Administration (FAA)
Shana Mell	Metropolitan Police Dept (MPD)
Carlos Mejia	Metropolitan Police Dept (MPD)
Fred Muccino	Federal Protective Service (FPS)
Scott Parker	US Dept of Homeland Security (US DHS)
Nicole Peckumn	Executive Officer of the Mayor (EOM)
Tiffany Peterson	Homeland Security and Emergency Management Agency (HSEMA)
Serge Potapov	Transportation Security Administration (TSA)
Robert Preston	Office of Risk Management (ORM)
Casey Priester	Cyber Security Small & Medium Enterprises (SME)
Otto Romero	Metropolitan Police Dept (MPD)
Terry Ryan	Metropolitan Police Dept (MPD)
Mark Scott	Homeland Security and Emergency Management Agency (HSEMA)
Will Shelby	National Counter Terrorism Center (NCTC)
Jessica Smith	Office of the Deputy Mayor for Health and Human Services (DMHHS)
Kyle Sparks	Insurance Carrier
Michael Spochart	US Capitol Police (USCP)
Chad Sutton	Transportation Security Administration (TSA)
Chris Sutton	Office of the Chief Technology Officer (OCTO)
Daniel Thau	Metropolitan Police Dept (MPD)
Muriel Turner	Insurance Broker
Mark Varanelli	US Park Police (USPP)
Tracy Walraven	Dept of Forensic Sciences (DFS)
Victoria Wassmer,	Ernst & Young
Kyle Wolf	US Dept of Homeland Security (US DHS)

TIGER TEAM STAFF

Homeland Security and Emergency Management Agency (HSEMA) Staff	Title
Charles Guddemi	Lead
Annah Akasa	Coordinator
Adam Baron	Action Officer
James Farley	Action Officer
Steven Hoodjer	Action Officer
Nicole McDermott	Action Officer

UAS TIGER TEAM TECHNICAL ADVISORS

Name	Affiliation
Deepu John	New York City Police Dept (NYPD)
Mike Keefe	Virginia Dept of Energy Management
Kyle Miller	Skyfire Drones
John O'Conner	Small Unmanned Aircraft Systems Program - Seat Pleasant, MD (SUAS)
Chris Sadler	York County (VA) Police
Gunner Smith	Measure Inc.
Andrew Sussman	Geospatial Corporation
David Thirtyacre	Embry Riddle's Drone Program
Wayne Wylie	Virginia Department of Emergency Management

TIGER TEAM EX OFFICIO MEMBERS

Name	Affiliation
Angela Stubblefield	Federal Aviation Administration (FAA)
Peggy Gilligan (Retired)	Federal Aviation Administration (FAA)
Mark Bathrick	Department of Interior (DOI)
Joseph Mazel	Federal Bureau of Investigation (FBI)
Roy Shrout	Fairfax Office of Emergency Management
William "Tom" Hewitt	US Dept of Homeland Security (US DHS)
Michael Spochart	US Capitol Police (USCP)
Robert Campbell	US Capitol Police (USCP)
Dan Gettinger	Center for the Study of the Drone at Bard College
Charles Werner	Drone Responders
Bill Staton	Federal Aviation Administration (FAA)
Darshan Divakaran	North Carolina Department of Transportation (NCDOT) (also UAS & GIS)
Tom McMahon	Association for Unmanned Vehicle Systems International (AUVSI)
Gregory S. Walden	Small UAV (Unmanned Aerial Vehicle) Coalition
Todd Craig	Federal Bureau of Prisons (DOJ)
Vincent Guerrieri	New York City Police Dept (NYPD)
Arthur Mogil	New York City Police Dept (NYPD)

Please see attachment "Q33c HSEMA Part 1" for meeting agendas, "Q33c HSEMA Part 2" for meeting minutes, and "Q33c HSEMA Part 3" for meeting sign-in sheets.

34. Please list all reports or reporting currently required of the agency in the District of Columbia Code or Municipal Regulations. Provide a description of whether the agency is in compliance with these requirements, and if not, why not (e.g. the purpose behind the requirement is moot, etc.).

The "Homeland Security, Risk Reduction, and Preparedness Amendment Act of 2006" requires the Executive to submit to the Council of the District of Columbia an annual report describing the current level of preparedness in the District. Work on the 2019 annual report is currently underway.

35. Please provide a list of any additional training or continuing education opportunities made available to agency employees. For each additional training or continuing education program, please provide the subject of the training, the names of the trainers, and the number of agency employees that were trained.

Course Name/Subject	# of Participants (HSEMA Staff, District and National Capital Region)	Training Entity Providing Instruction
Basic Public Information Officers Course	27	Contracted Instructor
Benefit-Cost Analysis: Entry-Level Training	9	Contracted Instructor
Bomb Threat Management Planning	11	National Disaster Preparedness Consortium
Continuity of Operations (COOP) Seminar/Table Top Exercise	40	FEMA
Continuity of Operations Plan (COOP) Workshop	43	FEMA
Continuity of Operations Planning Seminar and Table Top Exercise	53	FEMA
Design Thinking	36	Contracted Instructor
Emergency Liaison Officer Training (ELO)	36	HSEMA
ERisk Incident Reporting Portal Training (Internal HSEMA Course)	16	DC ORM
Foundations of Emergency Management Week 1	29	FEMA EMI
Foundations of Emergency Management Week 2	27	FEMA EMI
G 191: EOC/ICS Interface	12	HSEMA
G 191: EOC/ICS Interface	40	HSEMA
G-775: Emergency Operations Center (EOC) Management and Operation	40	HSEMA
Homeland Security Exercise and Evaluation Program (HSEEP)	22	HSEMA

Course Name/Subject	# of Participants (HSEMA Staff, District and National Capital Region)	Training Entity Providing Instruction
Homeland Security Exercise and Evaluation Program (HSEEP)	58	HSEMA
ICS - 300, Intermediate ICS for Expanding Events	88	HSEMA
ICS 400: Advanced ICS for Command and General Staff, Complex Incidents and MACS	49	HSEMA
IED Search Procedures	11	National Disaster Preparedness Consortium
Incident Response to Terrorist Bombings (Session I)	10	National Disaster Preparedness Consortium
Incident Response to Terrorist Bombings (Session II)	10	National Disaster Preparedness Consortium
Instructor Development Workshop	20	National Disaster Preparedness Consortium
Intelligence Writing and Briefing Fundamentals	47	Contracted Instructor
Introduction to Lean Process and Six Sigma	20	Contracted Instructor
L-364: Multihazard Emergency Planning for Schools	9	National Disaster Preparedness Consortium
L-548: Continuity of Operations Planning Program Manager Course	22	FEMA
L-550: Continuity of Operations Planning	15	FEMA
L-950: NIMS ICS All-Hazards Incident Commander	12	Wiland Associates
L-954: NIMS ICS All-Hazard Safety Officer	14	Wiland Associates
L-956: NIMS ICS All-Hazards Liaison Officer	30	Wiland Associates
L-958: NIMS ICS All-Hazards Operations Section Chief	12	Wiland Associates
L-962: NIMS ICS All-Hazards Planning Section Chief	10	Wiland Associates
L-964: NIMS ICS All-Hazards Situation Unit Leader	30	Wiland Associates
L-965: NIMS ICS All-Hazards Resource Unit Leader	21	Wiland Associates
L-967: NIMS ICS All-Hazards Logistics Section Chief	10	Wiland Associates
Planning: Emergency Operations	28	HSEMA

Course Name/Subject	# of Participants (HSEMA Staff, District and National Capital Region)	Training Entity Providing Instruction
Public Information and Warning	21	National Disaster Preparedness Consortium
Science for Disasters	29	FEMA EMI
Unmanned Aircraft Systems in Disaster Management	23	National Disaster Preparedness Consortium
WebEOC	22	HSEMA
WebEOC User Training	17	HSEMA
Writing For Clarity	30	Contracted Instructor
The Leadership Challenge	19	HSEMA & DCHR
Leadership Awareness	20	Andres Marquez-Lara
Failing Forward	24	HSEMA
Performance Management	17	DCHR
Change Management	16	Andres Marquez-Lara
Leading w/ Strategy	13	Andres Marquez-Lara

36. Please describe any initiatives that the agency implemented in FY19 or FY20, to date, to improve the internal operations of the agency or the interaction of the agency with outside parties. Please describe the results, or expected results, of each initiative.

See attachment "Q23 HSEMA" for our FY19 Performance Accountability Report (PAR). Additionally, please see FY20's first quarter reporting information, detailing our initiatives and progress in achieving the results for the current fiscal year, below:

- **Initiative 1:** In FY20, HSEMA will complete home surveys in Watts Branch (Ward 7) to determine the eligibility of homes for floodproofing mitigation. These surveys will be used to create a FloodSmart program, similar to RiverSmart and Great Streets, and increase the resilience of the community against potential flooding impacts.
    - ***Q1 Update: 0-24% Complete*** - *Contact with homeowners in the subject area has been achieved; currently awaiting voluntary enlistment of up to 70 participants.*
- **Initiative 2:** In FY20, HSEMA will create an outreach workshop in Ward 8 focused on insurance coverage including home owner, rental, and commercial policies. The workshops will also cover how FEMA and the Small Business Administration may subsidize insurance after a disaster or major loss.

- ***Q1 Update: 0-24% Complete*** *– Have conducted planning meetings in FEMA Region 3 and with DC government partners for workshop development.*

- **Initiative 3:** In FY20, HSEMA will continue to upgrade the capabilities of the District's Emergency Operations Center (EOC). Working with the Department of General Services, HSEMA will redesign the EOC floor space to increase efficiency and maximize capacity during operations. HSEMA expects the design phase of this project to be complete by the end of FY20. In addition, HSEMA expects to have an enhanced situational awareness platform in place by the close of FY20.
    - ***Q1 Update: 0-24% Complete*** *- To date, the contractor and architectural/engineering services has been selected. HSEMA anticipates a ratified contract by January 2020.*
- **Initiative 4:** In FY20, HSEMA will lead the inter-agency Incident Management Team Academy, which will graduate its first cohort and welcome a second cohort. Each IMT cohorts will provide enhanced incident management and emergency preparedness capabilities to District agencies and partners, building combined strength across the District for the management of major incidents.
    - ***Q1 Update: 25-49% Complete*** *- Cohort 1 members are completing training requirements and participating in exercises to practice and demonstrate skills in their IMT roles. This cohort will graduate in Q2 and continue to work towards completion of the fully signed task books required to achieve their final credential. Standard practice indicates a multi-year process to achieve final credentials. Recruitment and course scheduling are in process for Cohort 2.*
- **Initiative 5:** In FY20, HSEMA will establish physical risk assessment teams to conduct periodic physical risk assessments of District government buildings to identify vulnerabilities that could put the facilities at increased risk. Teams will be formed, trained, and ready for deployment by the end of FY20.
    - ***Q1 Update: 0-24% Complete*** *- During Q1 HSEMA completed the administrative requirements to put the necessary trainings in place. During Q2, the agency will identify and begin training the appropriate staff to participate in training for the physical risk assessment teams.*

37. What are the agency's top five priorities? Please explain how the agency expects to address these priorities in FY20. How did the agency address its top priorities listed for this question last year?

In FY20, HSEMA will continue to address the top five priorities introduced in FY19, building upon our progress over the past year:

- *Strengthening HSEMA's organizational performance* – HSEMA will improve organizational performance by building on process improvements made last year, continuing to integrate our intelligence and emergency management functions, and by developing and deploying a key piece of technology (ESRI) that will improve situational awareness of the District. In

FY19, we focused on improving performance by developing new policies, as well as new administrative tools and processes (e.g., purchase request forms, travel forms, performance review forms), and continuing the quarterly performance reporting process and re-training all staff.

- *Optimizing the way HSEMA spends grant dollars* – HSEMA will optimize the way it spends grant money by evaluating return on investment for key grant programs. In FY19, the Agency continued examining current spending against historical spending, preparing for federal budget cuts potentially impacting our grant programs, and continuing to refine the annual budgeting cycle to better track spending.
- *Building a regional intelligence capability* – HSEMA seeks to expand upon the capabilities and responsive of the National Capital Region Threat Intelligence Consortium (NTIC) by standing up a cybersecurity center and integrating a regional watch center into the fusion center. HSEMA will continue to invest resources for hiring and training new analysts and improve the quality of our analytic products.
- *Develop a whole of community approach to disaster management and disaster preparedness* – HSEMA will continue to focus on improving outreach to two key constituencies in the District – the private industry and faith-based communities. Moving the needle forward with our identified audience, in FY19, we launched the agency's first ever advertisement campaign specifically geared towards the District's faith-based community. HSEMA partnered with Radio One's 104.1 Praise FM station to inform District residents of the faith-based preparedness materials offered through ReadyDC and of the Interfaith Preparedness and Advisory Group (IPAG). The campaign consisted of on-air interviews with Director Rodriguez, a digital component on the station's social media channels, and the presence of HSEMA's community outreach team at the 13th Annual Spirit of Praise Concert held in October 2019. The Spirit of Praise Concert is the largest event held in the District targeting the faith-based community and was held at the Sports Arena in Ward 8.
- *Become a more anticipatory organization* – HSEMA is proactively acquiring and utilizing new technology to improve our operational and preparedness capabilities. HSEMA has created and continues to develop a suite of weather-related products to help the District better prepare for the impacts of severe weather events. Additionally, the agency continues to invest resources in impending threat analyses ahead of multiple first-amendment events.

38. Please list each new program implemented by the agency during FY19 and FY20, to date. For each initiative, please provide:

a. A description of the initiative;
b. The funding required to implement the initiative; and
c. Any documented results of the initiative.

School Safety Initiative

a. Description: The School Safety Initiative is a collaborative effort undertaken by District agencies to enhance school safety and security efforts through the School Safety Alliance (SSA). The SSA is an interagency team comprised of representatives from District government agencies.
b. Funding: There is no additional funding associated with this initiative. It is completely supported through existing resources.
c. Results: This project has already accomplished several goals:
    - HSEMA's National Capital Region Threat Intelligence Consortium (NTIC) launched a new tool, a school resource packet, highlighting threat issues for students and school personnel. The tool helps secure schools and raises awareness of emerging issues, safety trends, and available resources. To date NTIC has circulated three resource packets.
    - HSEMA, in collaboration with DCPS, the U.S. Department of Homeland Security (U.S. DHS), and DGS, has conducted an all-hazards risk assessment and completed school security assessments of seven school campuses.
    - HSEMA and DCPS are finalizing the School Emergency Preparedness Playbook. This Playbook provides guidance to assist schools in developing new plans or updating existing plans using national best practices for emergency management.
    - HSEMA is collaborating with DCPS to provide planning, training and exercise support in assisting the River Terrace Education Campus (RTEC) with emergency response protocols and capabilities. RTEC is a public school catering to students with disabilities.

Interfaith Preparedness & Advisory Group (IPAG)

Description: The IPAG mission is to provide a platform for Faith-Based Organizations (FBO) to exchange information among themselves and with District Agency representatives concerning threats, vulnerabilities, best security practices, and protective measures related to the safety and security of their congregations and facilities. The IPAG is sponsored by the Mayor's Office of Religious Affairs, the DC Homeland Security and Emergency Management Agency (HSEMA) and the Metropolitan Police Department (MPD). The IPAG provides a platform for faith-based organizations to exchange information with security and preparedness professionals on threats, vulnerabilities, best security practices, and protective measures related to the safety and security of congregations and facilities.

a. Funding: There is no additional funding associated with this initiative. It is completely supported through existing resources.
b. Results (Quarterly Meetings):

    On February 28, 2019 the IPAG kicked off its first quarterly meeting at 401 E Street, SW. The meeting highlighted the goals and objectives of the IPAG and brought in keynote speaker John Cohen to provide

an overview of threats that houses of worship face today.

On May 13, 2019 the IPAG hosted its second meeting at the Washington National Cathedral where a panel, moderated by Pierre Thomas, and consisting of Reverend Eric Manning, Alan Hausman, Reverend Frank Pomeroy, and Sherri Pomeroy, spoke to IPAG members about lessons learned from tragic incidents of mass violence around the nation.

- On September 3, 2019 the Adas Israel Congregation hosted IPAG's third quarterly meeting where participants were given training on how to report suspicious activity and training on "Until Help Arrives", part of the Stop the Bleed campaign to teach first aid to members of the faith community.
- On December 12, 2019 IPAG hosted its final quarterly meeting of 2019 at Shepard's Baptist Church and took time to reinforce how to report suspicious activity, as well as listening to presentations from FBI's Private Partnership Engagement team and DC's Department of Behavioral Health Community Response Team. IPAG members also received TECC kits if they attended the "Until Help Arrives" training.

Museum Partnership Strategic Initiative

a. Description: The Museum Partnership Strategic Initiative (MPSI) is a project designed to engage District public and private museums of varying scales, sizes, and subject matters with the goal of increasing interconnectedness and raising the collective level of security for this sector.
b. Funding Requirements: There is no additional funding associated with this initiative. It is completely supported through existing resources.
c. Results: Through this initiative, the NTIC has built relationships with existing museums with whom we had no previous engagement, strengthened existing relationships, and catalyzed information sharing through participants' use of NTIC-created "be on the lookout" and suspicious activity reporting templates.

*Updated Training for Emergency Liaison Officers (ELO***)**

a. Description: During emergencies and planned major events, District agencies and outside partners send staff to the District's Emergency Operations Center (EOC) to coordinate operations and foster collaboration. This role is known as the Emergency Liaison Officer (ELO). This initiative is designed to improve the training course that HSEMA provides to all ELOs by taking feedback from ELOs and incorporating lessons learned during the very previous two years to provide better and more effective training for ELOs.
b. Funding Requirements: There is no additional funding associated with this initiative. It is completely supported through existing resources.
c. Results: HSEMA delivered the first course to ELOs on 1/23/2019 and

received overwhelmingly positive feedback from the participants.

Joint All-Hazards Operations Center (JAHOC) Enhancements

a. Description: HSEMA is working to enhance the District's JAHOC operations by increasing hands-on training opportunities; developing additional watch and warning capabilities; expanding representation of other District agencies; and integrating the fusion center's intelligence capabilities into daily watch and warning operations.
b. Funding Requirements: There is no additional funding associated with this initiative. It is completely supported through existing resources.
c. Results: HSEMA has expanded our supervisor staffing in the JAHOC to provide one-on-one training opportunities for staff. The agency has also added three staff members to each shift to enhance existing capabilities and expand our services. HSEMA implemented an updated training program for JAHOC watch. The agency has also integrated an intelligence analyst into the JAHOC. We have also fully integrated a 24/7 intelligence component into the JAHOC and integrated our local and FEMA regional watch component.

Incident Coordination and Support Teams

a. Description**:** Building upon the success of the team that manages the District's Emergency Operations Center, HSEMA is working with a number of District agencies and outside partners, chiefly FEMS, to build deployable incident management teams. HSEMA is also updating the agency fleet to support collaboration at incidents and events.
b. Funding Requirements: There is no additional funding associated with this initiative. It is completely supported through existing resources.
c. Results: HSEMA has increased the frequency with which we are deploying incident coordination and support staff to incidents, specifically residential fires with displacements. We have also dedicated additional resources to developing a replicable safety program for our deployable staff that we will be sharing with our partners for them to implement within their own agencies in 2020.

Disability Integration Initiative (DII)

a. Description: The District of Columbia and Disability Advocacy groups reached a groundbreaking settlement agreement May 03, 2019. Under the historic settlement, the District has agreed to a comprehensive three-year implementation plan that includes: (1) creating a Disability Community Advisory Group that will provide disability-specific recommendations for emergency plans and trainings, (2) ensuring that emergency-related public communications are disseminated in accessible formats, (3) considering physical accessibility as a priority when opening emergency shelters, (4)

creating a Post-Emergency Canvassing Operation plan, (5) ensuring that transportation resources are sufficient to meet the potential demand for accessible transportation during emergencies, and (6) creating and implementing a work plan to improve procedures for evacuating people with disabilities from high-rise buildings. Through the completion of these requirements updates to the District's emergency plans to provide individuals with disabilities equal access to critical government services.

b. Funding: There is no additional funding associated with this initiative. It is completely supported through existing resources.
c. Results: DII has convened multifunctional working groups comprised of District agencies and community advocates to assist in updating and integrating emergency plans with inclusive strategies. A Mayor's Order and Memorandum of Agreement support the participation in completing the initiative holistically for the District. All milestones to date have been completed including, but not limited to, updating the HSEMA mobile app and website; Siteimprove, a web-based tool provided from OCTO to track 508 compliance[1] for all DC agency web pages; emergency sheltering analysis; and quarterly reports capturing progress in all the working groups.

Risk Reduction Consultation

a. Description: The purpose of this meeting was to strategize about the best use of public and private resources to collaborate on risk reduction programs and project delivery. Through this process, both the District and FEMA annually review risk reduction priorities, evaluate the status of reaching those priorities throughout the year, and identify the best way to leverage existing resources for implementation. As a result, District partners and FEMA can build upon the priorities identified in previous Risk Reduction Consultations.
b. Funding: There is no additional funding associated with this initiative. It is completely supported through existing resources.
c. Results: While the relevance and importance of the District's 2018 risk reduction priorities were reaffirmed, the focus for 2019 shifted to prioritizing planning areas (Watts Branch, Cardozo/Bloomingdale/Shaw, and the Southwest Waterfront) and one program area (FloodSmart). In light of 2019 findings, HSEMA prioritizes the need to collect more robust interior flood risk data within the metro area specifically geared towards interior flood measures. Mitigating the urban heat island effect, such as through green roofs and social interventions like Resiliency Hubs, presents a unique opportunity to reduce both extreme heat and flood risk. While the District has set a national example in blue-green infrastructure, there continues to be a need for deeper cross-agency collaboration as some mitigation strategies overlap priority planning areas for Resilient DC, Climate Ready DC, and Age-Friendly DC.

[1] Section 508 of the Rehabilitation Act requires that all website content be accessible to people with disabilities.

District Hazard Mitigation Plan

a. Description: The District Hazard Mitigation Plan (DHMP) serves as a District-wide guide for organized and coordinated efforts to mitigate the threats and hazards in the District. This Plan provides critical information, situation assessments, risk assessments, and operational tactics based on best practices to aid multi-agency efforts in mitigation District hazards, and establishes a base for thorough identification of hazards, risk analysis, efficient hazard management, and implementation of hazard reduction and avoidance measures. The mitigation strategy developed herein supports resilience through minimizing and eliminating human suffering and property loss associated with hazards and their consequential disasters.
b. Funding: Has a potential of $10M for pre-disaster mitigation, $10M for flood mitigation assistance, and a conditional amount based on the damages assessment if a disaster strikes.
c. Results: The DHMP was adopted on December 18, 2018, requalifying the District to be eligible for these grants and continued use of currently awarded funding.

Business Emergency Management Operations Center

a. Description: The Business Emergency Management Operations Center (BEMOC) is an alliance of public-private partners committed to improving the District's private sector's ability to prepare for, respond to, and recover from disasters. The BEMOC provides local businesses with emergency response information, planning assistance, trainings and exercises.
b. Funding: There is no additional funding associated with this initiative. It is completely supported through existing resources.
c. Results: The BEMOC has expanded membership, reaching to local, regional and national companies. The program also began hosting quarterly meetings, starting with an inaugural private sector emergency preparedness symposium on May 14, 2019, to discuss trends and topics related to the private sector's ability to prepare for and respond to business disruptions, daily disturbances, and large scale emergencies. The program also hosted a tabletop exercise that brought public and private sector partners together to discuss a coordinated response to a severe weather incident.

39. How does the agency measure programmatic success? Please discuss any changes to outcomes measurement in FY19 and FY20, to date.

In addition to the performance plan that every agency has, HSEMA employs a variety of other performance management tools and checklists to measure success. For example, FEMA's Threat and Hazard Identification and Risk Assessment (THIRA) is a preparedness tool that is used to measure growth, success, or improvements needed in a variety of core capability areas.

HSEMA submits its THIRA annually, along with a prioritized list of major program successes in core capability areas.

In addition, HSEMA continually measures ongoing compliance with industry best practices and standards as defined in Emergency Management Accreditation Program Standards (EMAP). HSEMA has successfully maintained its EMAP accreditation since 2003.

40. What are the top metrics and KPIs regularly used by the agency to evaluate its operations? Please be specific about which data points are monitored by the agency.

HSEMA tracks performance primarily through the KPIs and workload measures on our performance plan, as listed below. Among the highest priority metrics that HSEMA monitors are the increase in subscribers to our fusion center analytic products, the number of planning processes completed in accordance with the Emergency Management Accreditation Program requirements, readiness for EOC activation as measured by compliance with training requirements, and the increase in subscribers to the AlertDC program.

Please see the Key Performance Indicators and Workload Measures information, below:

Key Performance Indicators
Percentage of employees with activation responsibilities qualified in their EOC role
Percentage of eligible EOC staff in attendance at EOC Readiness training per quarter
Percentage of weekly EOC facility inspections completed per quarter
Percent of distributable analytic products co-authored with one or more federal, state or local partners
Percentage increase in subscribers to NTIC situational and analytic product distribution lists Percentage of EMAP accreditation standards for which HSEMA has current documentation
Percentage of employees funded through the FEMA Emergency Management Performance Grants (EMPG) program that have completed the EMPG training requirements
Percentage of new or revised plans (where the planning process was led by HSEMA) socialized through training or exercise.
Percentage increase of recipients of AlertDC
Percentage of Grant dollars spent within the timeframe of grants
Percentage of federal subgrants issued within 45 days of award receipt

Workload Measures	
Number of level 3 (enhanced) or higher Emergency Operations Center activations	Number of individuals trained by HSEMA
Number of days JAHOC teams are deployed to special events	Number of executive level staff completing an emergency senior/cabinet level training within 60 days of onboarding

Number of AlertDC messages sent to the public	Percent of District agencies with lead and support roles that participated in HSEMA led trainings or exercises
Number of HSEMA alerts sent to District government staff	Number of District agencies with lead and support roles that participated in HSEMA led trainings or exercises
Number of days agency staff are deployed to incident sites	Number of District agencies with lead and support roles
Alerts processed through JAHOC inbox	Number of community outreach events attended or conducted by HSEMA
Number of raw suspicious activity reports (SARs) processed	Number of special events that have been processed by the Mayor's Special Events Task Group
Number of requests for information (RFIs) processed	Number of reimbursements processed for subrecipients annually
Number of District plans created, revised, or reviewed for District Government partners annually	Number of active subawards
Number of trainings provided to first responders, District employees, and the public by HSEMA	Number of grant monitoring visits

41. Please identify whether, and if so, in what way, the agency engaged The Lab @ DC in FY19 or FY20, to date.

HSEMA has not engaged with The Lab @ DC in FY19 or FY20, to date.

42. Please list the task forces and organizations of which the agency is a member.

Locally, HSEMA manages the District Preparedness System and serves as co-chair of the District's Emergency Preparedness Committee (EPC). HSEMA is also an active participant in the following District- level task forces and working groups:

- School Safety Alliance (formerly the Emergency and Safety Alliance)
- Resilient DC Cabinet;
- Interagency Council on Homelessness;
- Smarter DC Tiger Team;
- Safe Passage to Schools;
- DC Department of Health Director's Opioid Committee;
- DC Health and Medical Coalition; and
- DC Human Trafficking Task Force.

In accordance with Mayor's Order 2018-084, dated October 22, 2018, HSEMA is the chair and coordinating agency for the Mayor's Unmanned Aerial Systems (UAS) working group, which is tasked with evaluating and making recommendations for a comprehensive program to incorporate UAS in the District's airspace. The working group will consider both public safety and commercial applications for the technology.

For additional information on UAS task force membership and LEPC membership and meeting information, please see question 33 response.

Information related to HSEMA's affiliated organizations and memberships may be found in question 6 response.

43. Please explain the impact on your agency of any legislation passed at the federal level during FY19 and FY20, to date, which significantly affected agency operations.

There has been no impact significantly affecting agency operations of any legislation passed at the federal level during FY19 and FY20, to date.

44. Please describe any steps the agency took in FY19 and FY20, to date, to improve the transparency of agency operations, including any website upgrades or major revisions.

Intranet:

In FY19 and FY20, to date, the agency continued to leverage the HSEMA intranet page as a tool to improve the transparency of agency operations. The HSEMA intranet is updated on a continuous basis to ensure the HSEMA community is kept abreast of information in a timely fashion. Additionally, in FY20, HSEMA launched the HSEMA Insights video series, which serves as a supplementary manner of updating the HSEMA community with agency news.

NTIC website:

In November 2018, the National Capital Region Threat Intelligence Consortium (NTIC) launched its public facing website—ncrintel.org—where we share information related to cyber, terrorism, and crime. Additionally, the website offers a subscription component for the public.

ReadyDC:

In FY19, HSEMA's Office of Public Affairs spearheaded the re-launch of the ReadyDC website (ready.dc.gov). Each section of the website (Be Aware, Be Prepared, Resources, and About Us) was reviewed for accuracy and additional content that needed to be edited, removed, and/or added based on emergency preparedness best practices. The re-launch of the content on the ReadyDC website included the addition of additional District-produced resources and information. When appropriate, District residents are now directed to other

District government websites before turning to external and federal partner sites. The ReadyDC site was re-launched in September 2019 to kick off National Preparedness Month.

HSEMA also created a 30-second, 508 compliant emergency preparedness video that debuted during National Preparedness Month. The video aims to empower District residents and businesses to become better prepared for the threats and hazards the District faces; and was aired on the jumbotrons during preparedness month events held at Audi Field, Nationals Park, and Capital One Arena.

Mobile App:

In FY19, HSEMA partnered with the Office of the Chief Technology Officer and the Office of Disability Rights to make major improvements to the compliance of the HSEMA website and the HSEMA mobile application with section 508 of the Americans with Disabilities Act. Utilizing SiteImprove, a tool provided to District agencies through OCTO, we were able to identify areas where our content was not 508 compliant. As of June 2019, HSEMA's website is 98% compliant, which is approximately 35% higher than the government benchmark for 508 accessibility. The HSEMA mobile application is also now 508 compliant, allowing our residents with hearing and/or vision impairments the same access to emergency preparedness resources as those without impairments.

Podcast:

In FY18, HSEMA's Office of Public Affairs laid the groundwork to launch the agency's podcast series, now known as HSEMA Off the Record. The podcast, officially launched in 2019 serves as an innovative channel for HSEMA to connect with District residents and visitors and provides a behind the scenes look, and listen, into the District's emergency preparedness efforts. Episodes cover the history of the field and profession, the District's integration of emergency management and intelligence, and how HSEMA staff members use innovation and creativity to meet industry challenges head on.

45. Please identify all electronic databases maintained by your agency, including the following:

a. A detailed description of the information tracked within each system;
b. The age of the system and any discussion of substantial upgrades that have been made or are planned to the system; and
c. Whether the public can be granted access to all or part of each system.

The table below includes information on all electronic databases maintained by HSEMA.

Type	Description	Age	Upgrades	Public (Y/N)
MS SQLServer	Production WebEOC database - Application front end is utilized by district agencies and public agencies	1Yr	Updated in 2019	N

Type	Description	Age	Upgrades	Public (Y/N)
	during events			
MS SQLServer	Database for Citywide closed-circuit television (CCTV) camera system integrated environment	3Yr	2016	N
MS SQLServer	Redundant Database for Citywide CCTV camera system integrated environment	3 Yr.	2016	N
MS SQLServer	Production database for HSEMA Training Tracking system - Application front end available to the public	1 Yr.	2019	Y
MS SQL Server	Redundant Database for WebEOC database application and HSEMA Training	1 yr.	2019	Y
MS SQLServer	Production database for HSEMA Destiny Risk Orientation system - Application front end available to the public	6 Yr.	None	Y
MS SQLServer	Production ManageEngine ServiceDesk - Application front end is utilized by DC HSEMA for Helpdesk ticketing	5 Yr.	None	N
MS SQLServer	Production ManageEngine DesktopCentral - Application front end is utilized by DC HSEMA for Desktop Management	5 Yr.	None	N
MS SQLServer	Doubletake Database - Utilized to replicate data to OCTO DR Environment	2 Yr.	None	N

46. Please provide a detailed description of any new technology acquired in FY19 and FY20, to date, including the cost, where it is used, and what it does. Please explain if there have there been any issues with implementation.

In FY19, HSEMA conducted an agency-wide workstation refresh. During this process the agency procured Dell laptops and workstations. The procurement of the new laptops and workstations allowed the agency to replace outdated equipment and increase the agency's productivity. The cost of the agency-wide laptop refresh was $278,845.08. During the agency-wide refresh, the 24/7 Joint All Hazards Operations Center workstations were replaced, costing the agency $9,594.00. Additionally, the National Capital Region Threat Intelligence Consortium (NTIC) procured new laptops, costing the agency $95,388.98.

Agency Operations

47. How did HSEMA promote awareness among the District's public and private sector partners regarding cybersecurity in FY19 and FY20, to date?

Under the District's Prevention/Protection Program, the Office of the Chief Technology Officer (OCTO) is the lead agency for cybersecurity. As the lead agency, OCTO is responsible for cybersecurity planning, training, and leading any cybersecurity response or initiatives. The upcoming Prevention/Protection training program will involve Cybersecurity training created by OCTO and taught by OCTO for members of the program, with the goal of pushing the training out to District public/private partners.

Information sharing, including cybersecurity information, is part of the HSEMA Business Emergency Management Operation Center (BEMOC), a program that facilitates the interaction between the public and private sectors before, during, and after an emergency. Once they have been approved for dissemination, relevant cybersecurity bulletins and reports are passed along to BEMOC members (businesses and other private sector groups). Information sharing is also a core function of HSEMA's public affairs team. The public affairs team works alongside the National Capital Region Threat Intelligence Consortium's (NTIC) Cyber Center to share unclassified products focused on cybersecurity to the general public. This is accomplished through the use of social media channels (Facebook, Twitter, and LinkedIn) and the ReadyDC Preparedness Bulletin, a monthly newsletter sharing preparedness tips, resources, and news with the community. The NTIC publishes a quarterly newsletter called the School Safety Packet, that provides timely and relevant safety and preparedness information for teachers and administrators, students and parents. Finally, cybersecurity was a featured topic on HSEMA's newly launched podcast, HSEMA Off the Record. One of the two episodes launched in December 2019 focused on the topic of cybersecurity and preparedness during the holiday season.

In addition to this programmatic work, the NTIC's Cyber Center component produced and disseminated a combination of 90 cybersecurity awareness bulletins and threat intelligence products in FY 2019 to vetted private sector partners and government personnel. In December 2018, HSEMA hired two cyber threat intelligence analysts tasked with assisting the Cyber Center manager with the creation of NTIC Cyber Center's product line to provide stakeholders with timely and actionable cyber threat intelligence and analysis. The NTIC Cyber Center is dedicated to making the National Capital Region (NCR) more resilient to cyber-attacks by sharing analyses of current and emerging cyber threats, providing mitigation strategies, promoting the widespread adoption of best practices, and encouraging incident reporting.

The NTIC has established a liaison partnership with OCTO, and a partnership with US DHS Office of Intelligence and Analysis to help coordinate information sharing to protect the District's cyber infrastructure. Increasing its email distribution list by more than 300 new members in FY 2020, the NTIC continues to grow its network and build new relationships with members of both the public and private sectors within the District.

48. How does HSEMA ensure collective situational awareness and coordination among District agencies and federal partners in the area of cybersecurity?

HSEMA, through the National Capital Region Threat Intelligence Consortium (NTIC), works toward ensuring that situational awareness about, and indicators of compromise associated with, cyber threats are shared with OCTO's Security Operations Center (SOC), in conjunction with the national fusion center network, the Department of Homeland Security (USDHS), and the Multi-State Information Sharing Analysis Center (MS-ISAC). Details are included below:

- As the District's fusion center, the NTIC participates in the National Fusion Center Association (NFCA) Cyber Intelligence Network (CIN) to gain collective situational awareness on cyber-related reporting around the nation (among fusion centers) and to help coordinate a cyber-response with federal partners (if needed).
- HSEMA has a memorandum of understanding with the OCTO SOC to share threat information (both unclassified and classified level) and provide a liaison partnership between the two agencies. The MOU was signed in September 2017.
- NTIC analysts are members of the Multi-State Information Sharing Analysis Center (MS-ISAC). The ISAC is designed to share information on cyber threats to State, Local, Tribal, and Territorial (SLTT) entities between SLTT and federal partners.
- NTIC analysts work with US DHS entities, including the National Cybersecurity and Communications Integration Center (NCCIC) and Office of Intelligence and Analysis on cyber-related issues.
- The NTIC produced 90 situational awareness products on cybersecurity over FY 2019, reaching more than 1,500 vetted private and government partners in the District.
- During a cybersecurity event that impacts the District network, HSEMA also provides direct support to OCTO – who serves as the lead response agency – in two key ways. First, HSEMA provides OCTO with a method of alerting District staff of the incident through our Alert Notification platform which, by design, is cloud-hosted apart from the District's network. Second, while OCTO focuses on addressing the direct cyber crisis and restoring IT/network/application, HSEMA will coordinate the response across District agencies to enable continuity of operations and address the cascading impacts of system failures prior to resumption.

a. What protocols are in place for interagency communications regarding cybersecurity?

HSEMA has a memorandum of understanding with OCTO for information sharing and has built relationships with key government entities within the District, regionally, and nationally, to help facilitate communication regarding cybersecurity.

HSEMA is also part of the Smarter DC Tiger Team, a working group of agency representatives that is focused on building a smarter and more connected city using the emerging internet of things and connected device technologies. While cybersecurity is not the focus of the Tiger Team, the group does discuss cybersecurity information.

b. What cyber awareness outreach and training does HSEMA conduct?

When requested, the NTIC provides cyber awareness outreach to private sector partners through previously established relationships, including ones with the District's Business Improvement Districts. Additionally, the NTIC has participated in a newly established podcast called "HSEMA Off the Record" to inform listeners about cyber threats impacting the community.

c. How, specifically, does HSEMA share jurisdiction with OCTO regarding cybersecurity?

In the District, OCTO has sole jurisdiction over cybersecurity planning, preparedness, and response. As the lead for the District's planning and coordination of homeland security and emergency management efforts, HSEMA helps coordinate OCTO's planning and interaction with other District agencies.

In addition, HSEMA, through the NTIC, shares information received through government entities (both at the unclassified and classified levels) with OCTO to help ensure the safety and security of the District's cyber infrastructure. In turn, OCTO shares threat information received with the NTIC for timely notification and to gain assistance through government entities.

49. Please describe the activities of the Homeland Security Commission in FY19 and FY20, to date.

In FY19, the Homeland Security Commission (HSC) welcomed three new Commissioners, Joanna Turner, Brian Baker, and Edward Pearson. In FY19 and FY20, to date, the HSC has held five quarterly meetings. These were held on November 16, 2018; January 17, 2019; March 1, 2019; April 12, 2019; and May 20, 2019. The HSC continues work for the 2019-2020 annual report.

a. In August 2017, the Office of the District of Columbia Auditor hosted an event with past and present Homeland Security Commission members. What, if anything, has the Commission done differently based on this discussion?

Following the event in August 2017, the HSC held quarterly meetings on September 15, 2017 and December 8, 2017. In total, the Commission held 18 meetings between September 2017 and May 2019. The 2017 event hosted by the Office of the District of Columbia Auditor addressed the need to give greater focus to possible threats related to cyber security and waterfront access. The Commission focused on cyber security in its 2018 annual report.

b. How does HSEMA use the Commission's past reports to inform policy and operations?

HSEMA uses the Commission's reports as a resource to inform policy and operations within the agency, particularly through resource allocation, product development, and the identification of gaps within the District's Risk Assessments.

c. What is HSEMA's role in aiding the work of the Commission?

HSEMA provides staff who support the Commission. HSEMA staff aid the work of the Commission through scheduling quarterly meetings and additional fact-finding meetings, per the Commissioners' request and availability. HSEMA staff takes minutes and share those minutes with the Commissioners. In addition, staff engage in stakeholder outreach on behalf of the Commission and provide research, upon request, to support the development of the independent Commission's report.

d. The Commission has not published an annual report since 2015. Why? When can the Committee expect to see the next report? Why has HSEMA failed to approve the Commission's most recent draft report?

The Commission did not meet between December 2, 2015 and September 15, 2017. A contributing factor to this was that the Commission did not have enough members (four) to achieve quorum. As a result, the Commission did not produce a report in 2016 or 2017. In 2018, the Commission had full quorum and they produced a report on cyber security that was completed in 2019.

HSEMA only provides administrative support to the Commission and does not approve or disapprove the work products of the Commission, which is an independent body.

50. Please provide an update on Alert DC.

a. How does the agency track the number of subscribers? How has this number changed over the past two fiscal years?

Currently, HSEMA has 168,877 AlertDC subscribers, which we track through Everbridge, the alerting platform powering AlertDC. In FY19, the number of AlertDC subscribers increased by 14,122. In FY18, AlertDC increased by 14,700 subscribers.

b. How has this program been used to communicate important information?

During FY19, AlertDC was used to push 9,853 alerts to subscribers. Alerts range widely in topic, for example: silver alerts, emergency water outages, traffic advisories, street closures, special event information, hypothermia/cold emergency alerts, and more. As of January 21, 2020, in FY20, AlertDC has generated 492 alerts to subscribers.

c. Has the agency identified any ways to improve upon this program in FY19 and FY20, to date?

In the FY19 Q4 ReadyDC advertisement campaign, AlertDC was the primary call to action. During this time period, AlertDC received more than 3,000 new subscriptions. To help increase the AlertDC profile, it was added as a prominent topic in posts on the agency's social media channels and incorporated into the rotating carousels on the HSEMA and ReadyDC websites.

In Q1 of FY20, HSEMA partnered with EffecTV (previously known as Comcast Spotlight) to launch the agency's first cable television commercial, in which AlertDC was the primary call to action. During the time in which the commercial aired, we received an additional 1,846 subscriptions to the AlertDC service. HSEMA understands the value and importance of residents signing up for this service and has pledged to execute one advertisement campaign each quarter of FY20. In previous fiscal years, the agency has only executed one to two campaigns per fiscal year. We are in the planning process now for our Q2 campaign of FY20 and hope it will launch in mid-February.

Additionally, HSEMA's Office of Public Affairs and Operations Division are gathering subscriber feedback and putting together a plan to implement infrastructure changes with the intention of increasing user experience during the registration process and with the platform as a whole.

51. Please provide a list of all major special events that HSEMA monitored in FY19 and FY20, to date.

a. Please describe how the agency responded to each event.

Below is a list of major special events as of January 3, 2020.

Date	Event	Response Overview
Oct 13, 2018	H Street Festival	HSEMA deployed the Mobile Command Center and facilitated operational coordination among the event organizer and public safety departments/agencies including MPD, FEMS, DPW, and DDOT.
Dec 3-5, 2018	George H.W. Bush State Funeral	HSEMA activated the EOC (full activation), providing coordination and support to the Federal unified command and supporting entities.
Jan 21, 2019	Martin Luther King Jr Parade	HSEMA deployed ELOs to work in the Unified Command Center.
Feb 5, 2019	2019 State of the Union Address	HSEMA administered an Emergency Operations Center (EOC) full activation, providing coordination and support to the Federal unified command and supporting entities.
Mar. 9th, 2019	Rock and Roll Marathon	HSEMA deployed the Mobile Command Center and facilitated operational coordination among the event organizer and public safety departments/agencies including MPD, FEMS, DPW, and DDOT.
Apr. 13th, 2019	National Cherry Blossom Festival Parade	HSEMA deployed two Mobile Field Teams and facilitated operational coordination with the event organizer. Coordination with public safety departments/agencies including MPD, FEMS, DPW, and DDOT, went through the Mobile Command Bus which monitored three events.
Apr.13th, 2019	D.C. Emancipation Day Parade and Festival	HSEMA deployed the Mobile Command Center and facilitated operational coordination among the event organizer and public safety departments/agencies including MPD, FEMS, DPW, and DDOT.
Apr.13th, 2019	Sakura Matsuri-Japanese Street Festival	HSEMA deployed one Mobile Field Team to facilitate operational coordination with the event organizer. Coordination with public safety departments/agencies including DCRA, MPD, FEMS, DPW, and DDOT, went through the Mobile Command Bus which monitored three events.

Date	Event	Response Overview
May 11th, 2019	DC Funk Parade	HSEMA deployed two Mobile Field Teams to facilitate operational coordination with the event organizer. Coordination with public safety departments/agencies including DCRA, MPD, FEMS, DPW, and DDOT, went through Unified Command, set up at the DPW Snow Center in the Reeves Building.
May 13th, 2019	29th Annual NLEOMF Candlelight Vigil (USPP)	HSEMA deployed the Mobile Command Center and facilitated operational coordination with public safety departments/agencies including USPP, FEMS, DPW, and DDOT.
May 18th, 2019	2019 DC Bike Ride	HSEMA deployed two Mobile Field Teams and facilitated operational coordination among the event organizer and public safety departments/agencies including MPD, FEMS, DPW, and DDOT.
May 25th, 2019	United House of Prayer Memorial Day March	HSEMA deployed the Mobile Command Center and facilitated operational coordination with public safety departments/agencies including MPD, FEMS, DPW, and DDOT.
May 26th, 2019	Rolling Thunder	HSEMA deployed two Mobile Field Teams and coordination for the event went through the Joint All-Hazards Operation Center (JAHOC).
May 27th, 2019	National Memorial Day Parade	HSEMA deployed the Mobile Command Center and facilitated operational coordination with public safety departments/agencies including MPD, FEMS, DPW, and DDOT.
June 8th, 2019	Capital Pride Celebration Parade	HSEMA deployed the Mobile Command Center and facilitated operational coordination with public safety departments/agencies including USPP, FEMS, DPW, and DDOT.
June 9th, 2019	Capital Pride Celebration Festival	HSEMA deployed the Mobile Command Center and facilitated operational coordination with public safety departments/agencies including DCRA, MPD, FEMS, DPW, and DDOT.
June 22nd - 23rd 2019	National Capitol Barbecue Battle	HSEMA deployed the Mobile Command Center and facilitated operational coordination with public safety departments/agencies including DCRA, MPD, FEMS, DPW, and DDOT.

Date	Event	Response Overview
July 4th, 2019	July 4th Celebration	HSEMA deployed the Mobile Command Center and facilitated operational coordination with public safety departments/agencies including DCRA, MPD, FEMS, DPW, and DDOT.
July 4th, 2019	Independence Day Parade	HSEMA deployed two Mobile Field Teams and facilitated operational coordination with the event organizer. Coordination with public safety departments/agencies including MPD, FEMS, DPW, and DDOT, went through the Mobile Command Bus which monitored three events.
July 4th, 2019	Palisades Parade	HSEMA deployed two Mobile Field Teams and facilitated operational coordination with the event organizer. Coordination with public safety departments/agencies including MPD, FEMS, DPW, and DDOT, went through the Mobile Command Bus which monitored two events.
Sept. 7th, 2019	More Than Pink Walk	HSEMA deployed the Mobile Command Center and facilitated operational coordination with public safety departments/agencies including MPD, FEMS, DPW, and DDOT.
Sept. 8th, 2019	Adams Morgan Day Parade	HSEMA deployed the Mobile Command Center and facilitated operational coordination with public safety departments/agencies including MPD, FEMS, DPW, and DDOT.
Sept 21, 2019	H Street Festival	HSEMA deployed the Mobile Command Center and facilitated operational coordination among the event organizer and public safety departments/agencies including MPD, FEMS, DPW, and DDOT.
Sept. 21st, 2019	Fiesta DC Parade	HSEMA deployed a Mobile Field Teams and facilitated operational coordination with the event organizer. Coordination with public safety departments/agencies including MPD, FEMS, DPW, and DDOT, went through the Mobile Command Bus which monitored two events.
Sept. 22nd, 2019	Fiesta DC Festival	HSEMA deployed the Mobile Command Center and facilitated operational coordination with public safety departments/agencies including DCRA, MPD, FEMS, DPW, and DDOT.

Date	Event	Response Overview
Sept. 29th, 2019	Preparedness Day at Nationals Park	HSEMA deployed the Mobile Command Center to showcase some of the Agency's capabilities and provide preparedness tips to those at and around the ballpark.
Oct 5, 2019	DC Open Streets	HSEMA deployed the Mobile Command Center and facilitated operational coordination among the event organizer and public safety departments/agencies including MPD, FEMS, DPW, and DDOT.
Oct. 13th, 2019	Army Ten Miler	HSEMA facilitated operational coordination from the Joint All-Hazard Operation Center.
Oct 25-Oct 27, 2019	MLB World Series Games	HSEMA activated the EOC (full activation), providing coordination and support to the Federal unified command and supporting entities. The Mobile Command bus was deployed for all home games.
Oct. 27th, 2019	Marine Corp Marathon	HSEMA facilitated operational coordination from the Joint All-Hazard Operation Center.
Nov 2, 2019	MLB World Series Parade	HSEMA administered an Emergency Operations Center (EOC) full activation, providing coordination and support to the Federal unified command and supporting entities. HSEMA deployed the Mobile Command Center and facilitated operational coordination with public safety departments/agencies including DCRA, MPD, FEMS, DPW, and DDOT.

52. How did HSEMA improve its engagement with the Council in FY19 and FY20, to date?

Providing accurate and timely answers to inquiries from Council is a top priority for HSEMA. Several members of the HSEMA staff are tasked with tracking Council actions and responding to requests from Councilmembers. In addition, Councilmembers are encouraged to sign up for AlertDC to receive timely notifications about activities throughout the city. Further, the agency continues to work closely with the Mayor's Office of Policy and Legislative Affairs (OPLA) on any outstanding concerns from Council.

a. In an emergency situation, what is the formal protocol for notifying members of the Council about HSEMA's response plans?

HSEMA encourages all Councilmembers to sign up for AlertDC to customize the alerts that they receive on a daily basis. In addition, during larger scale emergencies that include level 2 or higher activation of the Emergency Operations Center, the Joint Information Center's (JIC) Legislative Affairs Unit is responsible for communicating with Council. During multi-day activations, the JIC hosts a daily call for Councilmembers and staff to update them on the District's response.

b. How can HSEMA and the Council work together to help keep constituents informed and apprised of important information?

HSEMA encourages the Council to promote AlertDC (alertdc.dc.gov), the District's emergency communications system, to constituents. We would also encourage Council to promote ReadyDC (ready.dc.gov), the District's personal preparedness campaign, in its constituent communications and urge residents to sign up for the ReadyDC Preparedness Bulletin (ready.dc.gov/bulletin). The Preparedness Bulletin is an electronic newsletter that shares preparedness news, resources, trainings, and tip with the community. ReadyDC asks residents to become a preparedness partner by being aware, making a plan, building a kit, and staying informed. Finally, Council is also encouraged to contact members(s) of HSEMA's community outreach team for presentations on emergency preparedness and printed preparedness resources by visiting hsema.dc.gov/communityoutreach.

In FY19, HSEMA worked with Councilmembers to modify the language of AlertDC messages based on feedback Council received from constituents. We continue to welcome the feedback of Councilmembers and their constituents to ensure that emergency messages and alerts are clear and actionable.

53. Please describe what the agency has done in FY19 and FY20, to date, to engage the public in emergency preparedness.

Engaging with residents, businesses, and visitors is the main responsibility of HSEMA's community outreach team and the Office of Public Affairs. In FY19, the community outreach team conducted multiple events promoting ReadyDC. During these events, outreach specialists shared the importance of building a kit, making a plan, being aware, and staying informed. Events ranged from tabling events at senior centers to interactive trainings with MPD/FEMS. September is National Preparedness Month. To kick off the month, HSEMA re-launched the updated ReadyDC website, providing the public with updated and improved emergency preparedness tips and a page dedicated to downloadable resources to help individuals better prepare. HSEMA also tried new approaches to engaging with the public, including hosting preparedness day events in partnership with the sports teams in the District. HSEMA's

outreach team attended DC United and Washington Wizards games to engage with fans, share preparedness tips, and provide free resources. On September 29, HSEMA sponsored the District's first Preparedness Day at Nationals Park to coincide with the team's last home game of the season. HSEMA had more than 50 staff members stationed at tables and walkways throughout the park to engage with fans, share preparedness materials, and encourage them to sign up for AlertDC. The agency also created a 30-second public service announcement video, which aired on the jumbotron during the home game to share the importance of personal preparedness with fans. The PSA also aired on the jumbotron at the DC United Game.

In FY19, the Office of Public Affairs was responsible for digital outreach, education, and preparation of residents. Social media outreach included daily posts providing emergency preparedness tips and resources. In FY19, HSEMA partnered with FEMA Region 3's Office to host a winter preparedness chat that provided an opportunity for HSEMA and local, regional, and federal partners to provide resources and begin the conversation about personal and winter preparedness. Through HSEMA's Twitter account alone, we had more than 3.5 million impressions; meaning our preparedness content was viewed more than 3.5 million times.

The Office of Public Affairs has also implemented new and innovative methods to share the District's message of preparedness. In FY19, HSEMA began planning for the launch of the agency's podcast, HSEMA Off the Record. The podcast provides insight into the District's emergency management efforts in a method which continues to increase in popularity. There have been 6 episodes to date.

54. How does HSEMA ensure collective situational awareness and coordination among District agencies and District residents in the event of a mass emergency?

a. How has HSEMA changed its operations or coordination with relevant public and private entities following the Capper Fire? How has HSEMA used its "lessons learned" from that event to inform agency operations?

In the wake of the Capper Fire and other smaller residential fires that resulted in displacements, HSEMA convened a working group, co-chaired with DMHHS and DHS, that included American Red Cross (ARC), OTA, DCHealth, DHCF, DCRA, FEMS, DPR, MOCRS, and DCHA. There are three principal outcomes of the working group to-date. First, HSEMA has established a new alert notification group in the HSEMA Alerts system that notifies all of these agencies that a residential fire has generated displacements, regardless of the level of required response. This allows each agency to begin preparations and expedites their activation even before that agency is required to respond. This shortens the lead time for an agency to provide services once we determine that they need to be involved.

Second, HSEMA and DHS have developed a common workflow for all residential displacements, regardless of cause. This means that we can apply a common approach to every incident based on the complexity of the incident and the volume of displacements. Most importantly, this work flow involves establishing coordination calls across the supporting agencies even before all of the agencies are

required at an incident scene. This allows HSEMA to ensure that there is a common operating picture during the immediate response and that there is, by default, a follow-up call the next day to continue to evaluate the need for services to the residents in the following days.

HSEMA is also working with DFHV to identify additional options to provide accessible transportation to people who need to move from an impacted building to a hotel or other location. Currently, DPR and OSSE DOT can provide support, but we believe that a needs-based, on-demand solution for individuals and families would be a strong addition to our resources to support the community.

Finally, following the Capper Fire, HSEMA purchased and took delivery of a second mobile command vehicle so that we can coordinate operations during multiple events or when one vehicle is out of service for routine maintenance. This closed a major after-action item from the Capper Fire.

b. Has HSEMA conducted any tabletop exercises or drills to practice how to respond to future large-scale events? If so, please explain.

This year, HSEMA focused on convening our District executives during a series of intense tabletop exercises facilitated by the Naval Postgraduate Institute. The exercises focused on how the District's consequence management team, led by the CA and DMPSJ, would convene and coordinate the District's response to a coordinated attack on the District at multiple locations. This type of scenario would challenge the District because it would cause confusion in the community, pull our emergency responders in different directions at the same time, and drive extensive community and media interest. At the conclusion of the initial exercise – which focused on assessing the situation and implementing the initial response to the various incidents – the CA requested a follow-up exercise to extend the scenario into the recovery phase which HSEMA and the Naval Postgraduate Institute hosted in November 2019. HSEMA is working with the Naval Postgraduate Institute to return again for an additional exercise in this series in November 2020.

c. In FY19 and FY20, to date, has HSEMA changed any internal policies on how it responds to large-scale events? Specifically, with regard to its responses to vulnerable populations, such as seniors or individuals with disabilities? If so, please outline these changes.

Overall, HSEMA has made significant changes to our operations to allow us to better support the community and our partners during large-scale events. We have revised our training for EOC staff to align with FEMA guidance to make our EOC more effective and we have conducted quarterly training for HSEMA and partner agencies to enhance our response readiness. We have increased the capacity to deploy HSEMA staff to support our partners and residents so that we can stay engaged as a member of or lead the incident management team in the days following an event to ensure that we support every resident that needs District support. Finally, as we do our routine plan updates, we have begun to focus more

on leaner more operationally-focused planning tools that our stakeholders can utilize, and we have received positive feedback to date on those changes.

Specifically, for supporting people with disabilities and others with access and functional needs, HSEMA continues to identify and train agency staff that will serve in key roles supporting people with disabilities and functional and access needs (DAFN) in the EOC and also as part of a unified command at the incident site. We have a DAFN officer position on each EOC team.

d. Does HSEMA have special emergency response procedures for individuals who are deaf and hard of hearing in the event of a mass emergency?

Alert DC can provide people who are deaf or hard of hearing with a text-based method to receive alert messages on their phones and the Wireless Emergency Alert system allows HSEMA to actively push emergency messages to cell phones. Specific to deaf and hard of hearing residents who require emergency sheltering, HSEMA works with OTA to leverage OTA's relationship with area hotels – most commonly the hotel at Gallaudet University – which is part of a signing community. We recently did this for a deaf resident following a fire on Martin Luther King Jr Ave SE. During that fire, we also assigned a JAHOC team member at the scene to work directly with that resident to help him with navigating our services and to help coordinate with FEMS to help him access his apartment to find his missing cell phone so that he had a means to communicate with his case manager.

55. Please describe the structure, membership, and responsibilities associated with the Mayor's Special Events Task Group ("MSETG").

As the nation's capital, Washington, D.C. hosts numerous special events requiring essential municipal services to ensure events occurring on public roadways in the District are conducted in a manner that protects public health and safety. Coordinating the city's interagency public safety planning efforts is the responsibility of the Mayor's Special Events Task Group (MSETG). The MSETG's structure is based on the functional areas of responsibilities listed below in support of the city's two special event licensing and permitting agencies (i.e., MPD for processional events and DCRA for stationary events).

Functional Area(s) of Responsibility	Lead Agency(ies)
Security	Metropolitan Police Department
Transportation, Public Space, and Public Works	Department of Transportation *and* Department of Public Works
Licensing, Permitting, and Inspections	Department of Consumer and Regulatory Affairs

Health and Medical	Department of Health *and* Fire and Emergency Medical Services Department
Unified Command and Communications	Homeland Security and Emergency Management Agency

In order to ensure effective deliberation and working representation of agencies with primary and supporting functions, the MSETG's membership includes the following:

MSETG Membership	
Homeland Security and Emergency Management Agency	Department of Consumer and Regulatory Affairs
Department of Fire and Emergency Medical Services	Alcoholic Beverage Regulation Administration
Metropolitan Police Department	Office of Risk Management
District Department of Transportation	Department of Health
Executive Office of the Mayor	Department of Public Works
DC Water	Office of Tax and Revenue
National Park Service	Department of Parks and Recreation
Washington Metropolitan Area Transit Authority	Office of Cable Television, Film, Music, and Entertainment
Events DC	Smithsonian Institute
U.S. Park Police	U.S. Capitol Police
U.S. Department of Homeland Security – Federal Protective Service	Department of General Services Protective Services Division
National Gallery of Art	Department of Energy and Environment

a. Please describe the work of the MSETG in FY19 and FY20, to date, including any changes to its reporting structure within the Executive branch, membership, operations, policies, procedures, and member agency fees.

The MSETG held semi-monthly meetings during FY19 and FY20, to date, for the purpose of providing interagency reviews and assessments of the operational, public safety, and logistical components of proposals for special events occurring on public roadways under the jurisdiction of the District of Columbia. The Meeting Activity Report (attachment "Q55a HSEMA part 1") provides a list of the event proposals reviewed and assessed by the MSETG for production during FY19 and FY20 Q1. The MSETG's reporting structure within the Executive Branch remains under the Executive Office of the

Mayor (via the Mayor's Office of Community Affairs). There were no changes to the MSETG's membership, operations, or procedures. The infographic of the MSETG's interagency coordination (attachment "Q55a HSEMA Part 2") provides an overview of the steps involved in the processing of special event proposals. Information relative to agency-specific requirements and fees is provided in the MSETG Special Events Planning Guides (attachments "Q55a HSEMA Part 3" for 2019 and "Q55a HSEMA Part 4" for 2020).

The special event user fees as determined by each respective agency incurring costs associated with the production of special events are provided in the MSETG Planning Guide beginning on page 32.

b. Please describe the reason for any fee increases in FY19 and FY20, to date (<u>if necessary to answer the question, consult with agency partners</u>).

The MSETG does not have a role in the determination or the assessment of agency-specific special event user fees. MPD, however, reported a 3 percent fee increase in both FY19 and FY20 in accordance with 24 DCMR § 720.

c. Is the fee structure standard, or does it change based on the size and scale of the event?

The special event fees are standard. The agencies' special event user fees are based on a level of cost-recovery and therefore do not vary based on the size or scale of an event. The agencies' application of cost-recovery fees is based on the direct provision of services and imposed under a fee-for-service structure.

d. Does HSEMA consider whether the fees assessed burden small-scale District special event organizers? How does HSEMA defray costs?

HSEMA does not make assessments of the impact of agencies' application of their respective cost-recovery special event user fees on any special event organizers. These fees are assessed in accordance with 24 DCMR § 720. HSEMA has been delegated the administration of the Community Events Fund (established by EOM) for the exclusive purpose of offsetting some of the costs for conducting events that are not produced for profit or gain through direct reimbursement to city agencies providing public services that are required for all events and necessary to protect public health and safety.

e. What did HSEMA budget for its Community Events Fund in FY19? FY20? How many special events were funded from the Fund, which, and in what amounts? What is the Fund balance? How many of those events were small fundraising events that benefit a District agency?

The FY19 budget for the Community Events Fund was $120,000. The amounts identified below were allocated for the following events through direct reimbursement to agencies:

Event	Amount
Anacostia River Festival	$1,854.32
Funk Parade	$22,327.04
17th Street Festival	$3,009.33
Adams Morgan Day	$3,159.22
Barracks Row Fall Festival	$3,205.34
Capital Pride Celebration	$26,135.11
Fiesta DC	$22,415.60
Celebrate Petworth	$2,093.34
H Street Festival	$35,554.09
Total	$120,000.00
Balance	$0

The FY20 budget for the Community Events Fund is $120,000. There have been no funds allocated to date for FY20.

How many of those events were small fundraising events that benefit a District agency?

None. The delegation of authority to HSEMA for the administration of the Community Events Fund established by the Executive Office of the Mayor authorizes the defraying of costs for an event in the District of Columbia that is held during a planned time of public celebration marked by special observance, or that features a program or other activity of cultural, historical, or neighborhood significance that is "not being conducted for profit or gain." Fundraising events, by their very nature, are events conducted for gain.

f. Does the MSETG publish hearing agendas in advance of the day of the hearing? If not, why not?

The MSETG provides meeting agendas to MSETG member agencies and event organizers scheduled for presentations in advance of the day of the meeting.

g. Does the MSETG require event organizers to submit after-action reports once their event is complete? How is an organizer's performance taken into consideration in a subsequent application?

The MSETG encourages event organizers to submit after-action reports subsequent to the production of their events. The submission of an after-action report is used as a method of documenting key successes and determining areas of improvement for future planned productions of events.

When there are issues or problems identified in an after-action report or during an event, event organizers are required to participate in after-action meetings with the MSETG to establish action items and implement measures that will specifically address identified deficiencies prior to the MSETG's consideration of the event for approval in a subsequent year.

h. What new requirements did the MSETG or its member agencies impose upon event organizers in FY19 and FY20, to date, related to homeland security concerns (e.g. sandbags, placement of vehicles to block access)? What evidence supported these requirements?

No new requirements have been imposed by MSETG or its member agencies in FY19 and FY20.

i. What are the policies and procedures for requiring event organizers to tow vehicles in event spaces?

MPD imposed the implementation of the "Clear Route" initiative in FY18 requiring event organizers to secure the towing services of DPW to support enforcement of the policy. As the agency responsible for enforcing policies and procedures related to vehicle towing, DPW would be the appropriate agency to detail the requirements for event organizers.

j. How did HSEMA determine what type of ambulances and first aid is required at special events? How is this determination standardized across events?

HSEMA does not determine medical asset requirements. The Health Emergency Preparedness and Response Administration (HEPRA) of DC Health is responsible for the determination of medical asset requirements for special events.

k. What is the fund balance of the Public Space Security Assistance Fund in the Mayor's Office of Community Affairs? <u>If necessary, consult with that office.</u>

The Mayor's Office of Community Affairs has advised there is a zero balance as of September 30, 2019 in the Public Space Security Assistance Fund.

56. How has HSEMA adapted its operations to account for increased development in waterfront areas and increased use of the water itself? Does HSEMA play a coordinating role for other District government agencies on waterfront issues? If not, why not?

HSEMA has made an effort to create a strong working relationship with the security staff and businesses in the District Wharf. On October 2, 2017, HSEMA hosted the District Wharf Grand Opening Table Top Exercise (TTX). The Exercise partnered senior Wharf security and public safety officials with counterparts representing the District and Federal departments and agencies who fulfill primary emergency support function roles. The gathering facilitated discussion on emergency and disaster response authorities, policy, and procedure and associated considerations such as site features and evacuation protocol. Wharf officials were also provided a tour of the JAHOC to help them understand the District's 24/7 operational coordination and communications capabilities. Ultimately, the event forged relationships amongst critical stakeholders that will facilitate quick and coordinated responses to emergencies or hazards.

In addition, as the lead agency in the District for alerting and warning, HSEMA closely monitors the flooding hazards associated with the Potomac and Anacostia Rivers. Through AlertDC notifications, we incorporate flood watches and warnings to both internal and external partners and to the community with timing and estimates of the flooding and protective measures, when appropriate. Through our public-private partnerships program, we maintain strong relationships with the Georgetown BID and the District Wharf security team and we communicate directly with these partners when we expect to see significant flooding. This allows those properties to implement protective measures like the Georgetown BID's privately managed floodwall.

Nationally, HSEMA is a member of Silverjackets supported by United States Army Corps of Engineers (USACE). Silverjacket teams bring together multiple states, federal, and sometimes tribal and local agencies to learn from one another in reducing flood risk and other natural disasters. Shared knowledge is used to enhance response and recovery efforts when such events do occur. HSEMA LTRR Mitigation collaborated with Silverjackets with the DC Levee Outreach, flood risk management planning, and Watts Branch flood risk study. The DC Wharf is working with HSEMA to conduct a Preparedness TTX/Workshop in February for their businesses.

The NTIC is actively engaged with the security teams of various waterfront entities to assure that relevant homeland security-related information and support are provided in a timely manner. Due the sensitive nature of these security arrangements, we are not permitted to publish in an unclassified document the names of the entities nor specifics of the nature of support that the NTIC provides.

57. In June 2017, the Office of the Inspector General audited HSEMA's management of Continuity of Operations Planning. Please discuss any changes the agency made based on the report's recommendations.

In 2017, HSEMA went through an Office of the Inspector General Audit of the Continuity of Operations Planning Program. The report, OIG Project Number, 16-1- 10BN was completed in June 2017. The report made two recommendations for HSEMA to follow, in order to meet the mission of Mayoral Order 2012-61. The recommendations are listed below:

1. Provide a more comprehensive annual report to the Deputy Mayor for Public Safety and Justice that includes information and metrics on the status of agencies' COOP planning and performance.

   Response: As of January 28, 2019, 82 percent of Tier 1 agencies, 57 percent of Tier 2 agencies and 75 percent of Tier 3 agencies are in full compliance with Mayoral Order 2012-61 for calendar year 2019.

2. Develop and implement policies and procedures to fulfill the requirements of the Mayor's Order that include reviewing all COOP plans and AARs; providing COOP assistance and guidance; and establishing an outreach process with accurate contact information to communicate with all pertinent agencies.

   Response: HSEMA developed a series of outreach methods for District agencies to learn about the importance of the COOP plan, how to effectively plan, update, and review, as well as exercise their individual plans.

   HSEMA developed a COOP Toolkit that was designed to assist agencies with building, updating, reviewing, and exercising their plans. The COOP toolkit is reviewed at all COOP training and includes a "welcome packet" explaining how to use the toolkit and some additional tips, tricks, and best practices.

   HSEMA held four half-day COOP Workshops. These events were designed with a dual purpose: coordinators were educated on the importance of COOP, the COOP toolkit, and HSEEP.

   HSEMA hosted a symposium in May 2019 with a COOP track to assist coordinators with understanding the importance of COOP training. Agencies were invited to request a personalized tabletop exercise. From these requests, six separate breakout sessions were scheduled. Five were agency specific and one was a general session during the symposium.

   These events were designed with four primary goals:

   1. To serve as a workshop, educating coordinators on the importance of maintaining their agency's COOP capabilities
   2. To guide coordinators in the evaluation of their COOP plans
   3. To educate agencies on how to utilize FEMA's Homeland Security Exercise and Evaluation Program (HSEEP) as the national best practice for designing and conducting exercises
   4. To provide a tabletop exercise (TTX), at which COOP coordinators were given the opportunity to test their COOP plans against a winter weather emergency scenario

Over the course of 2019, HSEMA conducted 10 workshops with roughly 92 participants from 36 agencies.

a. Is HSEMA fully compliant with Mayor's Order 2012-61?

Yes, HSEMA is fully compliant with Mayor's Order 2012-61. Additionally, on January 10, 2020, the Office of Inspector General notified HSEMA that we have sufficiently closed the open recommendations.

b. How does HSEMA work with individual District agencies to ensure they develop a Continuity of Operations Plan ("COOP")?

HSEMA works with agencies in a multitude of ways to ensure they develop a COOP program that complies with both District standards and federal best practices. This includes, but is not limited to, the following: COOP plan section-by-section document review, facilitation of training seminars to agency staff, facilitation of collaborative workshops, facilitation and evaluation of discussion-based Tabletop Exercises, facilitation and evaluation of operations-based exercises, and development of After Action Reports and Improvement Plans. All of the aforementioned services are specifically tailored to meet the unique needs of a particular agency. In addition, HSEMA socializes its comprehensive COOP services via direct email to agency COOP coordinators as well as presentations at Mayoral Cabinet meetings, Risk Council meetings, and Emergency Preparedness Council meetings.

c. Please provide a chart of District agencies, noting whether they have been fully COOP compliant in FY19 and FY20, to date.

Please see pages 3-6 in attachment "Q57 HSEMA" for a chart of District Agencies and the status of their COOP compliance in FY19 and FY20 (current through January 15, 2020).

d. Please provide a copy of the most recent COOP annual report that HSEMA produced.

Please see attachment "Q57 HSEMA".

58. How does HSEMA support religious institutions with security and preparedness?

HSEMA, along with the Metropolitan Police Department and Mayor's Office of Religious Affairs, supports the District's religious institutions through the Interfaith Preparedness & Advisory Group (IPAG). In FY19, the IPAG convened faith leaders from across the country who have lived through mass violence at their places of worship for the group's second quarterly meeting. The meeting was held at the Washington National Cathedral for a group

discussion involving District of Columbia public safety officials and members of the District's faith-based community. The goal of the meeting was to learn from the faith leaders who have experienced such violence first-hand so that we can better help the faith community here in the nation's capital become safer, stronger and more resilient.

At HSEMA, the IPAG's activities are managed by the National Capital Region Threat Intelligence Consortium (NTIC). HSEMA facilitates the production of content for quarterly meetings and shares and disseminates information relevant to the safety of faith-based communities. HSEMA, through the IPAG, supports religious institutions by providing:

Security Grant Funding

- The IPAG provides a platform for HSEMA to engage faith based organizations (FBOs) on procedures to apply for FEMA's Nonprofit Security Grants and other federal funding. HSEMA serves as the recipient and pass-through entity for the Nonprofit Security Grant Program (NSGP) for the National Capital Region. HSEMA distributed information to prospective applicants through email, training webinars and meetings in the community, including leveraging the IPAG to enhance outreach efforts. These funds are distributed annually to NCR FBOs to build resilience and emergency preparedness. HSEMA collects applications, submits them to FEMA, receives the federal award, and issues subawards to the selected nonprofits. HSEMA grant program management staff also support NSGP subrecipients in compliance with federal regulations.

Analytic Support

- HSEMA staff fields and supports all analytic requests from the IPAG and produces products to promote and encourage two-way communication with faith-based communities. Most products will be produced in response to incidents, but our Preparedness Division also includes general threat briefs to build security consciousness.

Training and Preparedness workshops

- The IPAG offers trainings through its quarterly meetings for the faith community on Suspicious Activity Reporting (SARs) training at each meeting, along with specialized trainings that focus on current threats.

Intelligence Briefings

- The IPAG meets with senior District leadership on a quarterly basis and convenes ad hoc meetings to address specific threats, meetings either initiated by the NTIC or at the IPAG's request. HSEMA drafts, as needed, security and threat talking points for the HSEMA Director and facilitates these meetings/teleconferences with the Office of Public Affairs.

Cyber Security

- The NTIC monitors current and emerging cyber threats impacting FBOs and produce timely and actionable intelligence to help faith-based communities mitigate risk. Additionally, HSP provides training opportunities and exercises designed to strengthen and improve their overall cybersecurity posture.

a. Are security and preparedness grants available for District non-profit organizations operating at faith-affiliated institutions available on an ongoing basis?

The DHS/FEMA Nonprofit Security Grant Program (NSGP) is available annually for nonprofit entities within the National Capital Region at risk of terrorist attack. In FY2019, 132 applications were received, and 47 applicants were selected by FEMA to receive awards. Congress has appropriated $50M for the FY2020 NSGP but the application period has not yet started.

b. What types of improvements have already been made by HSEMA grantees?

Recipients of NSGP grant funds are approved for a variety of different physical security enhancement projects, including upgrades to doors and windows, alarm systems, video monitoring systems, barricades, lighting, alert and warning systems, and contracted security personnel. Most FY2019 NSGP awards are still going through FEMA's environmental and historic preservation review process and haven't started expending funds.

Q 27 HSEMA

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

January 17, 2019

National Capital Region Cyber Threat Spotlight

The NTIC Cyber Center regularly observes stolen login credentials shared on publicly available websites, so we wanted to remind our partners in the National Capital Region (NCR) about the importance of securing online accounts with two-factor authentication (2FA). Although creating lengthy and complex passwords is important for cybersecurity, they can no longer be viewed as the most effective security solution. Malicious actors can easily obtain stolen email addresses and passwords via data breaches, malware infections, phishing attacks, and on dark web marketplaces and use them to hijack accounts and commit fraud. To combat the threat of stolen credentials, many online accounts offer 2FA as an added security measure. Accounts with 2FA require information in addition to a username and password before a user is granted access. 2FA is available in several forms:

- a hardware authentication device such as a specially-designed USB key
- a mobile application that generates a time-based one-time code such as Google Authenticator
- a text message containing a link or a code for verification sent to a mobile phone

Online accounts that have 2FA enabled are far less likely to be compromised through the use of stolen passwords. ***To add this extra level of security, the NTIC Cyber Center encourages all users to enable this feature on every account that offers it.***

Current and Emerging Cyber Threats

New Ransomware Campaign Includes PayPal Phishing Scheme

Security researchers recently discovered a new two-part ransomware campaign that includes both a file encryption process and a phishing attempt designed to capture victims' PayPal login credentials and personal information. After the ransomware infects a system, it displays a ransom note advertising decryption services payable via Bitcoin or PayPal. The "Buy Now" button included on the note redirects victims to a phishing site masquerading as the legitimate PayPal landing page prompting victims to enter their name, payment card information, date of birth, address, telephone number, and PayPal login credentials. ***The NTIC Cyber Center would like to remind our members that ransomware continues to pose a high risk to both individuals and organizations. We strongly recommend backing up data regularly and keeping all devices and software updated with the latest patches. In addition, refrain from opening email attachments or clicking on links sent by unknown or suspicious sources.***

Business Email Compromise Scam Targets Employee Paychecks

Security firm Agari reports observing an increase in business email compromise, also known as a BEC scam, targeting payroll departments and designed to divert employees' paychecks to unauthorized accounts. In these scams, the attacker obtains an employee's name and identifies a contact within the targeted organization's human resources or payroll department using various social engineering and online reconnaissance methods. Spoofing the employee's email address, he sends an email to the payroll contact requesting a change to the employee's direct deposit account. Absent security protocols within the organization to prevent this type of attack, the employee and organization would likely suffer financial losses. ***The NTIC Cyber Center recommends all organizations review their payroll update procedures to ensure that employees are properly verified before any changes are made to personal or account information.***

Data Breach Alert

Hanover County Residents Impacted by Click2Gov Breach

Officials in Hanover County, Virginia issued a warning to residents about a data breach that recently impacted the county's Click2Gov online portal. Residents who used this portal between August 1, 2018 and January 9, 2019 to pay utility bills and building inspection fees likely had their names and payment card information compromised. It is important to note that this is not the first time that attackers breached Click2Gov payment processing systems. According to a December 2018 report by Gemini Advisory, the first publicly reported Click2Gov breach occurred in California in 2017.

The report indicated there have been 46 confirmed compromised US locations and one Canadian location totaling 294,929 stolen payment records. ***The NTIC Cyber Center advises all impacted residents to monitor their bank and credit card statements closely and immediately report any unauthorized activity to their financial institutions. As this appears to be an active and ongoing criminal campaign, we recommend those who currently use a Click2Gov payment system, regardless of location, consider using an alternate bill payment method such as a check, money order, or a single-use prepaid debit card to protect personal accounts from compromise. Furthermore, all NCR jurisdictions employing a Click2Gov payment system are encouraged to contact the vendor for guidance and update their software to the latest version.***

OXO International Customer Data Compromised in Breach

OXO International, a US-based home goods manufacturer, released a data breach notice warning customers about a cybersecurity incident that may have exposed personal and sensitive information. Shoppers who ordered from the company's e-commerce website on the dates listed in the notice may have had their names, addresses, and credit card information compromised in an attack that exploited website vulnerabilities. ***The NTIC Cyber Center recommends affected consumers apply for the free credit monitoring service offered by OXO, monitor bank and credit card statements closely, and immediately report any unauthorized activity to their financial institutions. Victims of this or other data breaches are encouraged to visit the Federal Trade Commission's online identity theft resource page and consider placing a fraud alert or security freeze on their credit file.***

Nearly 773 Million Compromised Login Credentials Discovered

Last week, Troy Hunt, a security researcher and owner of the Have I Been Pwned website, discovered a collection of 2.7 billion records containing nearly 773 million unique email addresses and associated passwords in a massive data breach he labeled "Collection #1." He found the compromised credentials after several sources directed him to a popular online hacking forum and the cloud service hosting the nearly 87 GB of breached data. After obtaining and analyzing the collection, Hunt notified victims who subscribe to his email alerts that their credentials had been compromised and provided guidance on securing affected accounts. ***The NTIC Cyber Center strongly recommends using 2FA to secure every account that offers it and discourages using the same password for multiple accounts.***

Upcoming Webinar - A Conversation with Norman Marks

Norman Marks is a CPA, a certified risk manager, an author, and an evangelist for "better run business," focusing on corporate governance, risk management, internal audit, enterprise performance, and the value of information. He will participate in a webinar and live chat on Tuesday, January 22, 2019 at 2:00pm EST and discuss his personal experiences, his forecast of the future of Governance, Risk, and Compliance (GRC), and Information Rights Management (IRM). To register for this free webinar, visit BrightTalk here.

Patches and Updates

Oracle
Drupal
Schneider Electric IIoT Monitor (Update A)

Vulnerabilities

Multiple Vulnerabilities in PHP Could Allow for Arbitrary Code Execution

Vulnerabilities in the PHP programming language can allow attackers to execute arbitrary code in any web-based software applications scripted with PHP. Depending on privileges assigned to the application, an attacker could exploit vulnerabilities in PHP to install programs; view, change, or delete data; or create new accounts with full user rights. ***The NTIC Cyber Center recommends reviewing both the Center for Internet Security advisory and updating to the latest versions of PHP to mitigate attacks and potential exploits of these vulnerabilities.***

Vulnerabilities Found in PremiSys IDenticard Access Control System

Researchers at cybersecurity firm Tenable discovered four vulnerabilities in the PremiSys IDenticard access control system that, if exploited, could be used to create counterfeit identification cards, disable locks and gain unauthorized access to protected facilities, and access sensitive information. These vulnerabilities exist primarily due to the system's use of hardcoded passwords and weak encryption methods. There is currently no patch available. ***The NTIC Cyber Center recommends all users of the PremiSys IDenticard access control system review Tenable's report, ensure that the system is not exposed to the Internet, and properly segment their network to isolate the system from external and unauthorized access.***

Cyber in the News

Courts Hand Down Hard Jail Time for DDoS

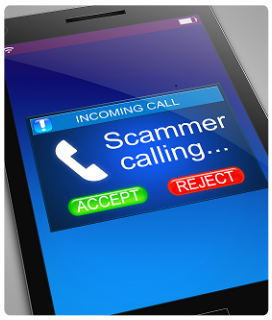
Analytic Comment: Although penalties for computer-related crimes vary between states and countries, law enforcement agencies across the globe are increasingly committed to bringing those responsible to justice. Attribution can be difficult, though, and state-sponsored hackers will likely never be held accountable, even if their identities are discovered. However, harsher penalties levied against smaller criminal groups and nuisance hackers who are caught can serve as a deterrent to others, especially younger hackers who may not want to risk serving several years of jail time.

Pentagon Faces Backlog of More Than 260 Cyber Weaknesses, Some a Decade Old

Analytic Comment: This report highlights the challenges large organizations face in managing their cybersecurity risks when they lack the governance needed to successfully identify gaps and take appropriate corrective actions. As the cyber threat landscape expands and evolves, organizations must act quickly to protect against new threats, exploits, and vulnerabilities. Implementing a comprehensive IT change management framework and cyber incident response plan can help organizations tackle these challenges and more effectively secure their network infrastructure.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.



A ***neighbor number scam***, also called ***neighbor spoofing*** or ***caller ID spoofing***, is a technique that scammers use to deliberately falsify telephone caller ID information to conceal their identifying information. Masquerading as a neighbor or otherwise legitimate local caller, scammers prey on those who answer these calls in any number of ways. Click here to read more about this prevalent phone scam and learn how to protect yourself.

Report a Cyber Incident

If you are the victim of a cyber attack, please click here to report the incident using our online submission form. Your report helps the NTIC Cyber Center develop a better understanding of cyber threats impacting our region. Submitting a report will not generate a criminal investigation; however, our analysts may be able to provide you with guidance and mitigation recommendations. All incident reports submitted will remain confidential.

Please note that the NTIC Cyber Center does not perform computer repairs and cannot endorse any commercial vendors, products, or solutions.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

January 24, 2019

National Capital Region Cyber Threat Spotlight

In addition to the financial hardship that many US federal employees currently face from the ongoing government shutdown, there is increasing concern from government officials, law enforcement agencies, and security experts that this will have a lasting negative impact on efforts to bolster the nation's cybersecurity posture and reduce cybercrime. In a KrebsOnSecurity article published yesterday, a federal agent expressed his concern about the talent drain that is occurring as furloughed employees begin to seek professional opportunities in the private sector. The vacuum created by this loss of experience, knowledge, and manpower is already evident by the inability for new and current employees to obtain the security clearances needed to perform their jobs effectively. Furloughed workers who find themselves financially strapped during this time risk becoming easy targets for malicious social engineering schemes promising lucrative opportunities in exchange for sensitive information. Additionally, the increase in outdated Web security certificates held by US agencies sparks concern among security professionals who worry that this may be evidence of larger cybersecurity gaps, namely the maintenance and protection of critical systems, networks, and infrastructure. For these reasons and more, the security of the National Capital Region and the nation as a whole is and will remain at risk until the federal government reopens and furloughed employees can return to work.

In light of this situation, the NTIC Cyber Center would like to take this opportunity to offer our heartfelt gratitude to our dedicated federal partners who continue to work tirelessly without pay to uphold their duties and protect our nation. Your hard work and dedication have not gone unnoticed.

Current and Emerging Cyber Threats

Top Free Virtual Private Network (VPN) Android Apps Pose Privacy and Malware Risk to Users

According to security researchers at Top10VPN, there are serious malware and privacy risks among the top 150 free VPN Android mobile applications available in Google's Play Store. Of these VPN apps, 27 apps potentially contain malware, 25 percent fail to protect user privacy as a result of DNS leaks, and 85 percent contain functions designed to collect user data or access the device's camera and microphone. The affected apps have been downloaded and installed nearly 260 million times. ***The NTIC Cyber Center encourages all mobile device users to exercise caution before installing any app and to pay close attention to required permission settings. If the permissions required do not match the advertised functionality of the app, do not install it. After installing any new app, monitor the device for unusual behavior such as excessive power consumption, excessive data usage, overheating, or device malfunction and uninstall problematic apps immediately.***

New Rumba Ransomware Variant Bundled in Software Cracks

Security researchers identified a malware campaign that distributes a new variant of STOP ransomware, dubbed Rumba, by bundling it with adware in downloads of software cracks – programs that illegally activate unlicensed or pirated software, bypass copyright protection features, or generate product activation keys. Once a system is infected, Rumba encrypts files, appends the *.rumba* extension to the file names, and then drops a ransom note named *_openme.txt* in each folder that contains encrypted files. In some cases, victims impacted by Rumba may be able to recover their files without paying the ransom by using a free decryption tool provided on the Bleeping Computer forums. ***The NTIC Cyber Center would like to remind members that using pirated software and cracks is not only illegal but also creates a security risk as these files can be a vehicle for various types of malware. Additionally, as ransomware continues to pose a high risk to individuals and organizations, we strongly recommend backing up data regularly and keeping all devices and software updated with the latest patches.***

Data Breach Alert

Valley Hope Association

Valley Hope Association, an alcohol and drug addiction treatment center with 16 facilities in seven states, released a notice to patients informing them of a data breach that occurred between October 9th and 10th of last year. An investigation determined that, during that timeframe, an unauthorized user gained access to an employee's email account and may have used it to access sensitive patient

information. According to investigators, the compromised information may include one or more of the following data points: name, address, medication/prescription information, Social Security number, financial account information, driver's license or state identification card number, patient claim/billing information, date of birth, health insurance information and medical record number, and doctor's name. Valley Hope Association is offering affected patients free credit monitoring services through Kroll for one year. ***The NTIC Cyber Center recommends all affected patients review Valley Hope Association's** Notice of Security Event **and follow the guidance provided.***

Upcoming Webinar:

6 Proactive Cybersecurity Precautions to Take Now

Todd Fitzgerald, veteran CISO and co-author of the book *CISO Leadership Skills: Essential Principles for Success* will participate in a live webinar on Wednesday, January 30th at 2:00pm EST to discuss the 7S framework used to trace an organization's performance problems and strategies for improving cybersecurity programs within organizations. To register for this free webinar, visit BrightTalk here.

Patches and Updates

ABB CP400 Panel Builder TextEditor 2.0

Adobe

Apple

Cisco

ControlByWeb X-320M

Dräger Infinity Delta

Johnson Controls Facility Explorer

Juniper

Microsoft

Omron CX-Supervisor

Vulnerabilities

WordPress Plugin Social Network Tabs Exposes Twitter Accounts to Compromise

A vulnerability recently discovered in *Social Network Tabs*, a popular third-party WordPress plugin, exposed some Twitter accounts to compromise by storing account access tokens in the source code of the associated website. Access tokens are used to keep account sessions active and reduce the need for the owners to repeatedly provide authentication. However, if the tokens are stolen, they can be used to gain unauthorized access to – and control over – an online account. ***The NTIC Cyber Center recommends WordPress website administrators who installed the Social Network Tabs plugin remove it immediately, change their Twitter password, enable two-factor authentication on the account, and remove the plugin from Twitter's connected apps list.***

Cisco Small Business Switches Contain Privileged Access Vulnerability

Cisco announced a vulnerability in its Small Business Switches software that, if exploited, could allow attackers to bypass authentication on the device and execute commands with full administrative rights. Although there is currently no patch available, Cisco advises users to add at least one user account with access privileges set to level 15 in the device configuration in order to disable the vulnerable default user account. ***The NTIC Cyber Center recommends all administrators of Cisco Small Business Switches review the Cisco Security Advisory and apply the recommended workarounds until a patch becomes available.***

Vulnerability Discovered in Common Wi-Fi Chipset

A researcher from security firm Embedi discovered a vulnerability within the modified firmware of Marvell Avastar 88W8897, a common Wi-Fi chipset used in various computers, gaming platforms, routers, and Internet-of-Things (IoT) devices. If exploited, this vulnerability could allow an attacker to execute malicious code and take control of the affected device even if it is not connected to a network. There is currently no patch or workaround available for this vulnerability. ***Although the NTIC Cyber Center is not presently aware of any reports of this vulnerability being actively exploited in the wild, we do recommend powering down devices that contain the affected chipset when not in use, if possible, and monitoring them for unusual activity when in use. If a patch becomes available, we recommend applying it to affected devices as soon as possible.***

Cyber in the News

Senators Worry That New DC Metro Railcars Could Carry Cyber Risk

Analytic Comment: As concerns grow over cybersecurity risks to the US industrial supply chain and infrastructure, there are questions being raised about potential threats posed by non-US companies linked to foreign governments that have a history of conducting espionage operations for political and financial gain. Allowing foreign-built products to establish a foothold in the transportation network of the nation's capital could open the door to privacy and security risks that would be difficult to mitigate, which is why four US lawmakers are requesting federal oversight of

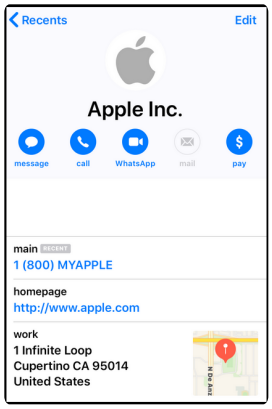
the Metro railcar procurement process.

[Ex-Employee Hacks WPML WordPress Plugin Site and Spams Users]

Analytic Comment: This incident highlights the risks insider threats can pose to an organization. Insider threats can be current or former employees, contractors, third-party vendors, or partners who have or had authorized access to a network and uses that access to cause harm to an organization's systems, data, or reputation. Organizations are encouraged to perform regular audits of network access and account privileges, immediately deactivate accounts of separated employees, and review the US Department of Homeland Security's advisory titled *Combating the Insider Threat*.

Securing Our Communities

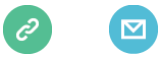
Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.



A recently-discovered ***Apple phone-based phishing scam*** uses sophisticated tactics to target Apple users and obtain sensitive, personal information such as login credentials and financial information. In this scam, the inbound phone call appears as though it originates from Apple's customer support number. Along with the phone number, the associated contact card displayed in the target's recent call list even spoofs other Apple information such as the company's website address and business location to appear legitimate. Click here to read more about this prevalent phone scam and learn how to protect yourself.

TLP:WHITE

We welcome your feedback. Please click here to complete a brief survey and let us know how we're doing.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

January 31, 2019

Announcement

MS-ISAC Releases Alert on DNS Flag Day

On January 30, 2019 the Multi-State Information Sharing & Analysis Center (MS-ISAC) released an alert on Domain Name System (DNS) Flag Day, which is Friday, February 1, 2019. On DNS Flag Day, DNS software and service providers will release updates to remove workarounds that allow users to bypass the Extension Mechanisms Protocol for DNS (EDNS). While the updates will improve DNS operations, some domains served by DNS servers operating out-of-date software may become unavailable. The NTIC Cyber Center and MS-ISAC recommend taking inventory of DNS servers to determine if they are EDNS compliant. EDNS compliancy testing platforms and a list of participating DNS providers is available at: https://dnsflagday.net/ and http://ednscomp.isc.org/. Although the average Internet user does not need to take any steps in preparation for DNS Flag Day, domain holders, DNS administrators, and DNS software developers are encouraged to visit the aforementioned resources and take the recommended steps to avoid operational issues.

Current and Emerging Cyber Threats

Phishing Campaigns Deliver Gandcrab Ransomware and Ursnif Malware

Carbon Black security researchers identified a phishing campaign that delivers both Gandcrab ransomware and Ursnif malware via attached Microsoft Word documents. The Word documents, of

which researchers have identified roughly 180 variants, reportedly contain an embedded macro that, when run, executes a script to access a command-and-control address and then downloads ransomware and data-stealing malware to victims' computers. The malware proceeds to harvest credentials and gather system and process information while the ransomware encrypts files and extorts victims for payment. Most antivirus solutions do not flag or block Word documents with embedded macro code, as macro functionality is a normal operating feature of programs in the Microsoft Office Suite. ***Since exploiting this functionality to deliver malicious payloads is a common attack vector, the NTIC Cyber Center recommends users disable macros by default and avoid opening documents from unknown and untrusted sources.***

Cyber Attacks Increasing against Vulnerable Cloud Infrastructure

Securonix researchers report an increase in automated attacks targeting exposed cloud infrastructure via the exploitation of Apache Hadoop, Redis, and Active MQ vulnerabilities as well as weak or default login credentials. The goal of these attacks typically includes either a malware infection such as cryptocurrency-mining malware or ransomware, or to obtain remote access of the targeted cloud instance. ***The NTIC Cyber Center recommends administrators of cloud infrastructure services review the indicators of compromise included in the Securonix report linked above and reduce their risk of compromise by implementing strong authentication policies to mitigate against brute-force entry attacks.***

Phishing Campaign Targets Microsoft Account Credentials Using EML Attachments Masquerading as Voicemail Notifications

Cybersecurity website Bleeping Computer warns readers of a phishing campaign that uses EML attachments masquerading as voicemail delivery notifications to pilfer login credentials from unsuspecting victims. If email recipients open the attachment, they will be directed to a phishing site designed to capture their Microsoft account login credentials. When credentials are entered, the individual is prompted to enter them again because the website will display an "incorrect password" warning. Researchers believe that this step helps to make the campaign appear more legitimate and to obtain verification of victims' passwords. After the password is entered a second time, the phishing site will play a generic audio recording of a voicemail. ***The NTIC Cyber Center recommends users maintain vigilance when receiving unsolicited emails containing attachments and check URL address bars for suspicious-looking links that may be masquerading as legitimate services. Users who believe they may have fallen victim to this phishing scam should promptly change passwords for any accounts that use the password entered on the fraudulent Microsoft account login page.***

Data Breach Alert

Discover Financial Services

Discover Financial Services notified cardholders of a data breach that the company discovered on August 13, 2018. According to sample notices filed with the California Attorney General's office on January 25, 2019, the breach did not involve Discover card systems. Although it is currently unknown how many cardholders were affected, California law requires companies who conduct business with the state's residents to file security notices if a cybersecurity incident impacts more than 500 California residents. ***The NTIC Cyber Center recommends all affected Discover customers monitor their accounts for unauthorized activity, activate their replacement Discover card when it arrives, and follow any additional guidance the company provides.***

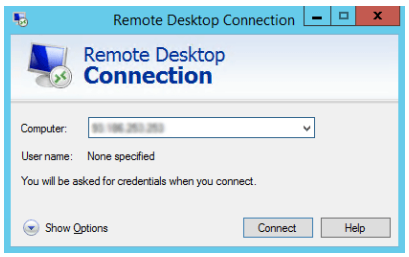
Upcoming Briefings and Webinars:

Chinese Malicious Cyber Activity Awareness Briefings

The US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) will conduct a series of virtual awareness briefings on Chinese malicious cyber activity targeting managed service providers (MSPs). Briefings will be held from 1:00pm to 2:00pm ET on the following dates:

- Wednesday, February 6
- Friday, February 22

CISA encourages MSPs and their customers to register for the briefing by clicking on one of the dates listed above. The briefing will provide a background on the identified cyber activity and mitigation techniques.



Securing Organizations from Remote Desktop Protocol Exploits

Dr. Matt Kraning, Chief Technology Officer and co-founder of Expanse, will participate in a live webinar on Wednesday, February 6 at 1:30pm EST to discuss the risks that insecure instances of Remote Desktop Protocol pose to organizations and how misconfigurations can occur. To register for this free webinar, visit Data Breach Today here.

Patches and Updates

AVEVA Wonderware System Platform

BD FACSLyric

Cisco

Google Chrome

Mitsubishi Electric MELSEC-Q Series PLCs

Mozilla Firefox

Mozilla Thunderbird

Phoenix Contact FL Switch

Stryker Medical Beds

Yokogawa License Manager Service

Vulnerabilities

Total Donations WordPress Plugin

Researchers at cybersecurity firm Wordfence discovered vulnerabilities in Total Donations, a third-party WordPress plugin, that could be used to access sensitive information, manipulate site content, and hijack accounts. Engineering defects within the plugin resulted in Asynchronous JavaScript and XML (AJAX) manipulation. AJAX is used to keep website content dynamic by fetching new data, thereby reducing the need to reload web pages. However, if AJAX endpoints are compromised, they can be used to harm a WordPress account. There is currently no patch or workaround available for this vulnerability and the developers appear to have deserted the plugin and associated webpage.

The NTIC Cyber Center recommends WordPress website administrators who installed the Total

Donations plugin to delete it immediately instead of just disabling the plugin, as that would still make the site vulnerable. Changing the affected website's administrator password, enabling two-factor authentication, and properly vetting all plugins prior to and after installation is also recommended.

Cyber in the News

Three Charged for Working with Serial Swatter

Analytic Comment: Swatting is the practice of making a false report of an ongoing emergency or imminent threat intended to prompt an immediate tactical law enforcement response at a specific location. This practice is popular among teenagers and young adults, particularly within gaming communities, and is often used as a method of retaliation for a perceived grievance. In addition to public endangerment, swatting incidents can cost responders approximately $10,000 per incident and divert necessary resources from legitimate emergencies. Caller-ID spoofing technology can make it difficult to identify perpetrators, but fortunately, coordinated law enforcement efforts are helping to bring those responsible for deadly swatting incidents to justice.

Salisbury Police Hit by Ransomware Attack

Analytic Comment: The cyber incident that recently impacted computer systems at the Salisbury Police Department in Maryland highlights the risk that ransomware continues to pose to organizations. Fortunately, there was no indication that any data was stolen and, due to the department's robust maintenance of system backups, there was no permanent loss of data. However, an investigation revealed that the attacker allegedly gained access to the department's network via a software vendor's access to the police department's information system. Organizations are encouraged to review security policies for third-party vendor access into networks and to maintain regular backups of all critical data and resources to mitigate against the effects of ransomware attacks. For additional mitigation strategies, please download the NTIC Cyber Center Ransomware Mitigation Guide on our website at NCRIntel.org.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Have you ever received an unsolicited phone call or email from someone offering to help fix a computer problem? How about a pop-up or error message indicating your device was infected and urging you to contact a support person who could help? If so, you were a target of a ***tech support scam***. Tech support scammers can impersonate technical support professionals through many avenues, but their end goal is always the same—to steal your money, information, or identity. Click here to read more about this prevalent scam and learn how to protect yourself.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

February 7, 2019

National Capital Region Cyber Threat Spotlight

Yesterday, the US Department of Homeland Security (DHS) hosted a public webinar detailing the activities of APT10, a cyber-espionage group associated with China's civilian intelligence agency, the Ministry of State Security. US officials stated that APT10 targets the networks of global managed service providers to gain access to data-rich environments and conduct economic espionage and intellectual property theft. APT10 targets multiple US critical infrastructure sectors, including information technology, energy, communications, critical manufacturing, and healthcare. Although DHS stated they have seen a reduction in APT10 activity since the US Department of Justice indicted two of its alleged members in December 2018, they warn organizations to remain vigilant and monitor network activity for signs of unauthorized activity. ***The NTIC Cyber Center recommends all network administrators review US-CERT Alert (TA18-276B) and follow the security recommendations provided to reduce their risk of a successful network intrusion.***

Current and Emerging Cyber Threats

SpeakUp Trojan Targets Linux and macOS

Cybersecurity firm Check Point identified a new Trojan dubbed SpeakUp targeting servers running various Linux distributions and macOS. SpeakUp exploits the CVE-2018-20062 PHP vulnerability to gain an initial foothold into the targeted system and then injects a backdoor to maintain persistence. It establishes a connection with its command-and-control (C2) server and sends information about the infected system to the attacker. It also scans the network for other vulnerable

servers and launches brute-force attacks against them to gain unauthorized access. Currently, this Trojan installs cryptocurrency-mining malware on compromised servers; however, the attacker behind the campaign could easily use it to deliver more destructive malware variants. ***The NTIC Cyber Center recommends network administrators running Linux servers or macOS systems review the Check Point Research report, patch any vulnerable systems, and monitor their network for the associated indicators of compromise (IoCs).***

New macOS Malware Steals Browser Cookies and Mines Cryptocurrency

Security researchers from Palo Alto Networks' Unit 42 warn of a newly discovered malware variant, CookieMiner, that targets cryptocurrency wallet and exchange accounts on systems running macOS. It does so by stealing browser cookies, login credentials, text messages, and cryptocurrency wallet keys to circumvent multifactor authentication. This malware also steals credit card credentials and uses victims' systems to mine for cryptocurrency. ***The NTIC Cyber Center recommends network administrators who manage macOS systems within their environment review Unit 42's report for IoCs and block the associated domain and IP address.***

Gmail "Dot Accounts" Used to Facilitate Fraudulent Online Activity

Agari security researchers report encountering business email compromise scammers abusing a feature of Gmail email addresses to perpetrate fraud. This feature, which allows emails sent to addresses that include any permutations of periods to direct back to the same inbox, permits spammers to register numerous variations of email addresses with different online services. Since most services treat dotted variations of email addresses as distinct, scammers add or modify periods in an email address to create multiple accounts that forward communication to a single Gmail account. ***The NTIC Cyber Center recommends administrators of online services monitor for instances of excessive or varying period usage among email addresses used in the creation of new accounts as an indicator of possible fraudulent activity.***

Data Breach Alert

houzz

Houzz, a home improvement website, released a notice stating that, in December 2018, an unauthorized third party accessed a file containing some user data. Affected information potentially includes certain publicly visible profile information such as names, locations, and profile descriptions, user IDs, one-way encrypted and salted passwords, IP addresses, and certain internal identifiers. Houzz states that no financial information or Social Security numbers were exposed in the breach. ***The NTIC Cyber Center recommends all affected users reset their Houzz account***

passwords and change passwords for any other sites or services that used the same login credentials.

Restaurant chain Huddle House released a statement disclosing a point-of-sale data breach that began in August 2017 and continued through February 2019. A law enforcement agency and the company's credit card processor notified Huddle House of a malware intrusion that affected point-of-sale systems at some of the restaurant's corporate and franchised locations. The malware used in the breach collected cardholder names, payment card numbers, card expiration dates, and CVV numbers. As the incident is still under investigation, it is currently unknown how many Huddle House locations were impacted. ***The NTIC Cyber Center recommends customers who used payment cards at any Huddle House location within the affected timeframe monitor their account statements and immediately notify their financial institutions of any unauthorized activity.***

Upcoming Webinar

Prioritizing Security Operations in the Cloud through the Lens of the NIST Framework

On Thursday, February 21st at 1:00 PM EST, John Pescatore and David Aiken will participate in a live webinar to discuss how to use the NIST Cybersecurity Framework to secure infrastructure-as-a-service and hybrid cloud implementations. Topics discussed will include best practices and how to implement security controls at the perimeter, host, and data boundaries. To register for this free webinar, visit SANS.org.

Patches and Updates

Android OS

AVEVA InduSoft Web Studio and inTouch Edge HMI

BD FACSLyric (Update A)

IDenticard PremiSys

Kunbus PR100088 Modbus Gateway

Marvell Avastar Wi-Fi

Microsoft Exchange

Omron CX-Supervisor (Update A)

Rockwell Automation EtherNet/IP Web Server Modules

Schneider Electric EVLink Parking

Siemens Devices Using the PROFITNET Discovery and Configuration Protocol (Update O)

Siemens Industrial Products (Update K)

Siemens SCALANCE X Switches, RUGGEDCOM WiMAX, RFID 181-EIP,

and SIMATIC RF182C (Update A)

Siemens SIMATIC S7-1500 CPU

Siemens SIMATIC, SINUMERIK, and PROFINET IO (Update B)

Siemens SIMATIC PCS 7, SIMATIC WinCC, SIMATIC WinCC Runtime Professional, and

SIMATIC NET PC Software (Update F)

WECON LeviStudioU

Vulnerabilities

Remote Desktop Protocol

Security researchers at Check Point Research discovered multiple vulnerabilities in Remote Desktop Protocol (RDP) clients that could allow a malicious actor to launch a reverse RDP attack. By exploiting the vulnerabilities detailed in the article, a malicious actor using the remotely-accessed machine can reverse the usual direction of remote access communication to gain elevated network permissions on the RDP client machine. Vulnerable RDP clients include MSTSC from Microsoft, FreeRDP from GitHub, and rdesktop, an open-source client that is packaged in the Kali Linux distribution. ***The NTIC Cyber Center recommends reviewing the vulnerabilities associated with these RDP clients, patching relevant software with the latest updates, and disabling the "bi-directional clipboard sharing" functionality configured as a default setting in Microsoft's RDP client MSTSC.***

Cyber in the News

Hackers Target SMBs That Support US Power Grid

Analytic Comment: As small and mid-sized businesses (SMBs) generally cannot afford the same kind of cybersecurity protections that larger organizations can and typically have less staff available to prevent, respond to, and mitigate cyber incidents, they can easily and unknowingly create vulnerabilities for other organizations that exist within the supply chain. This can especially be problematic for SMBs that operate in support of US critical infrastructure as malicious actors perceive them as low-hanging fruit that can help them exploit larger, more profitable, and more attractive targets. To reduce the cyber risk posed by less secure elements of

the supply chain, all organizations are recommended to audit the security protocols of their suppliers and actively monitor network access provided to external parties.

30 Percent of Automotive Companies Lacking a Dedicated Cybersecurity Team

Analytic Comment: Ponemon Institute researchers discovered that, while automobile manufacturers increasingly integrate software and wireless connectivity into their vehicles due to consumer demand and competition, properly implemented cybersecurity programs and practices are severely lacking throughout the industry. Surveys from IT professionals and automotive engineers reveal that 30 percent of automotive companies lack cybersecurity programs and 63 percent test less than half of their products for vulnerabilities. As drivers rely on their vehicles to get them safely to their destinations, cybersecurity must become as much of a priority for manufacturers as physical crash testing.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Virtual kidnapping is a type of phone scam in which the perpetrator uses online reconnaissance and social engineering tactics to research their victims and convince them that their loved ones have been kidnapped. The perpetrator then demands a ransom payment for their safe return. However, the kidnapping never actually took place and the victims' loved ones are safe, often having no knowledge of the alleged threat. In this scam, the perpetrator relies on generating a strong emotional response to cloud victims' judgment and extort large sums of money. Click here to read more about this prevalent phone scam and learn how to protect yourself.

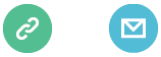
TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.

We welcome your feedback. Please click here to complete a brief survey and let us know how we're doing.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

February 14, 2019

National Capital Region Cyber Threat Spotlight

The NTIC Cyber Center regularly observes new campaigns and indicators of compromise (IoCs) associated with Emotet, a modular banking Trojan designed to steal network and account login credentials from unsuspecting users. It also acts as a dropper that delivers additional malware to an infected system. Emotet is delivered via phishing emails that contain malicious attachments or links. If an email recipient opens the attachment or clicks on the embedded link, Emotet will download onto the computer, create auto-start registry keys, and inject itself into running system processes to evade signature-based antivirus detection and maintain persistence. It then contacts a command-and-control server for additional instructions from the attacker. Emotet uses several built-in modules and utilities to scrape account and network login credentials stored in various locations on the infected system and collect names and email addresses from the victim's Outlook account. It then propagates to other systems on the network and sends additional malicious emails from the victim's compromised account. According to the US Department of Homeland Security, Emotet is among the most costly and destructive malware affecting state, local, tribal, and territorial (SLTT) government organizations and the private and public sectors. ***The NTIC Cyber Center would like to remind our readers to never open attachments, enable macros in documents, or click on links contained within unexpected or unsolicited emails. If you believe you have been infected with Emotet, notify your organization's IT security team immediately so they may contain and remediate the infection.***

Current and Emerging Cyber Threats

Phishing Campaign Delivers Trickbot to North American Banking Customers

Cybersecurity firm Blue Hexagon reported a phishing campaign beginning January 27, 2019 that attempts to deliver Trickbot, a banking Trojan, to unsuspecting victims. The emails originate from fraudulent domain names designed to spoof JPMorgan Chase and Bank of America domains and contain an Excel document with malicious macros. If recipients open the document and enable the included macros, Trickbot will download from compromised websites and infect recipients' systems, harvesting emails and stealing banking credentials from the compromised machines. ***The NTIC Cyber Center recommends never opening attachments or enabling macros in documents received from unexpected or unsolicited emails. If you believe you have been targeted by this campaign or infected with the Trickbot Trojan, notify your organization's IT security team immediately. For home users who have been infected, make sure your antivirus software is up-to-date with the latest virus definitions and run a complete scan of your system. After removing the infection, change the passwords for all online accounts accessed from the compromised system and enable two-factor authentication on any account that offers it.***

Phishing Campaign Spoofs Bank Secrecy Act Officers' Email Accounts

Security researcher Brian Krebs warns of a phishing campaign targeting anti-money laundering officials at financial institutions throughout the United States. The phishing emails associated with this campaign masquerade as official correspondence from a credit union Bank Secrecy Act (BSA) or Anti-Money Laundering (AML) compliance officer and urges the recipient to open an attached PDF document to review a report of suspected money laundering. While the attached PDF document itself does not carry any payload, the body of the document includes a link to a malicious site. ***The NTIC Cyber Center recommends email users refrain from clicking on links or opening attachments contained in unexpected or unsolicited emails.***

Dunkin' Donuts Reward Program Customers at Risk of Credential Stuffing Attack

Dunkin' Donuts reported numerous customers fell victim to a credential stuffing attack that allowed third parties to access customers' DD Perks reward program accounts. According to the report, hackers used dumped email and password combinations originating from other companies' security breaches to log into customer accounts and access information such as customer name, email address, account number, and QR code. In some cases, the malicious actors were able to transfer or use balances from the compromised accounts to make purchases at Dunkin' Donuts locations. This

credential stuffing attack underscores the dangers of relying on single-factor authentication and using identical login credentials for different accounts. ***The NTIC Cyber Center recommends organizations implement multi-factor authentication on login services and account users create strong and unique passwords to access different platforms.***

Data Breach Alert

The Virginia Department of Elections [confirmed] that an accidental posting of login credentials resulted in the exposure of personal information of 96 job seekers applying for a Chief Information Officer position at the organization. The personal data, which was made accessible through a username and password mistakenly included in the job posting, included names, resumes, salary information, references, education history, home addresses, emails, and phone numbers of all applicants to the vacancy. Though the information has now been secured, it is unclear how many viewers may have accessed the data. ***For any members who believe they may be impacted by this data exposure, the NTIC Cyber Center recommends remaining vigilant for attempts of phishing or social engineering schemes targeting these applicants.***

VFEmail, an email account and storage provider, suffered a [critical breach] that destroyed the company's primary and backup data from all of their US-based servers. An unknown, malicious actor gained unauthorized access to the company's network and proceeded to format the disks on the company's servers, resulting in the irreversible data loss. The damage extended to the company's entire infrastructure including mail hosts, virtual machine (VM) hosts, SQL server cluster, and hosted VMs, suggesting the attacker likely obtained multiple passwords prior to conducting this attack. VFEmail learned of the attack after its associated Twitter account began receiving reports from customers complaining of problems accessing and receiving email. After investigating the problem, VFEmail discovered the malicious actor in the act of formatting one of the company's Netherlands-based mail servers. The reason behind the attack is unknown as there have been no signs of extortion and no communication attempts by the attacker before, during, or after the incident. ***The NTIC Cyber Center would like to remind readers about the importance of creating and maintaining comprehensive backups of critical data, including any important data stored***

within a cloud environment. Data backups should always be stored off the network and in a secure location.

On February 8, 2019, photography website 500px released a statement disclosing a data breach that occurred on July 5, 2018 and exposed partial user data from 15 million accounts. User data affected includes first and last names, 500px usernames, associated email addresses, password hashes, birthdates, location, and gender. According to the company's website, 500px coordinated an investigation and response effort with both a third-party security expert and with law enforcement authorities and is resetting user passwords for all 500px accounts. ***The NTIC Cyber Center recommends all 500px account holders follow the instructions in the company's notification email and reset their passwords as soon as possible.***

Upcoming Webinar

New Year, New Phishing Threats: 10 Resolutions to Keep You Safe & Secure

On Tuesday, February 19th at 8:00 AM EST, Brandon Dunlap will moderate a discussion with David Mount and Molly Hollerman of Cofense about phishing defense programs that can help protect organizations from social engineering attacks. Topics discussed will include how employees can recognize and help defend against phishing threats, best practices, and solutions that are available to help organizations improve their email security. To register for this free webinar, visit BrightTALK.

Vulnerabilities

Stored Passwords in Apple macOS Vulnerable to Theft

A private security researcher uncovered a vulnerability in Apple's macOS that may allow a malicious app to read private password data stored locally in Apple's iCloud Keychain software. Though this vulnerability currently affects only the macOS platform, passwords stored on iPhones synchronized with Mac devices through iCloud Keychain may also be at risk. As there is currently a

discrepancy between Apple and the researcher with regards to compensation in exchange for details on the hacking methods, the vulnerability remains unpatched. ***The NTIC Cyber Center cautions users of Apple's iCloud Keychain software to avoid downloading unknown files or accessing untrusted links, both of which could deliver malware hiding the keychain exploit or launch rogue code to perform the password-stealing hack.***

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

A ***romance scam***, also known as a ***sweetheart scam*** or ***confidence fraud***, is a type of social engineering scheme in which a perpetrator masquerades as a potential love interest but conceals his or her true intentions to elicit money or material possessions from unsuspecting victims looking for love online. These scammers, who either work alone or as a part of an organized crime ring, create detailed fraudulent profiles on dating websites, apps, and social media platforms using images stolen from legitimate profiles or elsewhere on the internet. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Business Email Compromise Attacks See Almost 500 Percent Increase

Analytic Comment: As organizations work toward improving their cybersecurity posture and software vendors rush to release updates to patch known vulnerabilities, cyber threat actors are increasingly using social engineering methods to exploit one of the largest vulnerabilities – humans – to commit fraud and gain unauthorized access into networks. Researchers at cybersecurity firm Proofpoint found that business email compromise campaigns rose nearly 500 percent between 2017 and 2018, demonstrating that fraudulent emails remain a very large risk for organizations across all

sectors. Implementing effective email security controls and conducting regular security training for employees can help reduce this risk and harden networks against email-based threats.

Google Survey Finds Two in Three Users Reuse Passwords

Analytic Comment: Internet users must track and maintain more passwords now than ever before and, because it can be challenging to remember different login credentials for every account, users often find it easier to reuse passwords than to create unique, complex ones. However, once login credentials are stolen, every account secured by them is at risk of compromise. Reputable password managers can help users create and maintain a database of unique and secure login credentials for every account and two-factor authentication can help protect accounts from unauthorized access resulting from stolen usernames and passwords.

Patches and Updates

Adobe

Apple

Cisco

Fuji Electric Alpha5 Smart Loader (Update A)

Kunbus PR100088 Modbus Gateway (Update A)

Microsoft

Mozilla Firefox

Omron CX-Supervisor (Update A)

OSIsoft PI Vision

Siemens CP1604 and CP1616

Siemens EN100 Ethernet Module

Siemens EN100 Ethernet Communication Module and SIPROTEC 5 Relays

Siemens Industrial Products (Update A)

Siemens Industrial Products (Update L)

Siemens Intel Active Management Technology of SIMATIC IPCs

Siemens License Software for SICAM 230

Siemens OpenSSL (Update D)

Siemens SICAM A8000 RTU Series

Siemens SIMATIC S7-300 CPU

Siemens SIMATIC S7-1500, Software Controller, and ET 200SP OpenController (Update A)

Siemens SIPROTEC 4, Compact, and Reyrolle Devices (Update B)

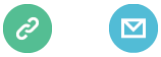
TLP:WHITE

about TLP designations, please visit US-CERT.

To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.

We welcome your feedback. Please click here to complete a brief survey and let us know how we're doing.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

February 21, 2019

National Capital Region Cyber Threat Spotlight

The NTIC Cyber Center regularly identifies new indicators of compromise (IoCs) associated with the GandCrab ransomware campaign. First discovered by security researchers in January 2018, GandCrab is a ransomware variant distributed via exploit kits, malicious online advertisements, and spam email campaigns. Once GandCrab infects a system, it attempts to connect to a command-and-control server. If the connection is successful, GandCrab will determine the IP address of the victim, terminate certain system processes, and begin encrypting files, appending an extension such as .GDCB to file names. It will also drop ransom notes named GDCB-DECRYPT.txt in multiple locations on the system.

Recently, NTIC Cyber Center analysts discovered a website on the Dark Web that advertised GandCrab ransomware "as a service" to anyone willing to pay a $230 licensing fee. Profit-motivated criminals have used the ransomware-as-a-service (RaaS) business model for different variants over the past several years to earn money without directly managing individual infections. RaaS also lowers the barrier to entry for criminals who do not have programming skills and makes attribution difficult for victims and law enforcement. Despite security researchers' efforts to create free decryption tools for GandCrab victims, the developers continuously update the malware's code to render these tools ineffective.

For these reasons, the NTIC Cyber Center assesses with high confidence that GandCrab ransomware will remain a persistent threat to individuals and organizations throughout the NCR and the United States. To reduce your risk of a ransomware infection, we encourage you to visit our

website and download the NTIC Cyber Center Ransomware Mitigation Guide and the NTIC Cyber Center Guide for Cyber Incident Response Planning.

Current and Emerging Cyber Threats

Rietspoof Malware Family Delivers Multiple Payloads, Updated Frequently

Cybersecurity firm Avast discovered Rietspoof, a new malware family that uses several methods of compromise and drops a variety of payloads to infect its target. Initial attack vectors include Microsoft Word documents containing malicious macros sent via instant messaging software such as Skype or Live Messenger. Once installed, Rietspoof acts as a bot and can download and upload files, start various processes, and issue self-destruct commands. It is also capable of establishing persistence on an infected system by adding a *WindowsUpdate.lnk* file to the Windows startup folder that runs a Portable Executable binary every time the system is rebooted. The associated command-and-control server has basic geofencing capabilities, allowing it to modify commands based on the infected system's IP address. Although the malware's primary function, targets, and infection chain are currently unknown, Avast researchers recently observed a notable increase in the frequency of updates implemented by the developers. This suggests that the developers may be preparing to deploy Rietspoof in a large-scale malware campaign. ***The NTIC Cyber Center recommends never enabling macros on unexpected or unsolicited documents. We also recommend network administrators review Avast's report, tighten macro security settings on all end user machines, and monitor their networks for suspicious activity associated with Rietspoof. The report can be viewed here.***

New Sophisticated Phishing Scheme Targets Facebook Credentials

Password management company Myki recently discovered a new and sophisticated attack vector designed to steal Facebook login credentials from unsuspecting victims. The attackers behind this campaign design phishing websites that launch realistic Facebook pop-up windows prompting visitors to log into their social media accounts before viewing the sites. However, these "pop-ups" are created using HTML and exist within the website itself; they do not actually launch a new browser window. If victims enter their login credentials into the pop-up, the information is sent to the attackers who can use it to gain unauthorized access to their social media accounts and any other accounts that share the same credentials. ***The NTIC Cyber Center recommends remaining vigilant when browsing the internet and scrutinizing websites for legitimacy prior to entering login credentials and sensitive information. Before entering login credentials into a pop-up, users are encouraged to try and drag the pop-up away from the current browser window. If the pop-up***

cannot be separated from the current window, it is likely fraudulent. A video demonstration of this attack is available on YouTube here.

Data Breach Alert

A hacker using the alias *Gnosticplayers* reportedly posted three sets of stolen database credentials to the Dark Web marketplace DreamMarket. To date, the breaches include 16 databases comprising 620 million user credentials, eight databases comprising 127 million user credentials, and another eight databases comprising 93 million user credentials. The data available via these breaches includes information such as names, physical addresses, email addresses, usernames, passwords, IP addresses, Facebook user IDs, and banking information. The following are databases and sites allegedly impacted by the breaches; the threat actor indicates more data may be forthcoming, so this list may not be exhaustive:

Dubsmash — 162 million accounts
MyFitnessPal — 151 million accounts
MyHeritage — 92 million accounts
ShareThis — 41 million accounts
HauteLook — 28 million accounts
Animoto — 25 million accounts
EyeEm — 22 million accounts
8fit — 20 million accounts
Whitepages — 18 million accounts
Fotolog — 16 million accounts
500px — 15 million accounts
Armor Games — 11 million accounts
BookMate — 8 million accounts
CoffeeMeetsBagel — 6 million accounts
Artsy — 1 million accounts
DataCamp — 700,000 accounts
Houzz — 57 million accounts
YouNow — 40 million accounts
Ixigo — 18 million accounts
Stronghold Kingdoms — 5 million accounts
Roll20.net — 4 million accounts
Ge.tt — 1.83 million accounts
Petflow — 1 million accounts
Coinmama — 420,000 accounts
Legendas.tv — 3.86 million accounts
Jobandtalent — 11 million accounts
Onebip — 2.6 million accounts
StoryBird — 4 million accounts
StreetEasy — 1 million accounts
GfyCat — 8 million accounts
ClassPass — 1.5 million accounts
Pizap — 60.8 million accounts

The NTIC Cyber Center recommends using lengthy and complex passwords that are unique to every online account to reduce the risk of further compromise in the event of a data breach. Additionally, enable two-factor authentication on any account that offers it as an additional security measure. Users of these and any breached site or service are encouraged to reset their passwords as soon as possible and monitor their accounts for suspicious activity.

Industry Report

2019 CrowdStrike Global Threat Report

This week, cybersecurity firm CrowdStrike released its 2019 Global Threat Report highlighting the increasing pace and sophistication of adversary tactics, techniques, and procedures (TTPs) observed over the past year. Highlights from this report include the following:

- CrowdStrike dives deeply into the data to show attackers most favored TTPs of 2018 through the lens of MITRE ATT&CK™ framework.
- Updates on global "breakout" time statistics, including observations on which adversaries showed the fastest tradecraft in 2018.
- No respite from nation-state threats: Nation-state adversaries were continuously active throughout 2018 — targeting dissidents, regional adversaries and foreign powers to collect intelligence for decision-makers.
- The continued rise of "Big Game Hunting", where cyber criminals combine advanced, targeted attack techniques with ransomware to achieve massive financial payoffs.
- The eCrime ecosystem continues to evolve and mature, showing increased collaborations between highly sophisticated criminal actors.

This report is available for free via CrowdStrike's website here.

Upcoming Webinars

72-Hours-to-Disclose Survival Guide: Accurate Scoping and Impact Assessment of Breaches

On Tuesday, February 26th at 1:00 PM EST, John Matthews of ExtraHop and John Pescatore of SANS will participate in a live webinar to discuss how to determine the scope and impact of a cyber incident and how analysts can use network traffic analysis to improve incident response time. To register for this free webinar, visit SANS.org.

NIST Recommendations for ICS & IIoT Security

On Thursday, February 28th at 3:30 PM EST, Phil Neray, Michael Powell, Jim McCarthy, and Tim Zimmerman will participate in a live webinar to discuss NIST recommendations to defend against cyber threats that target industrial control systems and the industrial internet of things. To register for this free webinar, visit SANS.org.

Vulnerabilities

Flaws in Popular Password Managers Expose Credentials in RAM

Independent Security Evaluators (ISE) published a report this week highlighting vulnerabilities discovered in popular password management tools such as 1Password, Dashlane, KeePass, and LastPass that, if exploited, could allow an attacker to obtain a victim's login credentials stored in the targeted system's memory. The team's findings reveal that the password managers in question store unencrypted passwords in RAM for varying amounts of time when users access their login credentials, providing an opportunity for malware on an infected system to scrape the RAM and collect the exposed data. The developers of these password managers are aware of this vulnerability with one declaring that the issue is "a well-known and documented limitation of the process memory protection." One password manager, LastPass, released a patch to address this problem within their software. ***Despite these flaws, the NTIC Cyber Center strongly recommends using a password manager to generate and store lengthy, unique passwords for all online accounts and to prevent password reuse. We also recommend all LastPass users ensure that they are running the latest version of the software. All current versions can be downloaded from the LastPass website.***

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Business Email Compromise (BEC) – also known as a ***CEO scam*** or ***whaling*** – is a type of phishing scheme in which the perpetrator conducts online reconnaissance against a target organization and then uses various social engineering techniques to try and convince employees within that organization to divulge sensitive personal or financial information. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Chinese and Iranian Hackers Renew Their Attacks on US Companies

Analytic Comment: As government agencies and private companies within the United States struggle to protect their networks against a variety of cyber attacks by a myriad of threat actors, experts warn that Chinese and Iranian hackers have increased their efforts to compromise networks in retaliation for recent decisions made by the current US administration regarding trade agreements and the Iran nuclear deal. Nation-state hackers are becoming increasingly sophisticated in their tactics, making cybersecurity a challenge for smaller organizations that may not have the budget for comprehensive security solutions.

Hackers Use Compromised Banks as Starting Points for Phishing Attacks

Analytic Comment: Although this report primarily focuses on vulnerabilities in the overseas banking infrastructure, it highlights how hackers can easily use a single compromised target to create a "chain attack" against other organizations. This attack vector allows hackers to expand their reach while simultaneously obfuscating their origins. Ultimately, organizations that work to improve their own cybersecurity posture by securing their networks and protecting their data also help improve the security of their customers, clients, and partners.

Patches and Updates

Cisco

Delta Industrial Automation CNCSoft

Horner Automation Cscape

Intel Data Center Manager SDK

Kaseya VSA

Mozilla Thunderbird

Rockwell Automation Allen-Bradley PowerMonitor 1000

VMware

WordPress

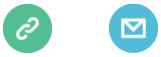
TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.

We welcome your feedback. Please click here to complete a brief survey and let us know how we're doing.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

February 28, 2019

National Capital Region Cyber Threat Spotlight

BabyShark Malware Targets US Think Tanks and Universities

Earlier this month, Palo Alto Networks Unit 42 researchers discovered a new malware variant, dubbed BabyShark, that they attributed to an Advanced Persistent Threat (APT) campaign originating from North Korea. The researchers determined that BabyShark shares the same malware infrastructure and behaviors as other North Korean APT campaigns such as KimJongRAT and STOLEN PENCIL. In November 2018, BabyShark targeted at least one US think tank and one US university via spear phishing emails that appeared to originate from a nuclear security expert working as a consultant within the United States. The emails had a subject line that referenced North Korean nuclear issues and contained an attachment embedded with malicious macros designed to download the malware onto the targeted system. Based on the contents of the decoy documents included in the emails, the researchers believe the hackers behind this campaign likely compromised the account of an individual who had access to private documents at a US national security think tank. ***The NTIC Cyber Center recommends never enabling macros on unexpected or unsolicited documents. We also recommend network administrators review Palo Alto Networks' report, tighten macro security settings on all end user machines, and monitor their networks for suspicious activity associated with BabyShark. More information about this campaign, including Indicators of Compromise (IoCs), is available here.***

Current and Emerging Cyber Threats

Phishing Campaign Spoofs United Nations and Multiple Other Organizations

Researchers at cybersecurity firm Anomali Labs discovered a phishing website that spoofs the sign-in page for the United Nations Unite Unity application in an attempt to steal users' login credentials. After logging into the site, the victim is redirected to an invitation to a film screening at the Poland Embassy in North Korea. Further analysis revealed that the same campaign also spoofed login pages for multiple email providers, financial institutions, and a payment card provider. Although Anomali submitted the offending URLs to Google and Microsoft to be blacklisted, spoofed websites designed to phish unsuspecting users' account credentials continue to be a threat. ***The NTIC Cyber Center recommends remaining vigilant when browsing the internet and scrutinizing websites for legitimacy prior to entering login credentials and sensitive information. Additionally, we encourage our readers to refrain from clicking on links in unexpected or unsolicited emails.***

LinkedIn Used to Deliver More_eggs Malware to Victims

Threat researchers at Proofpoint identified a phishing campaign that delivers More_eggs backdoor malware via fake job offers sent through the LinkedIn social media platform. Threat actors use Linkedin's direct messaging service to send emails offering phony employment opportunities to trick victims into visiting a spoofed staffing management webpage. Victims are then prompted to download a Microsoft Word file containing malicious macros that, if enabled, install the More_eggs backdoor malware that grants the threat actors remote control of the infected system. This malware campaign bears similar characteristics to those of a recently profiled phishing email scam targeting anti-money laundering officers at US financial institutions and researchers believe the same actors may be responsible for both attacks. Most antivirus solutions do not flag or block Word documents with embedded macro code, as macro functionality is a normal operating feature of programs in the Microsoft Office Suite. ***Since exploiting this functionality to deliver malicious payloads is a common attack vector, the NTIC Cyber Center recommends users disable MS Office macros by default and avoid opening documents from untrusted sources. We further recommend network administrators review Proofpoint's report, tighten macro security settings on all end user machines, and monitor their networks for the associated IoCs.***

Cr1ptTor Ransomware Targets Exposed D-Link Network Attached Storage Devices

BleepingComputer warns of a newly emergent ransomware called Cr1ptTor that targets the D-Link DNS-320, a network attached storage (NAS) device used to store and share data. The attack likely leverages numerous vulnerabilities in the device's outdated firmware to infect the device, encrypting

all data stored within it and demanding a ransom payment of approximately $1,200 worth of Bitcoin for the decryption key. It also provides the option to decrypt individual files for $19.99 each, requiring victims to send locked files to the attacker to be decrypted. ***As there are currently no updated patches available for the D-Link DNS-320 and a hardcoded backdoor has been identified within the ShareCenterDNS-320L, the NTIC Cyber Center recommends immediately decommissioning the vulnerable NAS device models.***

Profit-Motivated Criminal Campaigns Target E-Commerce Websites

A report by Malwarebytes Labs details ways in which hackers may be accessing popular content management systems such as Magento to launch skimming attacks that steal customer data from e-commerce websites. According to the report, hackers appear to be exploiting vulnerabilities in websites and plugins or using brute-force attacks to obtain websites' administrative account credentials to install skimming malware. This malware then steals customer information such as names, credit card numbers, usernames, and passwords entered during checkout and relays the data back to the perpetrators using a command-and-control server. ***The NTIC Cyber Center recommends e-commerce website administrators keep web server software, content management systems, and associated plugins up to date, regularly audit websites for unauthorized code changes, and consider implementing a web application firewall.***

Data Breach Alert

ZDNet reports that unidentified criminals recently posted a massive collection of credit card payment data valued at $3.5 million on Joker's Stash, a popular underground marketplace for stolen payment card information. While two-thirds of the credit card details in the data dump belong to Pakistani bank customers, the remaining third may include US-based customers. Because the cards include their associated PIN numbers, they are advertised at a higher-than-average price of $50 per card. Also, this week, a Joker's Stash vendor began advertising another data dump dubbed the "DaVinci Breach" that reportedly consists of 2.15 million new payment cards. ***The NTIC Cyber Center recommends all credit card users monitor their accounts regularly and immediately report***

any unauthorized activity to their financial institutions.

Sports collectible site Topps.com released a customer notice disclosing a data breach that occurred between November 19, 2018 and January 9, 2019. According to the notice, the company became aware of the security incident that allowed unauthorized access to the Topps website and potentially compromised customer names, mailing addresses, telephone numbers, email addresses, and payment card information. A security researcher from RiskIQ believes that the company was impacted by a MageCart attack after discovering that a malicious script had been injected into the Topps website. Topps has since upgraded its website platform and taken steps to strengthen the security of their systems. ***The NTIC Cyber Center recommends customers who made a purchase through the Topps website during the affected timeframe monitor their accounts and immediately report any unauthorized activity to their financial institutions.***

Industry Report

Malwarebytes Labs 2019 State of Malware

Cybersecurity firm Malwarebytes released the 2019 State of Malware Report highlighting the increasing pace and sophistication in adversary tactics, techniques, and procedures (TTPs) observed over the past year, along with future predictions. Highlights from this report include the following:

- The number of Trojan and cryptominer incidents surpassed ransomware incidents.
- Breached records increased 133 percent in 2018 compared to the previous year.
- Preparators shifted from victimizing individuals to targeting organizations.
- Rogue apps and extensions evaded detection during security audits.

This report is available for free via the Malwarebytes website here.

Upcoming Webinars

10 Incredible Ways You Can Be Hacked through Email & How to Stop the Bad Guys

On Thursday, March 14th at 11:30 AM EDT, join Roger A. Grimes, KnowBe4's Data-Driven Defense Evangelist and security expert with over 30-years of experience, for a webinar where he will explore 10 ways hackers use social engineering to trick your users into revealing sensitive data or enabling malicious code to run. To register for this free webinar, visit govinfosecurity.com.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Whether tax season elicits delight or dread, one thing is for sure: it's prime time for scammers to perpetrate ***Internal Revenue Service (IRS) tax scams***. These scams may come in a variety of forms, all designed to separate you from your money. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Criminals, Nation-States Keep Hijacking BGP and DNS
Analytic Comment: Although fixes for security issues in the Border Gateway Protocol (BGP) and the Domain Name System (DNS) currently exist, organizations have been slow to adopt them fearing difficulty in implementation, an increase in costs, and a reduction in functionality. Other security solutions prove challenging as older hardware is unable to support modern protocols leaving the internet vulnerable to BGP and DNS hijacking. Until these issues are addressed, criminals and nation-state hackers will continue to abuse these vulnerabilities for financial and political gain.

Payroll Provider Gives Extortionists a Payday
Analytic Comment: The ransomware attack that victimized Apex Human Capital Management

highlights the importance of not only having a comprehensive data backup plan in place, but also keeping data backups stored offline. Additionally, it demonstrates that paying the ransom will not always solve the problem, as Apex suffered damaged directories and executable files after attempting to use the decryption key provided by the hacker. To reduce your risk of a crippling ransomware attack, we encourage you to download the NTIC Cyber Center Ransomware Mitigation Guide.

Patches and Updates

Cisco

Drupal

ICS Releases Security Updates for BIND

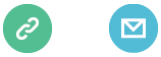
Moxa IKS, EDS

NVIDIA GPU Display Driver

OpenSSL

WinRAR

TLP:WHITE



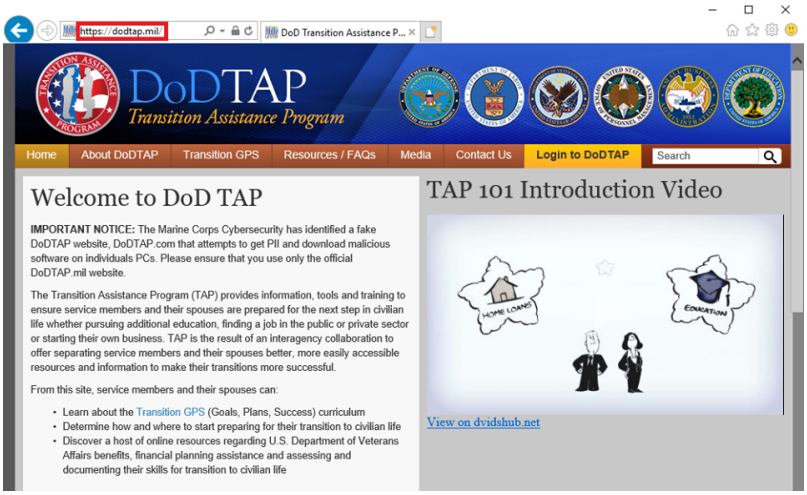
NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

March 7, 2019

National Capital Region Cyber Threat Spotlight



Malicious Website Spoofs US DoD Transition Assistance Program

The US Marine Corps and the US Air Force recently issued warnings of a phishing page that masquerades as a legitimate US Department of Defense Transition Assistance Program (DoDTAP) website. Using the technique of domain impersonation, hackers created a page that includes the program's proper acronym in the domain name but ends in *.com* instead of the *.mil* designation that would direct to the program's legitimate site. According to the US Marine Corps' assessment of the phony site, the *.com* page attempts to obtain personally identifiable information from visitors and initiates a download of malicious software onto victims' computers.

Phishing attacks that use techniques such as domain impersonation threaten public and private entities of all sizes. According to a recent Microsoft report, phishing continues to be the favorite attack method among threat actors seeking to steal sensitive data or distribute malware. The company further reports a staggering 250 percent increase in the number of phishing attacks

identified in 2018 alone.

For these reasons, the NTIC Cyber Center assesses with high confidence that phishing attacks will remain a persistent threat to individuals and organizations throughout the NCR and the United States. The NTIC Cyber Center recommends maintaining situational awareness of new and emerging phishing attempts and monitoring networks for indicators of compromise associated with malware campaigns.

US Department of Homeland Security Phone Numbers Used in Call Scam

The US Department of Homeland Security (DHS) warns that scammers recently used spoofed DHS phone numbers targeting individuals across the country to perpetrate scams. Altering caller ID information to make calls appear as if they originate from a legitimate DHS number, scammers impersonate law enforcement and immigration officials, solicit victims' personal information, and make phony threats of arrest to extort call recipients. DHS advises they will never use the affected phone numbers, which include the DHS HQ Operator number (202-282-8000) and DHS Civil Rights and Civil Liberties number (202-401-1474), to make calls of this nature. ***The NTIC Cyber Center urges phone users to remain vigilant when answering unexpected calls and to read our blog post on caller ID spoofing/neighbor number scams for tips on staying safe from these scams.***

Current and Emerging Cyber Threats

Ransomware GarrantyDecrypt Distributed Through Fake Proton Technologies Communications

A security researcher identified a new ransomware called GarrantyDecrypt being distributed through emails disguised as security notifications from Proton Technologies, creators of the popular ProtonMail email service. The ransomware's ransom note also masquerades as official Proton communications and demands $780 to decrypt the contents of afflicted hard drives. Contrary to the ransomware's clever name, there is currently no publicly available decryption tool available to unlock files impacted by GarrantyDecrypt. ***As such, the NTIC Cyber Center recommends***

maintaining regular system backups, disabling unnecessary remote desktop services, and keeping all hardware, software, devices, applications, and operating systems patched and up-to-date. In addition, users should avoid clicking on unknown links in websites or emails and restrain from downloading content from unknown or untrusted sources.

To reduce your risk of a ransomware infection, we encourage you to visit our website and download the NTIC Cyber Center Ransomware Mitigation Guide and the NTIC Cyber Center Guide for Cyber Incident Response Planning.

Phishing Campaign May Continue Target Banking and Financial Institutions

BleepingComputer warns of a phishing campaign dubbed "Behind the Grave" that recently attacked US and international hedge fund companies and may continue to target banking and financial institutions in the future. The campaign's perpetrators send phishing emails impersonating the financial research company Aksia to try to get banking and financial recipients to click on a phony link to a report. Instead of directing to the report, however, the URL forwards to a page that downloads a malicious payload onto victims' machines. ***On account of the increasing number of phishing attempts and the risks they continue to pose to institutions nationwide, the NTIC Cyber Center recommends email users refrain from clicking on links or opening attachments contained in messages from unknown or untrusted senders.***

Industry Report

Symantec 2019 Internet Security Threat Report

Symantec's 2019 Internet Security Threat Report takes a deep dive into insights from the world's largest civilian global intelligence network, revealing:

- Formjacking attacks skyrocketed, with an average of 4,800 websites compromised each month.
- Ransomware shifted targets from consumers to enterprises, where infections rose 12 percent.
- More than 70 million records stolen from poorly configured S3 buckets, a casualty of rapid cloud adoption.
- Supply chains remained a soft target with attacks ballooning by 78 percent.
- "Smart Speaker, get me a cyber attack" — IoT was a key entry point for targeted attacks; most IoT devices are vulnerable.

This report is available for free via the Symantec website here.

Upcoming Webinars

OSINT Webinar: Learn the Latest Email Investigation Techniques

On March 28th at 1:00 PM EDT, Michael Bazzell of IntelTechniques.com and host of *The Privacy, Security, and OSINT Show* podcast will present a free webinar on email investigation techniques. This live webinar will run for approximately one hour and will feature a Q&A session with the host. Webinar attendees will be limited to the first 2,000 registrants. To register, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Celebrity scams – also known as ***imposter scams***, ***impersonation scams***, and ***fan scams*** – are a type of social engineering scheme in which the perpetrator masquerades as a celebrity or popular social media personality, concealing his or her true intentions to elicit money or personal information or to

trick the victim into clicking on malicious links. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

One in Three Organizations Suffered Data Breaches Due to Mobile Devices

Analytic Comment: This report, consisting of survey results from 671 mobile device professionals, highlights challenges organizations face in maintaining mobile cybersecurity posture. Surveys show that mobile assets are not as protected compared to stationary systems and, though security risks are on the rise, companies are not keeping pace with defenses or implementing basic security protections. With the ever-changing nature of the cyber threat landscape, organizations must act quickly to protect against new threats, exploits, and vulnerabilities by raising awareness and implementing tested and comprehensive mitigation strategies.

40 Percent of Malicious URLs Were Found on Good Domains

Analytic Comment: Although cyber threat actors do register their own domains for malicious purposes such as phishing campaigns and to host malware, they understand that compromising existing domains can be more effective because these sites are less likely to be discovered and placed on blocklists. Additionally, websites that contain vulnerabilities and are not monitored for unauthorized changes make attractive targets, allowing hackers to hide malicious content for longer periods of time and use the reputation of established organizations to their benefit when attempting to trick victims into clicking on dangerous links. Therefore, websites and web servers should always be a consideration when conducting a cybersecurity risk assessment and creating an incident response plan.

Patches and Updates

Adobe ColdFusion

Cisco

Google Chrome

IDenticard PremiSys (Update A)

Kunbus PR100088 Modbus Gateway (Update B)

PSI GridConnect Telecontrol

Rockwell Automation RSLinx Classic

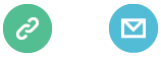
TLP:WHITE

otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.

We welcome your feedback. Please click here to complete a brief survey and let us know how we're doing.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

March 14, 2019

National Capital Region Cyber Threat Spotlight

US Army Criminal Investigation Command Warns of "Sextortion" Scams

The US Army Criminal Investigation Command recently profiled "sextortion" as a cybercrime of increasing prevalence targeting members of the military and other organizations. In these scams, cyber criminals approach victims through dating apps or social media platforms and seduce them into engaging in online sexual activities. The criminals record video of these encounters without the knowledge or consent of victims and then threaten to send the compromising content to victims' families or work associates if they do not receive payment. Criminals also pose as law enforcement entities, lawyers, or parents claiming to represent an underage victim and threaten fines or arrest if victims do not pay. In addition to demanding money, cyber extortionists also blackmail victims in exchange for sensitive information or access to military or government facilities.

The US Army reports that, to date, criminals have extorted more than 450 military members for a total of over $560,000 in payment and these numbers are expected to increase.

The NTIC Cyber Center assesses with high confidence that sextortion scams will remain a persistent threat to individuals and organizations throughout the NCR and the United States. We recommend remaining vigilant when corresponding with unknown entities on social media platforms, refraining from sending sensitive, personal, or compromising material to anyone, and

educating friends and relatives of the dangers associated with these types of scams. Anyone who believes they may have been targeted are encouraged to report the crime to a local law enforcement entity, the US Department of Homeland Security at assistance.victim@ice.dhs.gov, or the FBI's Internet Crime Complaint Center.

Current and Emerging Cyber Threats

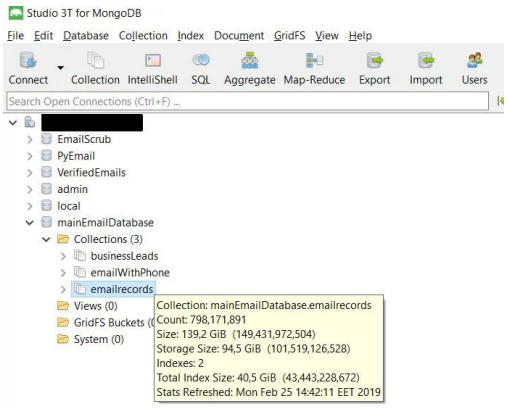
Trickbot Malware Distributed Through Fake Paychex Email

Human resources solutions company Paychex reports that a new email campaign disguised as a legitimate tax-related email delivers the Trickbot banking Trojan. Masquerading as legitimate correspondence, the email comes from the phony look-alike email address domain "@paychex.email," instead of "@paychex.com," and includes a macro-enabled Microsoft Word document attachment that, when opened and enabled, downloads the malware and infects systems. Most antivirus solutions do not flag or block Word documents with embedded macro code, as macro functionality is a legitimate operating feature of programs in the Microsoft Office Suite. ***Since exploiting this functionality to deliver malicious payloads is a common attack vector, the NTIC Cyber Center recommends users disable MS Office macros by default and avoid opening documents from untrusted sources. If you believe your Paychex accounts may have been compromised, contact Paychex support at 888-246-7500. We further recommend network administrators tighten macro security settings on all end user machines and monitor their networks for the associated IoCs listed here.***

SLUB Backdoor Malware Communicates Through GitHub and Slack

Researchers at Trend Micro Cyber Safety Solutions Team discovered SLUB, a backdoor that exploits Github, Slack and file.io cloud storage in Windows OS. SLUB can collect user and system information, execute commands and modify registry keys. Hackers first use GitHub gist snippets to execute commands then communicate through Slack from planted tokens and lastly funnel stolen files via file.io cloud storage. Slack and Github have since shut down violating accounts. ***The NTIC Cyber Center recommends updating Windows OS to the latest version, changing credentials, employing threat detection sandboxing, and monitoring external Slack applications.***

Data Breach Alert



2 Billion Records Leaked in Marketing Data Breach

Security researchers discovered a cache of roughly two billion email addresses in non-password protected databases hosted by marketing firm Verification. In some cases, in addition to email addresses, the data also included personally identifiable information including name, zip code, phone number, home address, gender, IP address, date of birth, social media details, credit score, and mortgage details of email account holders. ***Although there is no indication yet that threat actors accessed these records, the NTIC Cyber Center recommends remaining vigilant for increased phishing attempts perpetrated through email, social media, telephone, text message, and other avenues as a result of this data exposure.***

Upcoming Webinars

Outside the Network:
Protecting People and Customers Against Digital Threats

Social media, web domains and the deep and dark web pose areas of risk where companies are not directly in control of their communication security. Despite their value, these properties are often left unsecured against fraudulent activity. Since these are emerging threats, digital risks can be blind spots of focus for security teams. Join this webinar to learn about trends in digital risk including:

- Executive impersonations targeting your people on LinkedIn
- Social media protection on Instagram, Facebook and Twitter
- Credential threats on the dark web; physical threats to key locations
- Counterfeit domains in the retail space
- Visibility into the digital threat landscape
- How to protect against these threats

To register, click here.

Cybersecurity Event

DHS Cybersecurity and Innovation Showcase

The Department of Homeland Security Science and Technology Directorate will hold the 2019 Cybersecurity and Innovation Showcase March 18th through the 20th at the Washington Marriott Wardman Park Hotel in Washington, DC. The three-day event will introduce government, industry technology implementers, pilot and testing partners, investors, angel funders, and other potential market transition partners to more than 130 presentations, across more than 20 research areas, representing a combined $250 million of federally funded cybersecurity research and development. Featured thought-leaders include DHS Cybersecurity and Infrastructure Security Agency (CISA) Director Christopher Krebs, U.S. Customs and Border Protection Commissioner Kevin McAleenan, DHS S&T Senior Official Performing the Duties of the Under Secretary William N. Bryan, and cyberspace policy and cybersecurity expert Melissa Hathaway.

For more information, view the press release here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Grandparent scams are a type of fraud that targets senior citizens. Malicious actors pose as grandchildren in trouble and seek to exploit grandparents' emotional responses to steal money from unsuspecting elderly victims. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Rural Jackson County, GA Recovering from Ransomware Attack

Analytic Comment: Ransomware remains one of the most prevalent and destructive cyber threats facing organizations today. It is not enough to merely educate employees and monitor networks for indicators of compromise; organizations must have a comprehensive data backup plan in place along with a cyber incident response plan to mitigate the risk and reduce the operational downtime that could result from a ransomware infection. To help organizations in this effort, the NTIC Cyber Center provides a free Ransomware Mitigation Guide and a Guide for Cyber Incident Response Planning on our website here.

IoT Bill Would Require Gov't Use Devices Meeting Cybersecurity Standards

Analytic Comment: If passed, the Internet of Things (IoT) Cybersecurity Improvement Act of 2019 would reduce the risk that government agencies currently face resulting from vulnerable IoT devices within their network environments. Vulnerable and improperly secured IoT devices present one of the biggest challenges for cybersecurity teams as no minimum security requirements currently exist. This legislation would tackle these challenges by requiring NIST to create recommendations addressing the secure development, configuration, and management of IoT devices and restricting government agencies to only purchasing devices that are in compliance with these recommendations.

Patches and Updates

Adobe

Cisco

Cisco FXOS and NX-OS

Google Chrome

Microsoft Releases March 2019 Security Updates

MOXA

Siemens Desigo PXC (Update C)

Siemens Industrial Products (Update M)

Siemens SIMATIC PCS 7, SIMATIC WinCC, SIMATIC WinCC Runtime Professional, and SIMATIC NET PC Software (Update G)

Siemens SIMATIC S7 (Update A)

Siemens SINUMERIK Controllers (Update A)

Siemens SIPROTEC 4, SIPROTEC Compact, DIGSI 4, and EN100 Ethernet Module (Update C)

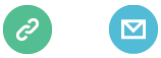
WIBU-SYSTEMS AG WibuKey Digital Rights Management (Update B)

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.

We welcome your feedback. Please click here to complete a brief survey and let us know how we're doing.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

March 21, 2019

National Capital Region Cyber Threat Spotlight

Montgomery County Department of Police Warns of Phone Scam

On Friday, the Montgomery County Department of Police issued a warning via Twitter about a phone scam targeting Maryland residents that spoofs the department's phone number and attempts to extort victims by threatening them with incarceration if they do not pay a fine. According to a WJLA-TV interview with Captain Tom Jordan, Director of the Public Information Division with Montgomery County Police Department, the scammers behind the ruse will initially call to inform the victim that there is an outstanding warrant or overdue fine that requires immediate payment and provide him or her with a phone number to call to complete the transaction. If the victim calls the number, he or she will be instructed to purchase Google Play or iTunes gift cards to pay the supposed fine. The Montgomery County Police Department reminds residents that no police agency will ever request payment in the form of gift cards. ***The NTIC Cyber Center encourages everyone to maintain awareness of this and other phone scams when answering a call from an unfamiliar number. Please share this information with friends and loved ones to reduce their risk of becoming a victim of financial fraud. For more information about other phone scams and social engineering schemes, please see our blog series titled "Securing Our Communities."***

Vulnerable Universal Plug and Play Devices Pose Risk to the NCR

Security researchers issued a warning regarding the large numbers of Internet of Things (IoT) devices exposed to the open Internet that are currently running outdated versions of Universal Plug and Play (UPnP) libraries. Devices such as routers that are enabled with outdated or unpatched UPnP libraries can easily be exploited, allowing threat actors to forward public ports to private devices, thereby exposing vulnerable devices located internally on networks to attack. For example, hackers recently abused this vulnerability to hijack Chromecast devices, Google Home devices, and smart TVs to promote a YouTube channel. ***The NTIC Cyber Center identified thousands of exposed devices in the National Capital Region that have UPnP enabled, including 195 in DC, 927 in Maryland, and 1,470 in Virginia. As such, we recommend users or owners of UPnP-enabled devices to keep firmware up-to-date and disable the UPnP feature when possible. Infected devices should be rebooted, reset to their original factory settings, or decommissioned.***

Announcement

Microsoft Ending Support for Windows 7

Microsoft announced that the company will no longer provide technical support or security updates for its Windows 7 operating system after January 14, 2020. Although PCs running Windows 7 will continue to work, users will face an increased risk of compromise resulting from unpatched vulnerabilities. ***The NTIC Cyber Center recommends Windows 7 users and administrators decommission all End-of-Life software and hardware as soon as possible and regularly audit network environments for unsupported systems. For additional guidance, please review the Microsoft End of Support FAQ.***

Current and Emerging Cyber Threats

Malicious Email Campaign Uses Boeing 737 MAX Concern to Deliver Malware

Cyber threat researchers discovered a malware campaign distributed through emails about the recent Ethiopian Airlines Boeing 737 crash. The email attachments, alleged to be documents forecasting future airline crashes, include a malicious JAR file that drops the H-Worm Remote Access Trojan (RAT) and the Adwind information-stealing Trojan upon downloading. Such attack campaigns that capitalize on tragic events are not uncommon and the Department of Homeland Security warns that attackers may start to leverage the recent events in New Zealand to perpetrate scams or malware campaigns. ***The NTIC Cyber Center recommends email users remain vigilant for such correspondence and refrain from clicking on links or opening attachments contained in messages from unknown or untrusted senders.***

Mirai Malware Identified on Popular Business IoT Devices

Palo Alto Unit 42 researchers identified a new variant of the Mirai botnet malware infecting popular IoT devices such as WePresent WiPG-1000 Wireless Presentation systems and LG Supersign TVs. Researchers believe threat actors compromised the devices using brute force attacks to bypass weak default password credentials. Previously in 2016, threat actors used this malware to leverage exploits in routers, network storage devices, network video recorders, and IP cameras and wage massive distributed denial-of-service (DDoS) attacks against specific targets. Now, researchers caution that the exploitation of these vulnerable presentation systems and smart TVs may indicate a shift in tactics toward leveraging IoT devices found in businesses and enterprise-scale networks to increase the size and power of botnets. ***The NTIC Cyber Center recommends users and administrators of WePresent WiPG-1000 Wireless Presentation systems and LG Supersign TVs change default passwords, monitor networks for suspicious activity, and ensure that all device firmware is patched and kept up-to-date.***

Active Phishing Campaigns Target Netflix and AMEX Users

The Windows Defender Security Intelligence team is warning Netflix customers and American Express account holders of two active and ongoing phishing campaigns designed to steal sensitive information such as account login credentials, financial account information, and Social Security numbers. Both campaigns send emails that attempt to trick recipients into thinking there is a problem with their accounts, encouraging them to open the included attachment or click on an embedded phishing link. ***The NTIC Cyber Center recommends never using a link or attachment in an email to visit a website that requires the input of your login credentials, even if you believe it is legitimate. Instead, visit the website directly by typing the address into the URL field of your web browser.***

Vulnerabilities

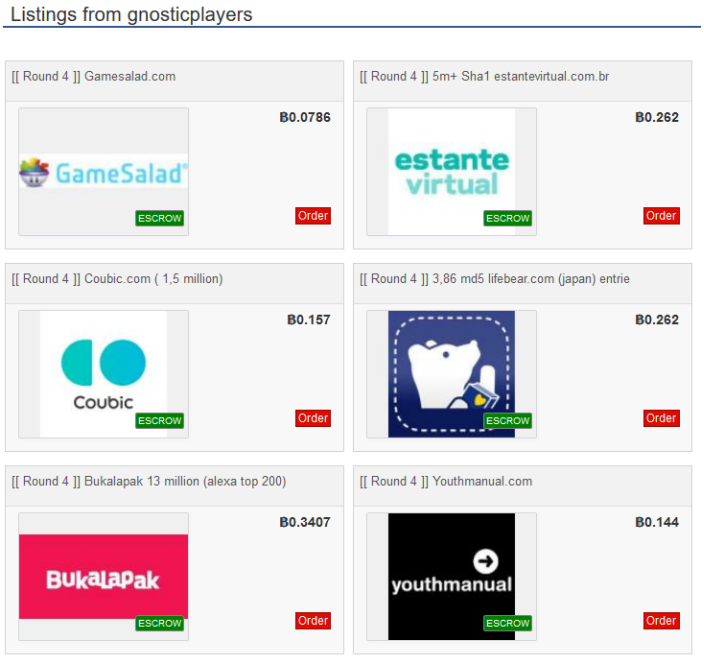
Botnet Exploited Vulnerabilities in Counter-Strike Game Client

Researchers at antivirus firm Dr. Web discovered the Belonard Trojan, a malware strain that contaminated 39 percent of Counter-Strike 1.6 game servers propagating unwanted ads, redirecting to other malicious servers, and delivering the Trojan itself. Hackers exploited the remote code execution vulnerabilities in the game client and altered it to promote the malicious game servers. The players' computers were infected once they joined the servers, creating a botnet designed to further propagate the infection. Dr. Web successfully coordinated efforts with a Russian domain registrar to dismantle the botnet's infrastructure and prevent the malware from spreading. Although Counter-Strike 1.6 players are currently no longer at risk of connecting to the Belonard botnet, the vulnerabilities in the game client remain, potentially allowing a new campaign to infect systems. There is currently no patch or workaround available. ***The NTIC Cyber Center recommends Counter-Strike players keep antivirus software on gaming systems updated with the latest virus definitions, monitor systems for unusual and suspicious activity, and to update game clients if and when a patch becomes available.***

WinRAR Vulnerability Prevalent Due to a Lack of Auto-Update Feature

McAfee Labs warns that hackers continue to actively exploit a critical vulnerability that allows them to install malware onto victims' machines using an infected RAR file. When a vulnerable WinRAR utility tool is used to extract, decompress, or "unzip" a RAR file bundled with malware, a malicious payload installs and runs after a victim restarts their machine. Of note, this WinRAR vulnerability affects every version of the software released over the past 19 years. ***Since WinRAR does not automatically install updates and remains one of the most popular compression/archive tools with over 500 million users, the NTIC Cyber Center strongly advises WinRAR users manually install the latest version of the software (5.70 beta 1) as soon as possible and avoid opening attachments from unknown or untrusted sources.***

Data Breach Alert



ZDNet reports that the same hacker responsible for posting three sets of stolen database credentials to a Dark Web marketplace in February of this year recently published a fourth set that contains compromised data from six new companies including GameSalad, Estante Virtual, Bukalapak, and YouthManual, among others. This data set reportedly totals 26.42 million user records and includes information such as names, email addresses, usernames, passwords, addresses, phone numbers, and IP addresses. ***The NTIC Cyber Center recommends using lengthy and complex passwords that are unique to every online account to reduce the risk of further compromise in the event of a data breach. Additionally, we recommend enabling two-factor authentication as an additional security measure on any account that offers it. Users of these and any breached site or service are encouraged to reset their passwords as soon as possible and monitor their accounts for suspicious activity.***

Upcoming Webinars

INTSIGHTS

CYBERSECURITY

Lock Down Leaked Credentials Before They're Exploited by Hackers

Since leaked credentials are one of the easiest ways for hackers to access corporate systems and steal sensitive data, companies must vigilantly monitor this risk online. This task becomes incredibly difficult with threat actors publishing and exchanging massive credential databases (like the recent Collection #1 and Collection #2-5). Learn how to quickly identify, process, and validate

whether or not leaked credentials are active and could be used to access corporate systems. In this webinar, IntSights will share the following:

- Which sources to monitor and identify new leaked credentials
- How to quickly validate if credentials are new or recycled
- How to automate the credential lockdown process before hackers can use them

To register for this free webinar on Wednesday, March 27, from 1:00pm to 2:00pm EDT, click here.

Recording of Chinese Malicious Cyber Activity Briefing Now Available

The Cybersecurity and Infrastructure Security Agency (CISA) has posted the February 14, 2019 Awareness Briefing on Chinese Malicious Cyber Activity. This webinar provides background and mitigation techniques on Chinese malicious cyber activity targeting managed service providers (MSPs). The NTIC Cyber Center encourages readers to view the February 14, 2019 Awareness Briefing on Chinese Malicious Cyber Activity and review the online resource on Chinese Malicious Cyber Activity.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Utility scams are fraudulent acts conducted by profit-motivated criminals who misrepresent themselves as utility company employees to steal money or valuables from victims. Sometimes, these criminals will call victims and attempt to convince them that they have an overdue utility bill

requiring immediate payment. Other times, perpetrators may arrive in person at the victim's door wearing a utility company uniform and demand entry into the victim's home. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Why Phone Numbers Stink as Identity Proof

Analytic Comment: Although securing accounts with SMS-based two-factor authentication (2FA) is better than not implementing 2FA at all, SMS-based 2FA is not foolproof and can be vulnerable to SIM swapping attacks that hijack victims' phone numbers. If malicious actors can successfully trick an account holder into clicking a malware-laden link or the mobile phone carrier representative into porting a targeted phone number to a new device, associated accounts with SMS-based 2FA enabled can be at risk of compromise. If accounts offer 2FA options beyond SMS such as a hardware authentication device or an authentication application, consider implementing them for added security.

Cyber Threats Are Emerging Faster Than DHS Can Address Them, Secretary Says

Analytic Comment: One of the largest challenges facing both public and private sector organizations today is the ability to properly identify and protect against rapidly emerging and evolving cyber threats. Additionally, the frequency of cyber attacks keeps organizations on the defensive, preventing them from devoting the time and resources necessary to take a more proactive approach to cybersecurity. However, organizations of every size can take a step towards bridging that gap and reducing their risk by tightening network security controls, enforcing an enterprise-wide adoption of best practices, and engaging in cyber threat intelligence and indicator sharing initiatives.

Patches and Updates

AVEVA InduSoft Web Studio and InTouch Edge HMI

Cisco

Columbia Weather Systems MicroServer

Drupal

Gemalto Sentinel UltraPro

Intel

Microsoft Azure Linux Agent

Mozilla Firefox

PEPPERL+FUCHS WirelessHART-Gateways

VMware

WordPress

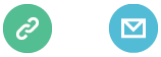
TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.

We welcome your feedback. Please click here to complete a brief survey and let us know how we're doing.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

March 28, 2019

National Capital Region Cyber Threat Spotlight

Chinese Intelligence Agencies Target US Government Employees via LinkedIn Profiles

According to a recent US Department of Justice announcement, a former Defense Intelligence Agency officer pleaded guilty on March 15, 2019 to attempting to transmit US national defense information to the People's Republic of China. Within the felony complaint, the FBI stated that the suspect collected information from his colleagues' LinkedIn profile pages. Additionally, a US counter-intelligence chief revealed to Reuters in August that Chinese intelligence agencies heavily leverage LinkedIn to recruit potential American spies. Targets of these espionage campaigns often post detailed work histories on their social media profiles, including security clearance statuses and classified intelligence units that the US government does not publicly acknowledge. Chinese nation-state actors posing as job recruiters or professional colleagues then use this information to establish contact with their targets and attempt to elicit additional sensitive and personal information from them. ***The NTIC Cyber Center recommends LinkedIn users who serve in US government roles limit the amount of professional information they share online through this and other social media platforms. We also recommend all social media users refrain from sharing sensitive, personal information online and with people they do not know.***

Current and Emerging Cyber Threats

Criminals Selling GlitchPOS Malware on Hacking Forums

Researchers at Cisco's Talos Security Intelligence and Research Group discovered GlitchPOS, a point-of-sale (PoS) malware variant that steals payment card data from online and physical retailers. GlitchPOS pilfers sensitive data from an infected system's memory using a VisualBasic malware packer disguised as a cat game. GlitchPOS is for sale on illicit forums for $250 and includes a video tutorial, enabling criminals who lack technical skills to easily conduct malware campaigns and create PoS botnets. ***The NTIC Cyber Center recommends network administrators review the Cisco Talos report linked above and block the associated Indicators of Compromise (IoCs). We also recommend all payment card users to frequently review their account statements and immediately notify their financial institutions of any unauthorized activity.***

Phishing Campaign Spoofs Entertainment Industry Websites

Researchers at ThreatConnect discovered a phishing campaign consisting of approximately 380 domains, subdomains, and IP addresses designed to spoof organizations associated with the entertainment industry such as Sony, Marvel Studios, and various public relations firms. These websites are designed to harvest login credentials for various accounts, including Microsoft Outlook. Notable tactics used in this campaign include utilizing common naming conventions across multiple domains and subdomains along with reusing SSL certificates. ***The NTIC Cyber Center recommends carefully scrutinizing websites that require the input of login credentials and refraining from clicking on links from unknown or untrusted sources. Enable two-factor authentication on any account that offers it to reduce the risk of compromise resulting from stolen account credentials.***

Phishing Campaign Spoofs the CDC to Deliver GandCrab Ransomware

Researchers discovered a new malicious email campaign that impersonates the Centers for Disease Control and Prevention (CDC) and attempts to infect victims with the GandCrab v5.2 ransomware variant. The email subject line "Flu pandemic warning" features fraudulent CDC branding along with a Word document attachment labeled *Flu pandemic warning.doc*. Users who open the attachment are prompted to enable macros designed to download and install the newest version of GandCrab ransomware, a variant that cannot be decrypted for free at this time. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as alerts from the CDC, avoid opening unexpected emails, and refrain from clicking on links and opening attachments from unknown or untrusted sources. If you receive this or a similar email in your work email account, notify your IT security team immediately.***

Vulnerabilities

Misconfigured Box Accounts Discovered Leaking Sensitive Data

Researchers at Adversis identified publicly accessible files and folders belonging to over 90 companies on the enterprise storage platform Box. Although the default setting for files and folders stored within the platform is "private", users can share content by sending intended recipients a link to a file. Researchers discovered these sharable links using an open-source scanning tool and combined company names and wildcard searches to identify and enumerate Box accounts. Information viewable within some of the accessible data includes customer names, phone numbers, bank account numbers, social security numbers, passwords, email addresses, passwords, and other information. Companies impacted by the breach include, but are not limited to, Amadeus, Apple, Discovery, Edelman, Herbalife, Opportunity International, Schneider Electric, PointCare, and United Tissue Network. ***The NTIC Cyber Center recommends Box users and administrators reconfigure default access for shared links to "people in your company" to reduce the threat of accidental data exposure.***

Medtronic Conexus Radio Frequency Telemetry Protocol

The Department of Homeland Security (DHS) recently issued an advisory warning of vulnerabilities affecting Medtronic cardiac devices that utilize the Conexus telemetry protocol. If successfully exploited, the vulnerabilities could allow attackers to interfere with, generate, modify, or intercept RF communications to capture device data or impact device functionality. ***As there are currently no patches available, the NTIC Cyber Center encourages users of Medtronic cardiac devices to consult the list of affected equipment and reference the mitigation strategies outlined in the DHS advisory until updates are deployed.***

Data Breach Alert

Security researchers at RiskIQ believe threat actors conducted credit card-skimming attacks to steal customer payment information from websites of retailers MyPillow and AmeriSleep. By injecting malicious scripts into companies' e-commerce sites—an attack technique dubbed "MageCart"—attackers were able to siphon customer data and payment information directly from the companies' checkout pages. RiskIQ believes affected customers may include those who made purchases through MyPillow's online platform in October or November 2018 or through AmeriSleep' online platform

from April through October 2017 and from January to March 2019. ***The NTIC Cyber Center recommends customers who made purchases via these websites during the affected time frames monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.***

Upcoming Webinars

Educate and Train Your Cybersecurity Workforce

The Cybersecurity and Infrastructure Security Agency (CISA) will be hosting a webinar on Thursday, April 4, 2019 at 1:00pm to discuss cybersecurity training, education, and workforce programs that are available to state, local, tribal, and territorial (SLTT) governments, including the Federal Virtual Training Environment (FedVTE). More information about FedVTE is available here. To join the webinar on its scheduled date and time, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Chinese phone scams are automated telephone calls that spoof official Chinese embassy or consular communications to extort money from Chinese speakers. Criminals direct these calls to phone customers with Chinese last names and to random people in locations with large populations of Mandarin speakers. Although these scammers are frequently located in China, their calls target people all over the world. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

70 Percent of Ransomware Attacks Targeted SMBs, BEC Attacks Increased by 130 Percent
Analytic Comment: Ransomware attacks continue to target predominantly small to medium-sized businesses with healthcare, professional services, and financial industries ranking among the most impacted sectors. Organizations with insecure remote desktop protocol (RDP) services, open RDP ports, and weak password credentials face a higher risk of compromise through brute-force entry attacks. Other cyber threats impacting organizations with increasing frequency include malware or ransomware distributed through sextortion emails and payment fraud perpetrated through credential theft and BEC campaigns, the latter of which increased by 133 percent from 2017 to 2018. The report's analysis underscores the value of educating staff about cyber risks as a complement to other IT security measures to protect organizations and individuals from current and emerging threats.

The 7 Biggest Cybersecurity Threats in an IoT World
Analytic Comment: The rapid and widespread adoption of Internet of Things (IoT) devices creates challenges for individuals and organizations attempting to secure their data and networks. As many IoT devices require little to no modification beyond the initial set-up, they are easily forgotten and can introduce vulnerabilities into a network. As hackers have heavily targeted IoT devices in recent years, it is crucial for administrators to regularly audit their networks to identify and track devices and to monitor network traffic for suspicious activity.

Patches and Updates

Apple

ASUS Live Update

Cisco

ENTTEC Lighting Controllers

Medtronic Conexus Radio Frequency Telemetry Protocol

Mozilla Firefox

Mozilla Thunderbird

NVIDIA

Phoenix Contact RAD-80211-XD

Siemens SCALANCE X

TLP:WHITE

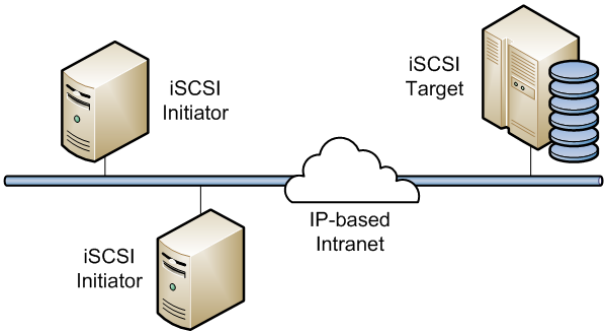
NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

April 4, 2019

National Capital Region Cyber Threat Spotlight



Poorly Configured iSCSI Storage Clusters Pose Risk to Networks

ZDNet reports that poorly configured security settings of exposed Internet Small Computer Systems Interface (iSCSI) storage clusters pose a high risk to networks as they create backdoors that could allow malicious actors to gain unauthorized access to networks. iSCSI is a protocol used for linking data storage facilities and to connect workstations and servers to data storage devices such as disk storage arrays and network-attached storage (NAS) devices. It is often used to facilitate the transfer and management of data across local area networks, wide area networks, and the Internet. If properly configured, this protocol will require the authentication of connections via a username and password; however, iSCSI instances configured without login credentials could allow an unauthorized user to gain access to storage devices, modify or delete data, format drives, and manually distribute malware and create backdoors on associated networks. Using Shodan, the Internet of Things search engine, NTIC analysts determined that there are approximately 160 iSCSI instances within the National Capital Region that do not authenticate connections. ***The NTIC Cyber Center strongly recommends users and administrators of network-attached data storage devices first limit their exposure to the Internet, if possible, and secure each instance with a username and password.***

Current and Emerging Cyber Threats

Android Trojan Steals Funds from Global Banks and Cryptowallets

Researchers at cybersecurity firm Group-IB recently discovered Gustuff, an Android banking Trojan that steals funds from international banks and 32 cryptocurrency Android apps. It spreads by collecting contact lists from compromised Android devices and sending hyperlinked APK installation files embedded in text messages. Once infected, Gustuff can read and modify text fields in targeted apps, send illegitimate financial transactions, and exfiltrate data. Gustuff has been active for approximately a year and its developer periodically updates its capabilities. Gustuff currently can display fake push notifications, transfer files to command and control servers, and disable Android's anti-malware guard. ***The NTIC Cyber Center recommends mobile device users refrain from clicking on links from unknown or untrusted sources and scrutinizing unexpected links sent via text message by known contacts. Enable two-factor authentication on any account that offers it to reduce the risk of compromise resulting from stolen login credentials. Users who suspect that their devices have been compromised should perform a factory reset and restore devices to manufacturer default settings as well as change their account credentials and monitor accounts for suspicious or unauthorized activity.***

Unam3d R@nsomware Demands Amazon Gift Card Payment

According to researchers, a new ransomware variant, dubbed "Unam3d R@nsomware," locks victims' files in a password-protected RAR file and demands ransom payments in the form of $50 Amazon gift cards. The threat actor behind the ransomware campaign has already sent approximately 30,000 emails disguised as an Adobe Flash Player update notice that prompts victims to click on a malicious link. Once installed, Unam3d R@nsomware locks files in RAR archives and displays a ransom note with instructions that include how to contact the ransomware developer "Uname3d" via the Discord messaging platform and how to submit the ransom payment. Victims of this ransomware campaign can contact researchers at BleepingComputer and possibly recover their files for free. ***The NTIC Cyber Center recommends users remain vigilant for ransomware attempts disguised as alerts from Adobe, avoid opening unexpected emails, and refrain from clicking on links and opening attachments from unknown or untrusted sources. If you receive this or a similar email in your work email account, notify your IT security team immediately.***

To reduce your risk of a ransomware infection, we encourage you to visit our website and download the NTIC Cyber Center Ransomware Mitigation Guide.

Joomla and WordPress are Used and Abused

A researcher from cloud security platform Zscaler discovered that popular content management systems Joomla and WordPress (versions 4.8.9 to 5.1.1) are being used by cyber threat actors to host malicious content on over 500 websites. These actors exploit a well-known hidden directory present on HTTPS websites and use it to host backdoors, redirectors, landing pages for phishing sites, and ransomware. Because the compromised sites use SSL certificates issued by reputable and well-known certificate authorities, visitors could easily be tricked into thinking the website is legitimate, as HTTPS is displayed in the URL field. Zscaler attributes the malicious content to unpatched plugins, themes, extensions, and server-side software. ***The NTIC Cyber Center recommends website administrators regularly audit their sites for outdated and unpatched plugins, themes, and extensions and either apply the appropriate updates or remove them. We also recommend regularly checking website directories for unauthorized content. Network administrators are encouraged to review Zscaler's report and block the associated Indicators of Compromise to prevent end users from accidentally visiting these sites.***

Phishing Campaign Hits Verizon a Third Time

Researchers at cybersecurity firm Lookout discovered a mobile device phishing campaign targeting Verizon customers. The campaign appears in waves, first emerging in November, then February and, most recently, March. The emails associated with this campaign masquerade as notifications from Verizon Customer Support that attempt to elicit Verizon account credentials. While the phishing pages may look suspicious on desktop platforms, they appear deceptively authentic on mobile devices. Recipients can be easily fooled as the perpetrator registered numerous domains and subdomains mimicking those from Verizon. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as alerts from Verizon Customer Support, avoid opening unexpected emails, and refrain from clicking on links from unknown or untrusted sources. We also recommend network administrators review Lookout's report and block the associated IoCs.***

Vulnerabilities

TP-Link SR20 Smart Home Router Vulnerability Grants Backdoor Access

A zero-day vulnerability in the TP-Link SR20 Smart Home Router and Hub may allow potential attackers to execute arbitrary commands and control the devices with backdoor access. Although a security researcher claims to have submitted information on the vulnerability to TP Link over 90 days ago, the company allegedly has not taken any steps to issue a patch, as the last firmware update for the device was released in June 2018. ***As the vulnerability currently remains exploitable, the NTIC Cyber Center recommends discontinuing the use of the SR20 Smart Home Router and Hub and removing the device from within your environment until TP-Link issues a patch resolving the issue.***

Microsoft Internet Explorer and Edge Vulnerable to Cross-Site Scripting Attacks

Two unpatched zero-day vulnerabilities in Microsoft Internet Explorer and Edge browsers may allow a remote attacker to bypass same-origin policy and perform universal cross-site scripting (UXSS) attacks against any domain visited through the browsers. The vulnerabilities would permit a malicious website to request data from sites other than those that share the same origin domain, granting attackers access to login sessions and cookies from other sites visited on the browsers. ***As the vulnerabilities currently remain exploitable, the NTIC Cyber Center recommends discontinuing the use of Internet Explorer and Edge in favor of more secure browsers until Microsoft issues a patch resolving the issue. We also recommend always running reputable antivirus software and keeping it up to date with the latest virus definitions.***

Data Breach Alert

Hospitality firm Earl Enterprises released a customer notice disclosing a data breach that occurred from May 23, 2018 to March 18, 2019 at company-owned restaurants throughout the United States. The firm believes that malware installed on point-of-sale systems allowed cyber criminals to steal customer credit and debit card numbers, expiration dates, and cardholder names at certain locations of Buca di Beppo, Earl of Sandwich, Planet Hollywood, Chicken Guy!, Mixology, and Tequila Taqueria restaurants. Customers who paid for online orders through third-party applications or platforms are not believed to have been affected by this incident. Within the NCR, this data breach may have affected customers of Buca di Beppo at 122 Kentlands Boulevard, Gaithersburg, MD. Other affected establishments can be identified here. ***The NTIC Cyber Center recommends that customers who made purchases at the affected restaurants during the ten-month period monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.***

Security researchers indicate that two third-party apps stored over 540 million Facebook user records in publicly-accessible Amazon S3 databases. The first set of records, which includes the plain text app passwords, account names, user IDs, interests, relationship status, comments, likes, reactions, and other details belonging to over 540 million users, appeared in a database owned by Mexico-based media company Cultura Colectiva. The second collection, hosted in a database belonging to the now-defunct app "At the Pool," comprises names, app passwords, interests, and other data points of 22,000 Facebook users. Though Facebook is not directly responsible for this leak of user credentials, news of this breach follows Facebook's recent admission of having stored hundreds of millions of user passwords for Facebook, Facebook Lite, and Instagram in plaintext format. ***As a result of these instances of massive public exposure of Facebook user credentials, the NTIC Cyber Center recommends Facebook users change their account passwords, enable two-factor authentication on their accounts, and avoid reusing passwords across multiple platforms.***

Upcoming Webinars

Anatomy of Container Attack Vectors and Mitigations Webinar

Join Data Breach Today on an investigative journey to explore popular attack vectors that have been used to breach container-based environments, provide best practices and tools to mitigate them, and discuss associated business risks.

Register for this webinar and learn about:

- Key known vulnerabilities affecting the container ecosystem (Docker, Kubernetes, RunC);
- Common configuration mistakes and human errors leading to attacks;
- Attack vectors that include crypto-currency mining, data exfiltration, and denial of service;

- Key steps and tools, including open source tools, to mitigate each attack, from the build stage through to run-time detection and response.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Social Security number (SSN) suspension scams are a type of government imposter scam in which perpetrators identify themselves as representatives of the Social Security Administration and attempt to convince victims that their SSNs have been suspended due to suspicious or criminal activity. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

The Latest Dark Web Cyber-Criminal Trend: Selling Children's Personal Data
Analytic Comment: Cyber criminals increasingly seek to acquire stolen credentials belonging to children to commit identity theft and fraud. In Dark Web marketplaces, “child fullz,” which are full kits of information containing a child’s name, date of birth, address, and Social Security number, are more valuable than similar credential collections that contain adult data. Because children rarely have any credit history at all, the fresh nature of their credentials makes their information extremely appealing to cyber criminals who seek to use it to file for fraudulent child tax credits or to set up new credit profiles and make purchases or apply for loans in children’s names. The state of cybercrime and identity theft perpetrated against children highlights shortcomings in the process of verifying credit applicants’ identities and underscores the importance of protecting children’s credit by activating credit freezes or conducting regular credit checks.

Only 10 Percent of Tech Companies Protected From Phishing by DMARC Enforcement

Analytic Comment: According to a study profiling global technology companies' use of email authentication protocols, only 10.5 percent of companies surveyed have properly-implemented Domain-based Message Authentication, Reporting, and Conformance (DMARC) technology in place to block messages identified as email spoofing-based phishing attacks. Properly configured DMARC standards allow enterprises to reject or otherwise alter the handling of phishing messages that fail authentication checks. As phishing attacks remain one of the most widespread and persistent cyber threats targeting individuals and organizations, the Department of Homeland Security advises administrators to set a DMARC enforcement policy of "reject" to provide the strongest protection against spoofed email and ensure that unauthenticated messages are rejected at the mail server before delivery.

Patches and Updates

Advantech WebAccess/SCADA

Apache

Cisco

Magento

Microsoft

NVIDIA

Rockwell Automation PowerFlex 525 AC Drives

VMware

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

April 11, 2019

National Capital Region Cyber Threat Spotlight

DHS and FBI Release Malware Analysis Report on North Korean Trojan HOPLIGHT

The US Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) released a joint Malware Analysis Report (MAR) yesterday detailing a newly discovered malware variant, dubbed HOPLIGHT, used by the North Korean government in HIDDEN COBRA cyber operations. The MAR includes the descriptions and analysis of nine malicious executable files associated with this threat, as well as suggested response actions and recommended mitigation techniques. Users and administrators are encouraged to flag malicious activity associated with HOPLIGHT and report it to the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI Cyber Watch (CyWatch), giving the activity the highest priority for mitigation. The NTIC Cyber Center recommends all network administrators review Malware Analysis Report (AR19-100A) and monitor networks for the associated indicators of compromise (IoCs). Additional information about HIDDEN COBRA is available on us-cert.gov.

Northern Virginia and Maryland Warn Residents about Scams Impacting the Region

Authorities in Northern Virginia and Maryland are warning residents about phone scams targeting aging residents and duping them out of millions of dollars. Phone scams are on the rise and, according to the Senate Special Committee on Aging, they are responsible for draining $42 million from victims over a recent 15-month period. Perpetrators of these scams use sophisticated social engineering techniques to trick victims into forking over their hard-earned money and it can be difficult to convince victims they have been fooled until it is too late. This is why the NTIC Cyber Center encourages all of our members to educate their friends and loved ones about common scams impacting the NCR so they can be armed with the knowledge they need to protect themselves. For more information on prevalent scams impacting the NCR, please visit our website and read our Securing Our Communities series where we explain how these scams work and how to avoid becoming a victim.

Current and Emerging Cyber Threats

Tax-Themed Spam Continues to Distribute TrickBot Malware

Researchers at IBM SecurityIntelligence warn of the prevalence of tax-themed malware attacks targeting individuals and businesses this tax season. According to their research, many recent malware campaigns spoof official correspondence from well-known accounting, tax, or payroll companies such as Paychex and ADP and include malicious Microsoft Excel documents enabled carrying the banking Trojan, TrickBot. TrickBot, which is often delivered through macro-enabled attachments, remains an extremely destructive malware that allows attackers to steal banking information and exfiltrate remote desktop and other Windows credentials. ***The NTIC Cyber Center recommends users remain vigilant for malspam disguised as official tax correspondence, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. If you receive an email that you suspect may be malicious, notify your IT security team immediately.***

Malicious PNG Image Files May Contain Lokibot Trojan

Trustwave SpiderLabs researchers identified a malspam campaign that stealthily delivers LokiBot malware embedded in PNG image files. Lokibot, a Trojan used to steal user information via tainted endpoints, is compressed and attached in a *.zipx* archive file and then altered to mimic PNG file signatures to bypass email security gateways. Perpetrators further obfuscate Lokibot through forged JPG icons. The victim is compromised when they unzip the *.zipx* file and extract and launch the executable file contained within it. Lokibot is for sale on illicit forums for $300 and, while extensively used, it's not commonly found within a PNG file. ***The NTIC Cyber Center recommends never opening attachments or enabling executables in files received from unexpected or***

unsolicited emails. If you believe you have been targeted by this campaign or infected with the Lokibot Trojan, notify your organization's IT security team immediately.

Researchers Identify New "Xwo" Bot Scanner

AT&T Alien Labs researchers observed Xwo, a bot scanner reconnaissance tool likely used for malicious purposes to aid in future attacks. Written in Python, Xwo continually scans the Internet for available and exposed web services that use default credentials and then sends the information back to command and control (C2) servers to use in subsequent attacks. Although Xwo is not categorized as malware, AT&T Alien Labs observed similarities to Xbash malware and MongoLock ransomware as they share C2 infrastructure and use similar code. So far, Xwo is known to collect information from the following services: FTP, MySQL, PostgreSQL, MongoDB, Redis, Memcached, SVN and Git paths, Tomcat, PhPMyAdmin, RealVNC, and RSYNC. ***The NTIC Cyber Center recommends network administrators review the AT&T Alien Labs report linked above and block the associated IoCs. We also recommend changing all default credentials associated with these and other web services.***

Newsletter Subscription Services Used to Disseminate Phishing Links

Security researchers identified phishing links contained in official newsletter subscription messages sent from major international companies. Researchers indicate that hackers have appropriated subscription services to register targets on newsletter distribution lists using phishing page URLs instead of email recipients' real names in registration forms. As a result, recipients of these emails receive a confirmation email originating from a known company's official newsletter subscription service containing an embedded link to a phishing website. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as official newsletter subscription notifications, avoid opening unexpected emails, and refrain from clicking on links from unknown or untrusted sources. If you suspect you have received a phishing email disguised as such correspondence in your work email account, notify your IT security team immediately.***

New Email Extortion Campaign Threatens Ransomware and DDoS Attacks

BleepingComputer reports the discovery of a new email-based extortion campaign that tries to trick recipients into thinking their computers were hacked and accuses them of hiding their taxes from the US Internal Revenue Service or other governmental tax authority. The email contains a payment demand of two Bitcoin and threatens to notify the "Tax Department," launch a distributed denial-of-service (DDoS) attack, and infect victims with WannaCry ransomware if they do not pay. The campaign also threatens to increase the extortion amount by one Bitcoin for each day the recipient refuses to submit payment. According to email samples, it appears that this campaign targets

companies rather than individuals. ***Although there are currently no reports of recipients experiencing a DDoS or ransomware attack as a result of non-payment, the NTIC Cyber Center recommends end users notify their IT security teams immediately if they receive this or any other extortion email. We also encourage recipients to report it to their local police department and the FBI's Internet Crime Complaint Center.***

Vulnerabilities

Cisco RV320 and RV325 Small Business Routers

Cisco recently patched vulnerabilities CVE-2019-1652 & CVE-2019-1653 in Cisco RV320 and RV325 routers that would allow perpetrators, without a password, to view device configuration details, modify data, and execute commands. Upon further inspection, the same routers revealed two more vulnerabilities, CVE-2019-1827 and CVE-2019-1829. CVE-2019-1827 can allow hackers to execute arbitrary code or access browser-based information potentially leaving victims vulnerable to a cross-site scripting (XSS) attack against a user. CVE-2019-1829 can allow hackers to access administrative credentials. There is currently no workaround for CVE-2019-1827 & CVE-2019-1829. ***The NTIC Cyber Center recommends applying the new Cisco patch 1.4.2.22 for the RV320 and RV325 routers to remediate CVE-2019-1652 and CVE-2019-1653, reset affected login credentials, and properly segment their network to isolate the system from external and unauthorized access.***

Verizon Fios Quantum Gateway Routers

Security researchers at Tenable identified vulnerabilities in Verizon Fios Quantum Gateway routers that could grant attackers full control of a wireless home network and access to connected network devices. By leveraging vulnerabilities in login password parameters, attackers can execute a script on the router's web portal interface, change router security settings, and obtain root privilege on the device. Although Verizon issued a patch, the company warns that since not all customers received the automatic update, users of the device may have to upgrade the router's firmware manually to obtain protection. ***The NTIC Cyber Center recommends users of the Verizon Fios Quantum Gateway router ensure that device firmware is updated to the latest version (02.02.00.13) and monitor for any indications of suspicious activity on their network.***

Data Breach Alert

AeroGrow

Gardening system retailer AeroGrow released a customer notice disclosing a data breach that occurred from October 29, 2018 to March 4, 2019. AeroGrow believes that card-skimming malware residing on its website allowed cyber criminals to siphon customer information during checkout such as payment card numbers, expiration dates, and security codes. ***The NTIC Cyber Center recommends that customers who made purchases through AeroGrow's eCommerce platform during the affected time frame monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.***

PIE FIVE PIZZA

craft pizza • so fresh • so fast

Restaurant chain Pie Five Pizza released a customer notice disclosing a data breach that occurred from September 6, 2018 to December 2, 2018 at numerous restaurant locations throughout the United States. The company believes that malware installed on payment processing systems granted attackers access to payment card information including customer names, card numbers, card expiration dates, and card verification codes. A list of affected Pie Five Pizza establishments is available here. ***The NTIC Cyber Center recommends that customers who made purchases at the affected restaurants during the three-month period monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.***

Upcoming Webinars

KnowBe4

Live Webinar: 12 Ways to Defeat Two-Factor Authentication

Join Roger A. Grimes, KnowBe4's Data-Driven Defense Evangelist, and security expert with over 30-years experience, will explore 12 ways hackers can and do get around your favorite 2FA solution. The webinar includes a (pre-filmed) hacking demo by KnowBe4's Chief Hacking Officer Kevin Mitnick, and real-life successful examples of every attack type. It will end by telling you how to better defend your 2FA solution so that you get maximum benefit and security.

You'll learn about the good and bad of 2FA and become a better computer security defender in the process, including:

- 12 ways hackers get around two-factor authentication
- How to defend your two-factor authentication solution
- The role humans play in a blended-defense strategy

To register for this free webinar on Tuesday, April 16, from 11:30 am to 12:30pm ET, click here.

Communications Exploitation for Investigators and Analysts Webinar

Presenter Darryl Valinchus brings over 29 years of experience from the NYPD where he spearheaded the creation and development of the Intelligence Bureau's Analytical Programs Unit. He has testified over 20 times in Federal and State court as an expert in the interpretation, understanding and mapping of cellular communications information.

This webinar will cover the different types of communication, the information available for these types of communication, and how you can use it in your investigations to build your case.

This webinar is for active law enforcement and military personnel - only requests using official agency emails will be accepted.

To register for this free webinar on Wednesday, April 24, from 12:00pm to 1:00 pm ET, click here.

To Bounty or Not To Bounty: Why Priceline Works with Hackers to Reduce Risk

In this webinar, Matthew Southworth, CISO of Priceline, will share why his organization works with hackers to reduce risk, what it means to lead the travel and booking industry when it comes to security, and how to make the most out of a hacker-powered program.

Topics include:

- Debating a collaborative and open approach to security
- Prioritizing consumer safety and security
- Lessons learned and evolving a program over time
- Actionable advice for those thinking about starting a program

To register for this free webinar on Tuesday, April 23, at 1:00 pm ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Two-factor authentication (2FA) scams are a type of man-in-the-middle phishing scheme in which criminals masquerade as customer service representatives to trick victims into revealing verification codes designed to authenticate account holders and prevent unauthorized access to online accounts. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Cyber Attack Shuts Down Hoya Corp's Thailand Plant for Three Days

Analytic Comment: Malware designed to steal user credentials and mine cryptocurrency on infected machines recently hampered operations at the Japanese optical manufacturer HOYA and the company's production plant in Thailand. The cyber attack reportedly compromised around 100 computers and reduced production at the plant by about 60 percent during its initial stage. Though network administrators quickly discovered the cryptojacking attempt by monitoring abnormal load on network servers, manufacturing efforts at the plant were delayed for three days following the attack. This event highlights the threat that cryptojacking continues to pose to organizations and the economic impacts that can result from these types of attacks.

Cybercrime Market Selling Full Digital Fingerprints of Over 60,000 Users

Analytic Comment: Cybercrime market Genesis features over 60,000 digital fingerprints on sale for criminals to use to perpetrate fraud, identity theft, and money mule schemes. Digital fingerprints contain victim data such as credentials for social networks, financial services, and email accounts, browser cookies, WebGL signatures, canvas image data, and other system data that is often used by anti-fraud systems to help determine the identity of a user and the legitimacy of a transaction.

Genesis' creators claim to have reviewed the "top 47 analytical systems and 283 major banks and payment systems" to determine what data is needed to circumvent anti-fraud measures, suggesting that profit-motivated hackers may be finding it increasingly difficult to breach accounts with stolen credentials alone.

Patches and Updates

Adobe

Intel

Juniper

Microsoft

Omron CX-Programmer

Rockwell Automation Stratix 5400/5410/5700 and ArmorStratix 5700

Rockwell Automation Stratix 5950

Samba

Siemens CP, SIAMTIC, SIMOCODE, SINAMICS, SITOP, and TIM

Siemens Industrial Products with OPC UA

Siemens OpenSSL Vulnerability in Industrial Products (Update E)

Siemens RUGGEDCOM ROX II

Siemens SCALANCE, SIMATIC, RUGGEDCOM, and SINAMICS Products (Update F)

Siemens SIMOCODE pro V EIP

Siemens SINEMA Remote Connect

Siemens Spectrum Power 4.7

WIBU-SYSTEMS AG Wibukey Digital Rights Management (Update C)

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

April 18, 2019

National Capital Region Cyber Threat Spotlight

Malicious Email Campaign Attempts to Deliver Fareit Trojan

The NTIC Cyber Center recently detected a malicious email campaign attempting to deliver the Fareit Trojan to unsuspecting victims. First discovered in 2014, Fareit is a Trojan designed to steal user data and download additional malware onto an infected system. It has previously been observed distributing several ransomware variants as well as Trojans associated with the Necurs and Zbot botnets. Its delivery methods include fake Adobe Flash Player updates, fake FedEx delivery email notifications, and MHT file attachments in malicious email campaigns. Researchers from cybersecurity firm Bromium recently reported discovering more than a dozen servers used to host and spread malware, including Fareit, that are potentially associated with the Necurs botnet. The NTIC Cyber Center assesses with moderate confidence that the recent email campaign targeting our organization is associated with this threat. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts and malicious emails, avoid clicking on links or opening attachments from unknown or untrusted sources, and alert their organization's IT security team if they receive a suspicious email.***

Current and Emerging Cyber Threats

eGobbler Group Leverages Chrome for iOS Vulnerability in Malvertising Campaign

Threat group eGobbler is currently leveraging a Chrome for iOS vulnerability to conduct "malvertising" (malicious advertising) attacks against users of the mobile browser application. This campaign tricks the iOS Chrome app's pop-up blocking feature by causing the app to think that the mobile device user has initiated the pop-up, thereby displaying the malicious advertisements. Researchers at security firm Confiant discovered the campaign and determined that this exploit is not currently preventable by "standard ad sandboxing attributes." Confiant estimates that nearly 500 million user sessions have been exposed to this malvertising campaign designed to divert victims to adult content and gift card scams. Chrome iOS developers are currently investigating the issue but have not yet released a patch. ***The NTIC Cyber Center recommends mobile device users remain vigilant when browsing and immediately close any browser app that displays unwanted or unexpected content and apply the appropriate patches if and when they become available.***

Attackers Abuse HTML5 Ping Attribute to Launch DDoS Attacks

Security firm Imperva reports that attackers are leveraging the HTML5 ping attribute to launch distributed denial-of-service (DDoS) attacks. The ping attribute is intended to be a single action that notifies a webpage when a user clicks on a link, but attackers have abused the attribute to amplify the ping into a greater data flow and overwhelm servers. Through social engineering, attackers direct users to a website containing malicious JavaScript that automatically pings a target website continuously for as long as the user visits the infected page. The particular attack profiled by researchers generated approximately 7,500 Requests per Second (RPS)—powerful enough to disable a mid-sized website. ***The NTIC Cyber Center recommends organizations that do not require ping requests to be received on web servers block any web requests containing "ping-to" or "ping-from" HTTP headers at the firewall or web application firewall.***

Scranos Uses Digitally-Signed Rootkit to Deliver Malware

Bitdefender researchers warn that a malicious operation, dubbed Scranos, is delivering a digitally-signed rootkit to victims in an effort to deliver additional malware designed to steal data. This particular rootkit masquerades as a video driver and, once it is installed on a system, it rewrites itself to disk to maintain persistence, deletes files that are still in use to remove other payloads in memory, and runs a payload dropper to push additional malware. It can also extract login credentials stored in the following browsers: Chrome, Chromium, Firefox, Opera, Edge, Internet Explorer, Baidu, and Yandex. Researchers state that, although the global infection rate of Scranos is currently low, it is steadily evolving and spreading to other regions. ***The NTIC Cyber Center recommends users***

refrain from installing software and drivers from questionable sources and to scan all downloaded executable files using VirusTotal, a free online tool that analyzes files for malware, prior to installation.

Cyber Criminals FIN6 Shift TTPs to Ransomware Attacks

FireEye researchers observed FIN6, a cyber-gang with Russian ties, change tactics from point-of-sale (PoS) attacks to ransomware attacks. From 2016 onward, FIN6 pilfered and sold credit card data from hospitality and retail PoS systems worth $400 million using malware known as Trinity or FrameworkPOS. FIN6 was able to establish persistence and move laterally within a network using another malware Cobalt Strike, which creates backdoors and enables additional malware along with Metasploit, a penetration testing tool. Around 2018, FIN6's tactics evolved to include distributing malware to targeted networks while their PoS use declined. The distributed malware includes LockerGoga or Ryuk, which are comparably new and are likely used to avoid detection. ***The NTIC Cyber Center recommends network administrators block the associated Trinity, Cobalt Strike, Lockergoga, and Ryuk IoCs. We also recommend keeping endpoint antivirus protection updated with the latest definitions and properly segmenting networks to isolate the system from external and unauthorized access.***

Vulnerabilities

Multiple Vulnerabilities in Broadcom Wi-Fi Chipset Drivers

Carnegie Mellon Software Engineering Institute's CERT Coordination Center reports that the Broadcom w1 driver and the brcmfmac driver for Broadcom Wi-Fi chipsets contain multiple vulnerabilities that, if exploited, could allow a remote attacker to execute arbitrary code on a vulnerable system or open the door to denial-of-service attacks. ***The NTIC Cyber Center recommends users of products containing the affected chipset and drivers refrain from connecting to unsecured, public Wi-Fi signals and implement the appropriate vendor patches if and when they become available.***

Zero-Day Internet Explorer Vulnerability Allows Attackers to Steal Files

A security researcher recently released details of a vulnerability in Internet Explorer that allows attackers to steal data from Windows users. By tricking users into opening malicious MHT files, a file format used to save copies of webpages, attackers can disable Internet Explorer's security warnings and exfiltrate local files. Because Windows automatically opens MHT files by default with Internet Explorer, any user with Internet Explorer present on Windows 7, 10, or Server 2012 R2 is vulnerable. The security researcher who discovered the vulnerability alerted Microsoft, but the

company declined to issue a patch at this time. As the details of this vulnerability and exploit are publicly available online, there is now an increased risk of malicious actors leveraging this vulnerability in future attacks. ***The NTIC Cyber Center recommends users and administrators refrain from using Internet Explorer and remove it from their systems and network environment, if possible. If removing Internet Explorer is not feasible, we recommend changing default application settings to launch MHT and similar files with a more secure browser.***

Insecure Tokens Leave Popular VPN Services Vulnerable to Session Spoofing

DHS's Cybersecurity and Infrastructure Security Agency (CISA) warns that vulnerabilities in VPN software packages of numerous providers may allow attackers to gain unauthorized access as an end user. By accessing session tokens and cookies stored insecurely in memory or log files, attackers with existing access to a compromised system can replay or spoof VPN sessions to gain access to applications through a VPN session. CISA advises that while VPN packages including Palo Alto Networks Global Protect and Pulse Secure Desktop Client and Network Connect have been patched, the AnyConnect VPN package from Cisco remains unpatched. ***The NTIC Cyber Center recommends users of VPNs from Palo Alto Networks or Pulse Secure install updates listed in this bulletin's Patches section, and users of Cisco AnyConnect VPN disable the service from their systems or network environment until a patch becomes available.***

Vulnerabilities in Shimo VPN Client Grant Attackers Root Privilege

Researchers at Cisco's Talos Security Intelligence and Research Group discovered six privilege escalation vulnerabilities for the "helper tool" in Shimo VPN client version 4.1.5.1 on Mac OS systems. In order to be exploited, attackers must have local device access. Some vulnerabilities allow root level access. There is currently no patch or workaround available for CVE-2018-4004, CVE-2018-4005, CVE-2018-4006, CVE-2018-4007, CVE-2018-4008, or CVE-2018-4009. ***The NTIC Cyber Center recommends Shimo VPN client users keep antivirus software updated with the latest virus definitions, monitor systems for unusual and suspicious activity, and update the VPN client if and when a patch becomes available.***

Data Breach Alert

Microsoft reported a data breach affecting an unknown number of Microsoft web email services customers. The breach, which occurred from January 1, 2019 to March 28, 2019, allowed cyber criminals to access information such as email addresses, folder names, and email subject lines using a support agent's compromised credentials. The company indicates that email contents, attachments, or user login credentials are not believed to have been accessed. ***As Microsoft warns that affected users may experience an increase in phishing or spam emails, the NTIC Cyber Center advises Microsoft web email service customers to remain vigilant for such correspondence and avoid opening emails and attachments from unknown or untrusted sources.***

Wipro Ltd., an India-based IT outsourcing and consulting firm, is reportedly investigating a breach that occurred after a sophisticated phishing campaign targeted some of the company's employee accounts. According to cybersecurity journalist Brian Krebs who initially broke the story on April 15, two anonymous sources claim that malicious actors compromised and leveraged Wipro's systems to conduct attacks against at least a dozen Wipro customers. The names of affected customers have not been released. ***The NTIC Cyber Center recommends Wipro clients and customers scan all incoming emails from the company for phishing attempts, monitor their networks for suspicious activity, and contact Wipro for specific indicators of compromise (IoCs) and adversary tactics, tools, and procedures (TTPs) associated with the breach. Brian Krebs also provides IoCs here.***

Upcoming Webinars

GOVINFO SECURITY®

Law Enforcement in Cyberspace: How AI Defends Today's Cities

Entrusted with protecting the personal information of their residents, with securing critical infrastructure, and with overseeing fair elections, local governments face few challenges more pivotal than cyber security. Yet most cities and counties rely on an outdated approach to defending their networks: relying on traditional security tools that detect only known threats and incident responders who can only investigate these threats so quickly.

With never-before-seen attacks striking municipal networks at machine speed, these governments need more help to keep pace with the sophisticated criminals targeting them.

Join this webinar and learn:

- Why only self-learning security tools can catch never-before-seen cyber-attacks
- Where criminals have found weaknesses in municipal infrastructure environments
- How to protect your network from machine-speed attacks
- What gaining 100 percent network visibility of your entire digital estate can reveal about the largely uncharted vulnerabilities that attackers are targeting today

To register for this free webinar on Thursday, April 25th at 1:30pm ET, click here.

GOVINFO SECURITY®

Revealing the Dark Web: How to Leverage Technologies to Alert and Block Dark Web Access

We've all seen what's possible with the Dark Web thanks to Silk Road. If you're interested in buying or selling someone's private data like social security numbers or credit card information, it's disturbingly easy to do. All you need is a computer, a Tor Browser and Cryptocurrency, and it's all completely anonymous.

So how do companies arm themselves with the right tools to protect themselves against rogue access to the Dark Web?

Join this webinar to learn more! To register for this free webinar on Wedneday, May 1st at 11:30am ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Charity scams, also known as donation scams or charity fraud, are a type of social engineering scheme in which the perpetrator elicits money or personal information from victims through fake charities and popular social causes.

Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

A Quarter of Phishing Emails Bypass Office 365 Security

Analytic Comment: According to analysis conducted by cloud security firm Avanan, one in every 99 emails can be categorized as a phishing attempt and 25 percent of phishing emails successfully bypass Microsoft Office 365 default security configurations. More than 50 percent of these emails contain malicious links or attachments designed to deliver malware to the end user's machine and 40 percent attempt to pilfer login credentials from unsuspecting recipients. These findings highlight the importance of end user cybersecurity education as software solutions are not 100 percent effective against these types of threats. To download and read Avanan's 2019 Global Phish Report, click here.

Keeping Workplace Privacy Accidents to a Minimum

Analytic Comment: Technological workplace innovations such as email, cloud services, and connected access management have made data leaks and spills easier. Emails are notorious for accidental reply-all messages, distributing information to the wrong recipients. Some email providers feature a recall option but this often proves futile due to a lack of user awareness and training. Cloud services often feature automatic backup and synchronization options that can result in the commingling of personal and private data. These issues all highlight the need for a combined effort from both employers and employees in order to improve an organization's security posture.

Patches and Updates

Apache Tomcat

Cisco IOS XR

Delta Industrial Automation CNCSoft

Drupal

Oracle

Palo Alto Networks GlobalProtect Agent VPN

PLC Cycle Time Influences

Pulse Secure VPN

VMware

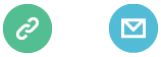
WAGO Series 750-88x and 750-87x

TLP:WHITE

removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.

We welcome your feedback. Please click here to complete a brief survey and let us know how we're doing.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

April 25, 2019

National Capital Region Cyber Threat Spotlight

NamPoHyu/MegaLocker Ransomware Targets Samba Servers

The NamPoHyu Virus, also known as the MegaLocker Virus, belongs to a new malware family that runs ransomware remotely to encrypt files on targeted machines as opposed to installing the ransomware executable locally on the system. NamPoHyu/MegaLocker searches for exposed Samba servers and brute forces passwords to gain access and encrypt files, appending *.crypted* or *.NamPoHyu* to the file names. It then drops ransom notes named *!DECRYPT_INSTRUCTION.TXT* onto the infected system. The notes demand $1000 worth of Bitcoin from companies and $250 from individuals, requesting victims send a photo of themselves at a personal event. In some cases, files encrypted by NamPoHyu/MegaLocker may be able to be recovered as security researchers affiliated with the forums on BleepingComputer.com are working on a free solution for victims. ***The NTIC Cyber Center assesses that there are over 550 servers within the National Capital Region that are potentially vulnerable to this threat. For this reason, we recommend network administrators proactively block the associated indicators of compromise listed in the BleepingComputer article. We also recommend maintaining regular system backups that are stored securely off the network and keeping endpoint antivirus software updated with the latest virus definitions.***

To reduce your risk of a ransomware infection, we encourage you to visit our website and download the NTIC Cyber Center Ransomware Mitigation Guide and the NTIC Cyber Center Guide for Cyber Incident Response Planning.

Local Educational Event

Operation Stop Scams: Scam Jam and Shredfest

AARP Virginia and Fairfax County Government's Silver Shield Task Force are joining together on Saturday, April 27, to educate Virginia residents about prevalent scams such as fake solicitor schemes, bogus investment deals, lottery scams, email fraud, grandparent scams, and the latest identity theft schemes. They also invite residents to bring any documents they would like to shred using their shred truck and to safely dispose of any unused medication in the Drug Take-Back box that will be available on-site. This event is free, but registration is required. Interested residents can register online or by calling 1-877-926-8300. For more information including times and agenda, please visit the AARP Virginia website.

Training Opportunity

The White House Office of Management and Budget and the Federal CIO Council are now accepting applications for the Federal Cyber Reskilling Academy, an initiative created in November 2018 to address the need for a skilled federal cybersecurity workforce. The application period is open from April 22 through May 15, 2019 and applicants will need to complete two online assessments no later than May 22, 2019. Selected candidates will be notified beginning June 10 and training will be held between July 8 and September 20, 2019. For more information and to apply, visit the CIO website here.

Current and Emerging Cyber Threats

Excel 4.0/XML Macros Leveraged to Deliver Malware

According to security firm Avira, hackers are exploiting a 25-year-old spreadsheet feature called Excel 4.0 (XLM macros) to deliver malware. While more current malicious files feature detectable VBA macros, backwards compatibility in recent Excel versions allow Excel 4.0 macros to bypass conventional antivirus detection enabling subsequent attacks. Subsequent attacks may include setting *Auto_open cell* to automatically run macros and accessing Win32 APIs to run malicious PowerShell scripts undetected. Microsoft recommends using the latest version of Microsoft Visual Basic for Applications (VBA) rather than Excel 4.0. ***Since exploiting this functionality to deliver malicious payloads is a common attack vector, the NTIC Cyber Center recommends users disable macros by default and avoid opening documents from unknown and untrusted sources. We also recommend network administrators block the ability to run Excel 4.0/XML macros.***

HotList Phishing Campaign Targets Instagram Users

An Instagram phishing campaign known as "The HotList" urges users to click on malicious links masquerading as pictures rated as "Hot" in an effort to steal user credentials. Targeted victims receive a message from a malicious Instagram profile stating their photos are featured on a scored "Hot" list and are prompted to click on a link to view their ranking. When clicked, the link leads to a spoofed Instagram login page. If victims enter their credentials, perpetrators will then hijack their Instagram accounts and use them to try and scam others. "The HotList" is based a similar social engineering attack known as the "The Nasty List" which rates users on a "Nasty" scale. ***The NTIC Cyber Center recommends Instagram users first verify the accuracy of the associated phone number and email address with their account. Once this step is complete, change their password to something lengthy and unique to that account, and enable two-factor authentication. Users unable to access their accounts may regain access by filing a report with Instagram.***

Vulnerabilities

WordPress Social Warfare Plugin

Security researchers at Palo Alto Network Unit 42 recently observed several successful exploits of vulnerabilities in Social Warfare, a third-party WordPress plugin that adds social sharing buttons to

a website or blog. Vulnerabilities in the plugin may allow attackers to run arbitrary PHP code, control the website and server without authentication, perform cryptojacking, and redirect website visitors to ad or phishing sites. The NTIC Cyber Center identified approximately 42,000 websites enabled with the Social Warfare plugin as of the time of this posting, with affected sites belonging to a variety of organizations in sectors including education, finance, news, technology, and others. ***As many of these sites appear to still be vulnerable to attacks, the NTIC Cyber Center recommends administrators of WordPress sites using an outdated version of the Social Warfare plugin update to the latest version as soon as possible.***

Data Breach Alert

Instagram's parent company, Facebook, Inc., revaluated the estimated thousands of exposed Instagram credentials last month as currently in the millions. Although Facebook, Inc. found no signs of internal abuse, Instagram user credentials were improperly stored in a readable format and accessible to employees. Facebook, Inc. states credentials were not exposed to outside threat actors as the data was stored on internal servers. ***As a result of the possible exposure of Instagram user credentials, the NTIC Cyber Center recommends Instagram users change their account passwords, enable two-factor authentication on their accounts, and avoid reusing passwords across multiple platforms.***

Security researchers discovered a cache of approximately 60 million LinkedIn user records in unsecured databases totaling 229 GB. Though the records contained mostly publicly-accessible information such as LinkedIn user profile information, work history, education history, location, listed skills, and links to other profiles, the databases also contained account creation email addresses that customers may have previously elected to keep private. LinkedIn believes the databases may belong to a third-party service provider who scraped public customer data from the site, but this explanation has left security researchers puzzled as to why private email addresses were found among the records. ***Although there is no indication yet that threat actors accessed the unsecured databases, the NTIC Cyber Center recommends LinkedIn users remain vigilant for increased phishing attempts perpetrated through email, social media, telephone, text messages,***

and other avenues as a result of this data exposure.

Numerous Chipotle customers may have fallen victim to a credential stuffing attack that allowed third parties to access customers' Chipotle accounts and make unauthorized purchases at Chipotle locations throughout the United States. Chipotle believes attackers may have used dumped email and password combinations originating from other data breaches to log into customer accounts and make purchases. Some Chipotle customers counter this explanation, however, and assert that they used unique passwords on the site, blaming the attack on a breach of customer data. The company is currently monitoring security issues related to these concerns. ***As credential stuffing attacks underscore the dangers of relying on single-factor authentication and using identical login credentials for different accounts, the NTIC Cyber Center recommends organizations implement multi-factor authentication on login services and account users create strong and unique passwords to access different platforms. In addition, we recommend Chipotle customers monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.***

BodyBuilding.com recently disclosed a data breach that may have affected current and former customers of the fitness store's ecommerce platform. The breach allowed cyber criminals to access customer information such as email addresses, usernames, passwords, billing/shipping addresses, phone numbers, order histories, birthdates, communications with Bodybuilding.com, and other information included in customers' BodySpace profiles. The company indicates that customer credit or debit card numbers beyond the last four digits are not believed to have been accessed. ***The NTIC Cyber Center advises current or former BodyBuilding.com customers to change their passwords on the site, avoid reusing passwords across multiple platforms, and remain vigilant for phishing emails disguised as security notifications concerning this incident.***

Upcoming Webinars

GOVINFOSECURITY®

The Anatomy of a Spear Phishing Attack: How Hackers Build Targeted Attacks (and Why They're So Effective)

Spear phishing is among the most dangerous cyber threats - and the most difficult to detect. Not long ago, C-level executives were the sole target. Today, any person at any company is at risk of receiving targeted emails attempting to trick them into completing wire transfers, purchasing gift cards, or fulfilling other financial requests.

In this webinar, we'll show you step by step how hackers create personalized spear phishing attacks. Discover how hackers identify and research targets, how they compromise email accounts from which to send their attacks, and how they leverage social engineering techniques to pressure recipients into taking immediate action.

Gain insight into:

- Spear phishing's rapid growth and how a successful attack could impact your business
- A step-by-step demonstration of how hackers create spear phishing emails
- Practical recommendations to protect your business from this growing threat

To register for this free webinar on Thursday, May 16th at 1:30pm ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Unsolicited robocalls and scam calls are an increasing and pervasive threat to residents within the National Capital Region and across the United States and recent legislation efforts have done little to curb the problem. In fact, experts believe that, by the end of 2019, scam calls will comprise nearly half of all US mobile call traffic. Unfortunately, distinguishing between scam calls and legitimate calls can be difficult as many of these nuisance calls employ caller ID spoofing techniques to trick recipients into answering the phone. However, mobile phone carriers and communications technology companies have been working together to develop solutions for customers. This week, as part of the NTIC Cyber Center's Securing Our Communities initiative, we are providing our readers with a list of tools and services offered by each major US mobile provider to help combat these unwanted calls.

Click here to see what solutions your mobile carrier provides to protect customers from scam calls.

Cyber in the News

Ransomware Interrupted a "The Weather Channel" Morning Show

Analytic Comment: The Weather Channel suffered a ransomware attack last week that prevented the network from broadcasting live programming of the daily news and weather program *AMHQ*. According to the network's Twitter feed, the show was unable to go on air at its usual 6:00 AM starting time. Fortunately, however, backups of critical network systems allowed the channel to restore full broadcasting functionality shortly after 7:30 AM that morning. As the incident is still under investigation, officials have not indicated how threat actors might have perpetrated the ransomware attack. The incident highlights the pervasiveness of ransomware attacks and underscores the importance of maintaining regular system backups to effectively respond to and recover from an attack.

Patches and Updates

Chrome

Fujifilm FCR Capsula X/Carbon X

Rockwell Automation MicroLogix 1400 and CompactLogix 5370 Controllers

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.

We welcome your feedback. Please click here to complete a brief survey and let us know how we're doing.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

May 2, 2019

National Capital Region Cyber Threat Spotlight

CISA Releases Binding Operational Directive 19-02 to Address Critical and High Vulnerabilities in Federal Information Systems

On April 29, 2019, the US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued Binding Operational Directive (BOD) 19-02 Vulnerability Remediation Requirements for Internet-Accessible Systems. BOD 19-02 requires all federal agencies to ensure effective and timely remediation of "critical" and "high" vulnerabilities in information systems. According to the directive, all critical vulnerabilities must be remediated within 15 calendar days of initial detection and all vulnerabilities deemed "high" must be remediated within 30 calendar days of initial detection. CISA will monitor federal agency progress and will engage Chief Information Security Officers, Chief Information Officers, and Senior Accountable Officials for Risk Management if agencies have not met the imposed remediation deadlines. ***The NTIC Cyber Center recommends all administrators of federal information systems and networks review the CISA blog post detailing BOD 19-02 and download the PDF version of the directive, available here.***

Event Announcement

Homeland Security and Preparedness Symposium

The District of Columbia Homeland Security and Emergency Management Agency (HSEMA) and Georgetown University's Emergency and Disaster Management Graduate Program are privileged to host the inaugural Homeland Security and Preparedness (HSP) Symposium to be held from May 13-14, 2019. This event will be held at the Georgetown University School of Continuing Studies campus located at 640 Massachusetts Ave NW, Washington, DC.

The theme of this multi-agency, multidisciplinary event is to bring experts together from around the National Capital Region to discuss homeland security, preparedness, and response to complex emergencies. This year, we are paying specific attention to the threats faced by houses of worship and schools. The spate of attacks and threats on these institutions across the world have drawn into sharp focus the need for collaborative planning efforts across all public safety and human service disciplines to respond to these incidents.

Over the course of two days, the symposium will feature tracks geared towards Intelligence and Information Sharing, Continuity of Operations Planning (COOP), Critical Infrastructure and Long-Term Risk Reduction, Disability Integration into Emergency Preparedness, Business Emergency Preparedness, School Safety, and Executive Leadership. Each day will provide structured opportunities to collaborate and network with practitioners and academics dedicated to homeland security and emergency preparedness. The HSP Symposium will aid District agencies and stakeholders in collectively planning for and responding to incidents of all hazards for the whole community. To register for Day 1, please click here. To register for Day 2, please click here.

Current and Emerging Cyber Threats

Chase Bank Phishing Scam Requests "Selfie" of Victims Holding ID Card

Security researchers identified a phishing scam designed to steal the personal information of Chase Bank customers. The scam directs users to a realistic-looking Chase login screen prompting a username and password and asking users to verify their personal information. The webpage proceeds to solicit the customer's email address, email password, billing address, phone number, credit card information, social security number, ATM pin number, mother's maiden name, and driver's license number. Finally, users are directed to upload a picture of their ID card and credit card as well as a photograph of themselves holding an ID card. Researchers believe the data captured in this phishing scheme would allow threat actors to create new accounts under the victim's name or access the victim's cryptocurrency funds. ***The NTIC Cyber Center recommends Chase Bank customers remain vigilant for phishing attempts and malicious emails, avoid clicking on links or opening attachments from unknown or untrusted sources, and report any suspicious***

activity or phishing attempts to Chase Bank's customer service.

Qbot Malware Delivered in New Malicious Email Campaign

Researchers in the JASK Special Operations team identified a new malspam campaign that delivers Qbot malware embedded in emails masquerading as parts of previous online conversations. Qbot, also known as QakBot and Pinkslipbot, is a banking Trojan used to steal victims' financial data and can log keystrokes, steal cookies, create backdoors, and inject additional malware onto an infected system. Victims receive an email prompting them to view a document hyperlinked to .zip archive file laced with VBScript-based dropper script. The victim is compromised when they click the hyperlink to a VBScript. Qbot establishes persistence by embedding itself into *%Appdata%\Roaming\{Randomized String}* and generating a new registry value before moving laterally within a network by brute forcing network accounts. ***The NTIC Cyber Center recommends never opening attachments or enabling executables in files received from unexpected or unsolicited emails. If you believe you have been targeted by this campaign or infected with the Qbot Trojan, notify your organization's IT security team immediately. For home users who have been infected, make sure your antivirus software is up-to-date with the latest virus definitions and run a complete scan of your system. After removing the infection, change the passwords for all online accounts accessed from the compromised system and enable two-factor authentication on any account that offers it.***

AESDDoS Botnet Variant Exploits Server-Side Template Injection Vulnerability

Researchers at Trend Micro Cyber Safety Solutions Team discovered an AESDDoS botnet malware variant (Backdoor.Linux.AESDDOS.J) that can execute code remotely, steal information, perform distributed denial-of-service (DDoS) attacks and mine cryptocurrency on vulnerable Atlassian Confluence Server and Data Center software. Trend Micro first noticed AESDDoS exploiting a Widget Connector macro in Atlassian Confluence Server via a server-side template injection vulnerability. Further analysis revealed that the threat actor deployed AESDDoS through two shell script commands, Trojan.SH.LODEX.J for initial penetration and then Trojan.SH.DOGOLOAD.J to deliver the malicious payload. ***The NTIC Cyber Center recommends all Atlassian users to upgrade to the latest version (6.15.1) and network administrators review AESDDoS Botnet Malware report and monitor networks for the associated indicators of compromise (IoCs).***

New Tech Support Scam Abuses Iframe to Freeze Browsers

Security researchers detailed a new technique that tech support scammers are using that combines iframe and authentication pop-up windows to freeze victims' browsers. This new tactic uses a typical landing page spoofing a Microsoft tech support site, but it displays two pop-ups: a dialog box with a fraudulent tech support phone number and an authentication request box prompting the input of user credentials. Attempting to interact with the authentication box, including clicking "cancel," "OK," or trying to close the box merely causes the page and dialog boxes to reload, mimicking the symptoms of a frozen browser window and entering the user into an inescapable loop. Scammers likely designed the page in this way to frustrate users into eventually following the dialog box instructions and calling the number provided for help. ***The NTIC Cyber Center recommends users remain vigilant for tech support scams disguised as security notifications and avoid clicking on links or opening attachments from unknown or untrusted sources. We advise users who may encounter malicious browser loops to use Windows Task Manager to end the browser process by typing Ctrl + Alt + Delete, clicking "Task Manager," selecting the affected browser, and clicking "End task". In addition, the NTIC Cyber Center encourages readers to reference our Securing Our Communities blog post for information on how to protect yourself from tech support scams.***

Vulnerabilities

Millions of IoT Devices Containing iLnkP2P Software Vulnerable to Attack

A security researcher recently assessed that nearly two million Internet-of-Things (IoT) devices are exposed to eavesdropping and compromise as a result of unpatched vulnerabilities (CVE-2019-11219 and CVE-2019-11220) within iLnkP2P, peer-to-peer communication software developed by China-based Shenzhen Yunni Technology and bundled with many IoT devices such as security cameras, baby monitors, and Internet-connected doorbells. If exploited, these vulnerabilities could allow attackers to bypass firewall restrictions and establish remote connections to devices, steal login credentials, and intercept live video feeds and stored footage. Vulnerable IoT devices include but are not limited to the following models: CamHi, P2PWifiCam, iMega Cam, Webvision, P2PPIPCamHi, IPCAM P, Eye4, EyeCloud, VSCAM, PnPCam, E View7, P2PPIPCAM, CoolCamOp, APCamera, and P2PCam_HD. There is currently no patch or workaround available for these vulnerabilities. ***The NTIC Cyber Center recommends users of products containing the affected iLnkP2P software refrain from connecting them to unsecured, public Wi-Fi signals and implement the appropriate vendor patches if and when they become available. We also recommend network administrators block UDP port 32100 to stop P2P communication. If possible, consider decommissioning affected devices and replacing them with devices from reputable vendors. For more information, including instructions detailing how to determine if***

your devices are vulnerable, visit the researcher's website at hacked.camera.

Dell SupportAssist Client

On October 10, 2018, an independent security researcher responsibly disclosed a severe vulnerability (CVE-2019-3719) to Dell that impacted the company's SupportAssist Client software, which comes preinstalled on nearly all new Dell systems running Windows OS. If exploited, this vulnerability could allow unauthenticated attackers to remotely execute arbitrary code on targeted systems. Additionally, another researcher responsibly reported an improper origin validation flaw (CVE-2019-3718) he discovered in the same software that could allow attackers to perform cross-site request forgery attacks against vulnerable systems. In late April 2019, Dell issued a patch to address both vulnerabilities. ***The NTIC Cyber Center recommends all users and administrators of Dell computer systems update the SupportAssist Client software to version 3.2.0.90 or later as soon as possible. More information about the vulnerabilities and a link to download the patch are available on Dell's website.***

WordPress WooCommerce Plugin

Security company Plugin Vulnerabilities disclosed details of an unpatched vulnerability in the WordPress plugin WooCommerce Checkout Manager. The vulnerability in the plugin's file upload feature may allow attackers to execute script code, access or modify data, and gain administrative access. ***As the researchers believe this vulnerability affects approximately 60,000 websites, the NTIC Cyber Center recommends administrators of WordPress sites using the WooCommerce Checkout Manager plugin disable the "Categorize Uploaded Files" option within the plugin settings or remove the plugin completely until a patched version becomes available.***

Oracle WebLogic

Security researchers warn of a highly critical vulnerability affecting all versions of Oracle WebLogic software. The vulnerability, if exploited, would allow attackers to remotely execute arbitrary commands by sending the server a malicious HTTP request. Researchers believe that up to 36,000 web servers are currently running WebLogic and may be vulnerable to exploitation through this attack vector. A recent Cisco Talos report suggests that threat actors are already exploiting this vulnerability to distribute Sodinokibi, a new variant of ransomware. ***The NTIC Cyber Center recommends administrators update the Oracle WebLogic software using the most recent patch issued here.***

Data Breach Alert

Docker Hub announced a security breach that exposed the sensitive information of 190,000 users. The breach, which occurred on April 25, allowed unauthorized parties to access usernames, hashed passwords, and tokens for GitHub and Bitbucket repositories. Third-party access to these items may allow threat actors to access and modify code of private repositories, insert malware into application containers, or perpetrate supply-chain attacks. ***The NTIC Cyber Center recommends Docker Hub users change their account passwords and administrators review GitHub and Bitbucket login logs for indications of unauthorized access or suspicious activity.***

A security researcher discovered a publicly-accessible database containing 24 GB of personal information on 80 million American families, amounting to roughly half the population of the United States. The database, which was hosted on a Microsoft cloud server, exposed information in plaintext such as names of family members, dates of birth, addresses, and longitude and latitude coordinates as well as coded information related to title, gender, marital status, income, homeowner status, and dwelling type. Though the owner of the database has not been identified, security professionals believe the information may belong to an insurance or mortgage company. ***As this information could allow threat actors to perpetrate identity theft and other crimes, the NTIC Cyber Center recommends remaining vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

Upcoming Webinars

Data Breach TODAY®
Prevention. Response. Notification.

SOC Processes Are Broken: Why We Don't Catch Critical Threats

Security Operation Center (SOC) processes are broken, analysts are feeling the cybersecurity job fatigue, and enterprises are still at risk. SOC leaders often struggle to understand how to make their

teams more effective and end up spending their budget on point solutions that add to the problem of data overload. How do you improve security analyst efficiency, and ultimately their ability to identify and focus on what matters to secure your business?

In this webinar, we will discuss the top five challenges plaguing today's SOCs and how SOC leaders can free up their security analysts by leveraging AI technologies to focus on crucial threats.

Register for this exclusive webinar to:

- Understand the pressing challenges impacting today's SOCs and security analysts
- Understand the broader scope and context of advanced threats with integrated user behavior analytics & machine learning
- Discover the benefits that adding AI to your SOC can bring to your security teams to focus on the most critical threats

To register for this free webinar on Tuesday, May 7 at 11:00am EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Interview scams, also known as video interview scams or chat interview scams, are a type of social engineering scheme in which the perpetrator uses fake job interviews to lure victims into providing their personally identifiable information (PII) or downloading malware.

Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Blancco Reveals 42 Percent of Used Drives Sold on eBay Are Holding Sensitive Data

Analytic Comment: Data erasure solutions provider Blancco Technology Group released a study on the lingering data on preowned hard drives sold through online auction website, eBay. After analyzing 159 drives with data recovery techniques, results show 42 percent of devices contain sensitive data and 15 percent contain PII. Findings include: resumes, passports, financial records, business emails, vehicle registrations, personal photos, and government clearance status. Some of the hard drives sold were advertised as being completely cleared of data. This study emphasizes the need for, and importance of, proper data sanitation and verification prior to decommissioning a hard drive.

"Ghost Users" and Non-Expiring Passwords a Major Security Issue for Most Businesses

Analytic Comment: A data risk assessment by data security company, Varonis, analyzed 70 TB of data from 130 organizations across various industries and countries. Results show that inactive "ghost user" accounts – accounts that IT administrators forgot to delete or disable after an employee leaves an organization – and accounts that have non-expiring passwords are prime targets for threat actors. Improper access control is an issue as 21 percent of all folders on a network are accessible by everyone in an organization, increasing the risk of malicious activity that could be conducted by insider threats. This assessment highlights the need for tighter security policies and regular audits of security controls within every organization.

Patches and Updates

Android

Chrome

Cisco

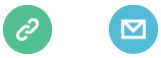
Oracle

Philips Tasy EMR

Rockwell Automation CompactLogix 5370

TLP:WHITE

We welcome your feedback. Please click here to complete a brief survey and let us know how we're doing.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

May 9, 2019

National Capital Region Cyber Threat Spotlight

Verizon 2019 DBIR: Public Sector Records Highest Number of Cyber Incidents in 2018 with Cyber-Espionage the Most Prominent Motive

According to Verizon's 2019 Data Breach Investigations Report (DBIR) released yesterday, the public sector recorded the largest number of cyber incidents, amounting to over 23,000 in 2018. Of these incidents, 330 are categorized as confirmed data breaches that resulted in the unauthorized access of data. According to the 2019 DBIR, cyber-espionage is rampant in the public sector and State-affiliated threat actors account for 79 percent of all public sector breaches involving external actors. Privilege misuse and insider error account for 30 percent of these data breaches. Verizon assesses that espionage-related public sector breaches are likely to go undetected for a long period of time, allowing threat actors to steal large amounts of data from compromised systems. ***The NTIC Cyber Center recommends all network administrators review Verizon's 2019 DBIR to gain a better understanding of how cyber threats have evolved over the past year and to learn about the most prevalent attacks and tactics used to infiltrate their networks, compromise their systems, and steal their data.***

Current and Emerging Cyber Threats

Git Repositories Targeted in Cyber Extortion Scheme

Unknown cyber threat actors are actively targeting accounts on Git hosting services GitHub, GitLab, and Bitbucket in a cyber extortion scheme, extracting all source code from victims' repositories and delivering a ransom note demanding 0.1 Bitcoin, worth approximately $570, for the code's return. Affected Git hosting services believe the cyber threat actors were able to gain access to victims' repositories via unknown third-party exposures or through credential-stuffing attacks if victims used the same passwords across multiple platforms. ***The NTIC Cyber Center recommends Git hosting service users change their login credentials to include a strong variety of unique passwords and enable two-factor authentication on any account that offers it. We also recommend Git repository administrators review their associated service logs for indications of unauthorized access or suspicious activity.***

New MegaCortex Ransomware Targets Large Enterprise Networks

Security firm Sophos discovered a new ransomware called MegaCortex targeting large enterprise networks. MegaCortex is composed of automated and manual elements designed to infect as many victims as possible. Current research suggest MegaCortex works by placing a meterpreter reverse shell onto the victim's system and pivots into PowerShell scripts to batch files remotely. It then uses commands to cause the malware to drop the secondary executable payload from the initial dropped malware on desired machines. From there, MegaCortex can spread throughout the entire network via Windows domain controllers. There is a speculated relationship between MegaCortex and other malware as networks impacted by this ransomware have also been infected by the Emotet and Qbot banking Trojans. ***The NTIC Cyber Center recommends network administrators proactively block MegaCortex, Emotet, and Qbot indicators of compromise (IoCs). We also recommend maintaining regular system backups and keeping all hardware, software, devices, applications, and operating systems patched and updated.***

Scammers Abuse Google Search Ads to Defraud Victims

Cybersecurity website BleepingComputer.com reports that scammers are abusing Google search ads to masquerade as popular web services such as PayPal, Amazon, and eBay and defraud unsuspecting victims. When users perform online searches to find a company's contact information, the first Google search result may be a malicious advertisement containing a fraudulent customer support number. If victims call the number displayed in the ad, they are greeted by a scammer posing as a customer support representative who claims that victims' accounts can be fixed by providing a code on the back of a Google Play Card. ***The NTIC Cyber Center recommends search engine users remain vigilant for fraudulent customer support advertisements, verify the authenticity of websites prior to entering any personal or sensitive information, ignore***

solicitations for money and gift cards during customer service calls, and report any suspicious advertisements to Google's ad flagging feedback form.

Vulnerabilities

Unsecure SAP Components Vulnerable to 10KBLAZE Exploits

Researchers at the April 2019 Operation for Community Development and Empowerment cybersecurity conference recently disclosed exploits that may affect approximately 900,000 unsecure SAP production systems. The publicly available exploits and tools, collectively known as 10KBLAZE, would allow attackers to fully compromise a system and perform critical business transactions such as creating fake vendors, creating fake employees, creating and modifying purchase orders, changing bank accounts, paying any vendor or employee, releasing shipments, changing inventory data, generating corrupted management reports, and bypassing automatic business controls—all without requiring a username or password. Affected SAP products include the SAP Business Suite, SAP ERP, SAP CRM, SAP S/4HANA, SAP Solution Manager, SAP GRC Process and Access Control, SAP Process Integration/Exchange Infrastructure (PI/XI), SAP Solution Manager, SAP SCM, and SAP SRM, and others. ***The NTIC Cyber Center advises administrators of SAP products reference and implement the mitigation strategies recommended in the recent Department of Homeland Security Cybersecurity and Infrastructure Security Agency Alert AA19-122A.***

PrinterLogic Print Management Software

Carnegie Mellon University researchers report that all versions of PrinterLogic Print Management Software up to and including 18.3.1.96 are currently vulnerable to multiple attacks. The software fails to validate SSL certificates and software update packages and does not sanitize web browser inputs. These vulnerabilities could allow attackers to spoof a trusted entity to launch man-in-the-middle attacks or remotely execute malicious code on machines running the software. ***As there is currently no patch available, the NTIC Cyber Center recommends administrators enable "always on" VPN to prevent man-in-the-middle attacks and enforce application whitelisting to prevent the execution of malicious code until a patch is released.***

Jenkins Plugins

A security consultant identified vulnerabilities in over 100 third-party plugins designed for the Jenkins open source software development automation server. The vulnerabilities, which include the storage of credentials in plain text and cross-site request forgery (CSRF) with missing permission checks, could allow attackers to steal user credentials or launch server-side request forgery (SSRF)

attacks. ***As the article details methods for exploiting zero-day vulnerabilities in Jenkins plugins, the NTIC Cyber Center recommends Jenkins platform users disable third-party extensions until plugin developers release patches resolving the issues. We also recommend Jenkins platform administrators review and implement the recommendations provided in*** *Jenkins Security Advisory 2019-04-03*.

Data Breach Alert

Security researchers at Trend Micro recently discovered Magecart online skimming attacks targeting 201 online campus stores of college and universities throughout the United States and Canada. By abusing vulnerabilities in the stores' ecommerce platform PrismWeb, attackers managed to install malicious code disguised as Google Analytics script to capture the personal and payment data of an unknown number of customers. The stolen customer data may include information such as card numbers, expiration dates, card types, card verification numbers, cardholders' names, addresses, and phone numbers. As a result of the novel attack techniques observed, researchers credited this digital heist to a new Magecart group dubbed "Mirrorthief." ***As a list of affected colleges and universities has not yet been made public, the NTIC Cyber Center advises any customers who may have recently made purchases via online campus stores to monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.*** To read more about the threat Magecart poses to ecommerce websites, please see our recent Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Online tutoring services company Wyzant recently disclosed a data breach revealing users' personally identifiable information (PII) and Facebook profile information. An investigation revealed that an unknown threat actor may have exploited a security flaw to breach Wyzant systems on April 27, 2019. Wyzant has over two million registered users and the company does not believe the perpetrators had access to any user financial details, passwords, or activity records. However, users who sign into the Wyzant platform through Facebook may experience further phishing

attempts due to cross-platform integration. Wyzant patched the suspected security flaw and will audit its entire network and application security infrastructure. ***The NTIC Cyber Center recommends Wyzant and cross-platform connected Facebook users change their account passwords, enable two-factor authentication on any account that offers it, and avoid reusing passwords across multiple platforms***.

Upcoming Webinars

Demystifying Machine Learning for Fraud Detection

The rapidly changing cybercrime landscape has required organizations to seek new methods, such as machine learning, that enable systems to learn, adapt, and uncover emerging fraud patterns quickly. However, there are many debates about the merits of machine learning models for fraud detection and which one works best. The bottom line: it's not about the model, but what's behind it that makes it work.

So how do you cut through the machine learning hype? As you start to evaluate fraud prevention solutions and the advantages of the machine learning models they offer, there are several questions you should be prepared to ask.

Register for this upcoming webinar and hear from leading experts on:

- The misconceptions about machine learning models
- The risks of building your own model
- How to optimize machine learning for fraud detection
- Top questions to ask solution providers

To register for this free webinar on Wednesday, May 29 at 1:30pm EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

One ring scam calls, also known as Wagiri (Japanese for "one ring and done"), are automated telephone calls – or robocalls – that ring targeted phones only one time before terminating to prevent recipients from answering. These calls are merely designed to generate a "missed call" notification on targeted phones to spark curiosity and bait victims into returning the calls. If victims call the number, they may hear recorded messages designed to keep them on the line or they may connect with a live person who tries to convince them to call back multiple times. Each time a victim initiates a call to the scammer's number, high connection fees or international rates will be charged to the victim's phone bill. The scammer then profits from these schemes by receiving all or a portion of the fees charged to the victim.

Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

55 Percent of Small Business Owners Would Pay for Their Data in a Ransomware Attack
Analytic Comment: Results from the recent AppRiver Q2 Cyber Threat Index for Business survey indicate that 55 percent of small businesses would be willing to pay a ransom to recover data lost as a result of a ransomware attack or breach. For larger small businesses, the statistic increases to 74 percent, with 39 percent of those respondents expressing willingness to "pay any price" to ensure data is recovered. Respondents' high willingness to pay ransom fees highlights the importance of data to business organizations while also underscoring the value of implementing robust security measures, training employees on best practices, and maintaining offsite backups of business data for recovery the event of an attack.

DeepDotWeb Dark Web Resource Dies with FBI Seizure
Analytic Comment: The US Federal Bureau of Investigation along with European law enforcement agencies seized DeepDotWeb, a Clearnet website containing Dark Web news, links to illicit market

places, and other Dark Web-related resources. The website's administrators, arrested in Israel, are suspected to have made millions of dollars through various money laundering activities and Dark Web referral sales. Other suspects associated with the website were also arrested in France, Germany, Brazil, and the Netherlands. This successful law enforcement operation demonstrates that combating cyber crime often requires a combined effort with the coordination of multiple agencies from various jurisdictions.

Patches and Updates

GE Communicator

Orpak SiteOmat

Sierra Wireless AirLink ALEOS

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

May 16, 2019

National Capital Region Cyber Threat Spotlight

DHS and FBI Release Malware Analysis Report on North Korean Malware ELECTRICFISH

The US Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) released a joint Malware Analysis Report (MAR) detailing a newly discovered malware variant, dubbed ELECTRICFISH, used by the North Korean government to exfiltrate data from victims in HIDDEN COBRA cyber operations. United States officials believe this malware may allow threat actors to bypass authentication and initiate a funneling session on a compromised system to exfiltrate data to a destination IP address. The MAR includes the description and analysis of a malicious executable file associated with this threat, as well as suggested response actions and recommended mitigation techniques. Users and administrators are encouraged to flag malicious activity associated with ELECTRICFISH and report it to the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI Cyber Watch (CyWatch), giving the activity the highest priority for enhanced mitigation. ***The NTIC Cyber Center recommends all network administrators review Malware Analysis Report (AR19-129A) and monitor networks for the associated indicators of compromise (IoCs). Additional information about HIDDEN COBRA is available on us-cert.gov.***

CISA Releases Analysis Report on Microsoft Office 365 Security Observations

CISA issued Analysis Report (AR19-133A) titled *Microsoft Office 365 Security Observations*. This report offers considerations and recommendations for organizations migrating email services to Microsoft Office 365 (O365) cloud service products and highlights configuration vulnerabilities associated with the implementation of these products. CISA indicates that a majority of organizations currently using O365 products had various configurations in place that lowered their overall security posture, leading to user and mailbox compromises and vulnerabilities. ***The NTIC Cyber Center recommends administrators of O365 cloud service systems review the CISA analysis report for mitigation strategies, best practices, and guidance on properly implementing cloud email service products.***

Current and Emerging Cyber Threats

Fake KeyPass Password Manager Website Delivers Malware

Unknown threat actors are distributing adware and malware through a network of counterfeit websites, one of which incudes a fraudulent website promoting KeePass, a password management platform. The software available through the legitimate KeePass website, keepass[.]info is safe; however, KeePass software downloaded from the illegitimate website keepass[.]com reportedly contains adware bundles that may deliver additional malware including ransomware, Trojans, and backdoors. The adware bundles are well-disguised as they feature a dynamic originating URL and signed certificates, but will pilfer the victim's personal information such as location, hardware settings, administrator access, and VPN usage to serve the victim targeted ads. ***The NTIC Cyber Center recommends only downloading KeePass from the from the official website found at keepass[.]info. We would also like to remind our members to only download applications from trusted and vetted sources and to always check the integrity of downloaded files by comparing hashes and signatures, if possible.***

New Dharma Ransomware Encrypts Files While Installing Antivirus Software

Researchers at Trend Micro discovered a new Dharma ransomware variant that installs legitimate antivirus software as a distraction while encrypting victims' data in the background. Dharma is delivered in malicious emails that contain a link to a password-protected archive file titled "MSC-ALERT-IMPORTANT." If victims download the archive file, an ESET AV Remover installer will launch and distract victims while the ransomware runs separately, encrypting files and appending .ETH to file names. ***The NTIC Cyber Center recommends never opening attachments or enabling executables in files received from unexpected or unsolicited emails. We also recommend all network administrators review Trend Micro's report and monitor networks for the associated***

indicators of compromise (IoCs). If you believe you have been targeted by this campaign or infected with Dharma ransomware, notify your organization's IT security team immediately.

LightNeuron Malware Used to Control Microsoft Exchange Servers

ESET researchers observed Turla, a nation-state Russian cyber-espionage group that used the LightNeuron malware to backdoor and control Microsoft Exchange email servers via image files embedded with commands. This malware campaign allowed Turla to intercept email, spoof email, and exfiltrate email data. Once LightNeuron is on a network, it weaves itself into the Microsoft Exchange work flow and gains persistence through the Exchange server transport agent allowing it to have "the same level of trust as security products such as spam filters." From there, Turla uses steganography, a process that hides information within images, to embed malicious commands in PDF and JPG files to control the mail server. ESET believes Turla has used LightNeuron in multiple campaigns against multiple unnamed targets since 2014. Turla is also known as Waterbug, Snake, WhiteBear, VENOMOUS BEAR, and Kypton. ***The NTIC Cyber Center recommends network administrators review the ESET report and block the associated LightNeuron IoCs.***

Vulnerabilities

"Unhackable" EyeDisk USB Drive Stores Passwords in Plain Text

Researchers from Pen Test Partners recently compromised an eyeDisk Secure Thumb Drive marketed as "unhackable" from eyeDisk. The thumb drive uses a combination of iris recognition and AES 256-bit encryption to keep data secure. While Pen Test Partners researchers were unable to bypass the iris recognition with photos, they were able to reveal passwords in plain text by capturing USB traffic using a network packet analyzer. This works because eyeDisk sends the initially entered password in plaintext before validation. EyeDisk has not issued a statement regarding the vulnerability. ***The NTIC Cyber Center recommends eyeDisk USB users encrypt any data stored on the device.***

WhatsApp Vulnerability Allows Remote Attackers to Read Messages

Messaging app company WhatsApp urges all of its 1.5 billion users to update the app to the most recent version to patch a major security vulnerability. The company reports that remote attackers have used this vulnerability to install surveillance software to read messages on targeted phones and devices. Some speculate that journalists, lawyers, activists, and human rights defenders may have been among those targeted, although WhatsApp has not confirmed how many users were affected. ***The NTIC Cyber Center recommends users of WhatsApp immediately update the app's software to the latest version (2.19.143 on Android devices; 2.19.51 on iOS devices).***

Data Breach Alert

Cellular phone carrier Boost Mobile disclosed a data breach in a customer notice distributed this week. The company reports that on March 14, 2019, threat actors accessed an undisclosed number of customer accounts using customer phone numbers and personal identification numbers (PINs). Although Boost Mobile has implemented a permanent solution to prevent future unauthorized account activity, customers are still advised to change the PINs associated with their online accounts. ***The NTIC Cyber Center recommends Boost Mobile customers immediately change their PINs, monitor their accounts, and immediately notify Boost Mobile customer service of any unauthorized or suspicious activity.***

Cyber threat intelligence provider Bad Packets Report discovered Magecart payment card skimming malware embedded in the Forbes Magazine website. By exploiting vulnerabilities in the website's ecommerce platform OpenCart, attackers injected malicious code into the site and used the WebSocket protocol to steal data such as customers' names, addresses, phone numbers, email addresses, and payment card data. It is currently unknown when the website became compromised. ***The NTIC Cyber Center recommends anyone who recently subscribed to Forbes Magazine through forbesmagazine[.]com monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.*** To read more about the threat Magecart poses to ecommerce websites, please see our recent Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Upcoming Webinars

National Critical Functions

Join the Cybersecurity and Infrastructure Security Agency (CISA) for a webinar on National Critical Functions. National Critical Functions are functions of government and the private sector

that are so vital to the United States that disruption, corruption, or dysfunction would have a debilitating effect on national security, economic security, public health or safety, or any combination thereof. The release of the set of National Critical Functions is part of CISA's evolved risk management approach. National Critical Functions provide a construct that focuses on better understanding the functions that an entity enables or to which it contributes, rather than focusing on a static sector-specific or asset world view. This more holistic approach is better at capturing cross-cutting risks and associated dependencies that may have cascading impact within and across sectors.

This webinar will highlight the utility of National Critical Functions for critical infrastructure risk management, how the set of National Critical Functions will provide the basis for deeper analysis to build a Risk Register, and how public and private sector partners can collaborate with us throughout this process.

To register for this free webinar on Monday, May 20 at 1:00pm EDT, click here.

Compromised Credentials: The Cyber Underbelly of Global Corporations

In late 2018, we saw the release of a massive amount of leaked credential "dumps." These expertly-curated collections highlight the risk posed by credentials leaked from large organizations. Join this webinar to understand how even most novice threat actors have the access and ability to exploit billions of sensitive corporate credentials, and how this threat affects your organization.

To register for this free webinar on Tuesday, May 21 at 1:00 pm EDT, click here.

How to Protect Your Executives from Cybercrime and Identity Theft

Business executives are easy and lucrative targets for cybercriminals. To ensure executive protection from dynamic exploits against VIPs, security practitioners must encorporate external tailored threat intelligence into their existing cyber defense strategies.

So how do companies arm themselves with the right tools to protect themselves against rogue access to the Dark Web?

Join this webinar to learn:

- Why executive threats equal enterprise threats
- How and where executives and VIPs are exposed on the clear, deep, and dark web

- How to automate detection and response to take down executive threats
- What best practices leading enterprises deploy
- How to strengthen your executive protection program

To register for this free webinar on Wednesday, May 22 at 9:00 am EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Sextortion is a cybercrime in which criminals threaten to distribute sensitive or incriminating content if a victim does not comply with certain demands. There are several ways criminals can perpetrate these scams, but their objective remains the same: to profit from the extortion of innocent victims. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

A Massive Accounting Hack Kept Clients Offline and in the Dark

Analytic Comment: An unknown malware strain has compromised global accounting information services company, Wolters Kluwer, specifically impacting their accounting and tax software suite, CCH. Their customers include academic medical centers, Fortune 500 companies, top accounting firms, and top banks. Customers using the cloud-based CCH services were reportedly unable to operate their software on May 6th and were unable to correspond with Wolters Kluwer's support team. Since then, Wolters Kluwer managed to restore CCH in a limited capacity. This highlights the fact that the increase in reliance upon cloud-based platforms without proper business continuity plans and robust data backup procedures in place can create a single point of failure, potentially resulting in costly recovery efforts for organizations.

Equifax's Data Breach Costs Hit $1.4 Billion

Analytic Comment: Credit reporting company Equifax continues to suffer significant monetary losses stemming from a data breach that occurred in 2017. The massive breach exposed the personal data of 148 million Americans, or nearly half of the entire United States population, as well as that of 15 million United Kingdom citizens and 20,000 Canadian citizens. Despite holding a $125 million cybersecurity insurance policy at the time it was breached, the company reports that costs

associated with legal and investigative fees, improvements to the company's security programs, and credit monitoring services for customers have mounted to $1.4 billion dollars since the event occurred. The company expects these costs will continue to increase due to additional penalties, settlements, and other resolutions expected in the future. The sheer scale of financial devastation resulting from this data breach highlights the severe impacts of security incidents on corporations and the importance of implementing strong data security practices and policies to avoid similarly costly events.

Patches and Updates

Adobe

Apple

Cisco

Drupal

Intel

Microsoft

NVIDIA

Samba

VMware

ICS-CERT Advisories

Omron Network Configurator for DeviceNet

Siemens CP, SIAMTIC, SIMOCODE, SINAMICS, SITOP, and TIM (Update A)

Siemens Industrial Products with OPC UA (Update A)

Siemens LOGO!8 BM

Siemens LOGO! Soft Comfort

Siemens S7-400 CPUs (Update A)

Siemens SCALANCE W1750D

Siemens SIMATIC Panels and WinCC (TIA Portal)

Siemens SIMATIC PCS 7, WinCC, TIA Portal

Siemens SIMATIC, SINUMERIK, and PROFINET IO (Update C)

Siemens SIMATIC WinCC and SIMATIC PCS 7

Siemens SINAMICS PERFECT HARMONY GH180 Drives NXG I and NXG II

Siemens SINAMICS PERFECT HARMONY GH180 Fieldbus Network

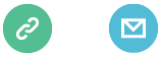
WIBU-SYSTEMS AG WibuKey Digital Rights Management (Update D)

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.

We welcome your feedback. Please click here to complete a brief survey and let us know how we're doing.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

May 23, 2019

National Capital Region Cyber Threat Spotlight

President Trump Issues Executive Order on Securing the Information and Communications Technology and Services Supply Chain

On May 15, 2019, President Trump issued an executive order (EO) to ban the use of information and communications technology produced by companies that are potentially under the direction of, or beholden to, foreign adversaries. While the EO does not mention a specific country, leading theories suggest that it is aimed at China-based telecommunications provider, Huawei, as there are major concerns that Huawei conducts espionage against other nations at the behest of the Chinese government. Although Huawei has denied these claims, the four largest private US-based telecommunications companies have agreed not to use Huawei hardware in their 5G networks. ***The NTIC Cyber Center recommends both public and private sector organizations decommission all products that violate this EO and remove them from their networks.***

Current and Emerging Cyber Threats

Tech Support Scams Abuse Azure Cloud Services

Independent security researchers discovered threat actors exploiting the Microsoft Azure platform to perpetrate tech support scams and phishing campaigns. Threat actors are using the *App Services* feature within Azure to create and distribute malicious sites in vast numbers appending *azurewebsites.net* to the domain name. A sample of these analyzed websites show that the malicious campaigns display a Windows or MacOS tech support scam depending on the victims' browser settings and use a legitimate Microsoft digital certificate. ***The NTIC Cyber Center recommends users remain vigilant for tech support scams disguised as Microsoft Azure sites and avoid clicking on links or opening attachments from unknown or untrusted sources.*** To read more about how tech support scams exploit individuals, please see our product Securing Our Communities: Tech Support Scams.

Threat Actors Target Unprotected MongoDB Databases in Cyber Extortion Scheme

An independent security researcher discovered that, over the last three weeks, threat actors deleted the contents of more than 12,000 unsecured MongoDB databases, leaving only a note with a contact email address in place of the deleted data. The researcher believes that, by inviting database owners to make contact, attackers extort victims and demand payments for data recovery. There is no indication, however, that owners who pay will recover their deleted data. At this time, researchers do not know what method attackers use to find and wipe databases in large numbers, although they believe the process may be automated. ***The NTIC Cyber Center recommends owners of MongoDB databases review MongoDB's documentation on securing database instances, enabling authentication, and ensuring databases are not remotely accessible.***

Vulnerabilities

WordPress Plugin: WP Live Chat Support

Researchers at cybersecurity provider Sucri discovered a cross-site scripting (XSS) vulnerability in WP Live Chat Support, a third-party WordPress chat plugin with over 60,000 users, that could be used to inject malicious code and compromise user accounts. Engineering defects within the 'wplc_head_basic' function allowed the plugin to be updated without proper privilege checks. This lack of authentication could allow for a widespread automated attack. ***The NTIC Cyber Center recommends WordPress website administrators who installed the WP Live Chat Support plugin update it to the latest version (8.0.29) immediately. Enabling two-factor authentication on website administrator accounts and properly vetting all plugins prior to and after installation is also recommended.***

Google Bluetooth Low Energy (BLE) Titan Security Keys

Google disclosed a vulnerability affecting the BLE Titan Security Key, the company's two-factor authentication USB hardware device. Google warns that a misconfiguration in the product's Bluetooth pairing protocols may allow attackers who are within the 30-foot Bluetooth range to spoof the security key and connect to a target's paired device. The company indicates that all users of vulnerable Titan Security Key devices marked with a T1 or T2 code on the back of the device are eligible to receive a free replacement device by visiting google.com/replacemykey. ***The NTIC Cyber Center advises users of the BLE Titan Security Key to restrict use of the device to private places where attackers are not likely to be in close proximity, to unpair the security key immediately after use, and to replace vulnerable devices as soon as possible.***

Data Breach Alert

An independent security researcher recently discovered an unsecured Ifficient database containing the personal information of approximately 8 million individuals. The exposed database contained the full names, addresses, email addresses, phone numbers, dates of birth, genders, and IP addresses of users who participated in online surveys, prize giveaways, and sweepstakes competitions. ***As the exposure of this information could allow threat actors to perpetrate identity theft and other crimes, the NTIC Cyber Center recommends remaining vigilant for phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues.***

Stack Overflow disclosed a breach that occurred between May 5 and May 11, 2019 affecting approximately 250 public network users. The unnamed threat actor exploited a bug in the stackoverflow.com development tier enabling access to the website's production version. An internal investigation reveals that the attacker may have obtained some user data including names, emails, and IP addresses. Stack Overflow will notify affected users and is remediating the situation by implementing an audit of all logs, cancelling unauthorized access, consulting with a third-party forensics firm, and resetting company passwords. ***The NTIC Cyber Center recommends affected Stack Overflow users follow the security recommendations provided in the company's official notification.***

TeamViewer, an international provider of remote desktop messaging services, recently announced that the company fell victim to a breach in late 2016. While the threat actors were able to penetrate TeamViewer's systems, they were unable to cause any substantial damage as the company successfully blocked the attack. Investigators believe the threat actors are of Chinese origin, most likely APT 10 or APT 17, and used Winnti malware to create a backdoor into the company's network. ***The NTIC Cyber Center recommends network administrators block the associated Winnti Indicators of Compromise (IoCs).***

Upcoming Webinars

Latest Business Email Compromise Scams - Don't Be the Next Victim

The bad guys are getting very creative, impersonating an executive in your organization and asking for financial reports or asking employees in payroll to make changes to bank accounts. According to the FBI, their efforts have earned them an estimated $12 billion through Business Email Compromise also known as CEO fraud scams. In addition, these attackers can be working on multiple potential victims at the same time.
Join this webinar to learn more more about:

- The truth about Business Email Compromise
- How to defend against these attacks using technical and non-technical controls
- Why building a human firewall is your best last layer of defense

To register for this free webinar on Tuesday, June 4 at 11:30 am EDT, click here.

Revealing the Dark Web: How to Leverage Technologies to Alert and Block Dark Web Access

We have all seen what's possible with the Dark Web thanks to Silk Road. If you are interested in buying or selling someone's private data like social security numbers or credit card information, it is disturbingly easy to do. All you need is a computer, a Tor Browser, and cryptocurrency, and it's all completely anonymous.
So how do companies arm themselves with the right tools to protect themselves against rogue

access to the Dark Web?

Join this webinar to learn more more about:

- Understanding the Dark Web
- How leading organizations leverage technology to combat cybercrime & fraud through the Dark Web
- What companies can do to eliminate these threats

To register for this free webinar on Thursday, June 20 at 11:30 am EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Ticket scams are a type of social engineering scheme in which the perpetrator sells fake tickets to steal money, elicit personally identifiable information (PII), and/or place malware on the victim's computer. These scammers masquerade as mainstream ticket providers, third-party sellers, promotional campaigns, and individual ticket resellers. They may create fraudulent tickets for a wide variety of events including sports, concerts, theater performances, conventions, festivals, and travel. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

After Two Years, WannaCry Remains a Threat

Analytic Comment: Although the number of reported WannaCry ransomware infections plummeted shortly after a researcher discovered the ransomware's "kill switch" in 2017, vulnerabilities that allowed the ransomware to spread laterally within targeted networks remains unpatched on many systems globally. Research indicates that over one million systems worldwide may still be vulnerable to exploits known as EternalBlue and EternalRomance, tools that enabled WannaCry to spread quickly through networks. There is evidence suggesting that threat actors continue to use these exploits in other malware campaigns to spread banking Trojans such as Emotet and Trickbot. This research underscores the importance of keeping systems regularly patched and updated to protect against current and emerging cyber threats.

Finally, Child Data Privacy Could Get Much-Needed Reform in New Bill

Analytic Comment: Child data and privacy advocacy group, Common Sense, is pushing to update the Children's Online Privacy Protection Act (COPPA) as new and emerging technologies have expanded consumer data harvesting techniques. Disingenuous companies have created gambling-like games and found loopholes to bypass COPPA regulation and children are not always adept at discerning advertisements from other content. Common Sense's CEO Jim Steyer seeks data deletion rights, an end to children-aimed ads, and a ban on the sale of insecure devices to children and teens. This highlights the need of constant parental and public awareness campaigns and personal accountability as emerging technologies are outpacing policy.

Patches and Updates

Microsoft - Remote Desktop Services Security Update

Microsoft - Remote Code Execution Security Update

Mozilla Firefox

ICS-CERT Advisories

Computrols CBAS Web

Fuji Electric Alpha7 PC Loader

Mitsubishi Electric MELSEC-Q Series Ethernet Module

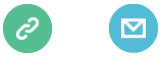
Schneider Electric Modicon Controllers

TLP:WHITE

To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.

We welcome your feedback. Please click here to complete a brief survey and let us know how we're doing.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

May 30, 2019

National Capital Region Cyber Threat Spotlight

Nearly One Million Windows Systems Contain BlueKeep Vulnerability

Researchers developed working exploits for vulnerability CVE-2019-0708, dubbed BlueKeep, that affect Microsoft's Remote Desktop Services and allow for the unauthorized execution of arbitrary code on a remote system. It is estimated that nearly one million Windows systems running Windows XP, Vista, 7, Server 2003, and Server 2008 are vulnerable. Similar to the EternalBlue exploit developed by the US National Security Agency, BlueKeep can allow malware to spread quickly through networks without user interaction and cripple systems in a similar manner to that of the infamous 2017 WannaCry ransomware attack. Cybersecurity firm GreyNoise reports heightened scanning for BlueKeep-vulnerable systems by an unknown actor; however, to date, no attacks exploiting this vulnerability have been reported. Microsoft released patches to address the BlueKeep vulnerability on May 14, 2019. ***As BlueKeep has a severity score of 9.8 out of 10, the NTIC Cyber Center recommends users and administrators of affected Windows operating systems apply the available patch as soon as possible. Additionally, we recommend network administrators proactively block TCP port 3389 at the perimeter firewall to protect unpatched systems within a secured network and disable unneeded Remote Desktop Services in their environment.***

Current and Emerging Cyber Threats

Malicious Email Campaign Threatens Recipients with Lawsuit and Bypasses Multiple Antivirus Software Products

Security firms Fortinet and Sophos identified a malicious email campaign disguised as a legal notice from a spoofed law firm. The body of the email threatens recipients with a pending lawsuit and contains a malicious Microsoft Word attachment laced with a Trojan dropper designed to install additional malware onto the victim's system. At the time of discovery, the attached Trojan bypassed multiple antivirus software products. ***The NTIC Cyber Center recommends never opening attachments or enabling macros in files received from unexpected or unsolicited emails. If you believe you have been targeted by this campaign or infected with malware, notify your organization's IT security team immediately.***

Threat Actors Exploit Android Push Notifications in Phishing Scheme

Researchers at cybersecurity firm Lookout discovered a mobile device phishing campaign targeting Android customers that attempts to elicit victims' account credentials. Threat actors exploit push notifications masquerading as alerts from Google Chrome or missed calls and using their respective icons. While not all notifications show a spoofed icon, they may contain messages designed to engage the recipient such as advertising free prizes or displaying an actionable alert. Android users will not receive these types of notifications if their devices are set to block notifications from unknown domains. ***The NTIC Cyber Center recommends Android users remain vigilant for phishing attempts disguised as push notifications and refrain from clicking on links from unknown or untrusted sources. We also recommend Android users restrict notifications from unknown domains and block the associated spam domains listed on BleepingComputer.***

New Mirai Botnet Variant Uses 13 Exploits

Researchers at Trend Micro identified a new variant of the Mirai botnet (Backdoor.Linux.MIRAI.VWIPT) that uses 13 exploits in a single campaign and contains brute-forcing capabilities along with its common distributed denial-of-service (DDoS) and backdoor behavior. This variant is known to exploit and infect vulnerable and exposed routers, surveillance products, and other internet-connected devices. Researchers state that the malware spreads in various ways and uses three keys for encryption. It can be propagated through a batch of URLs, some of which serve as command-and-control servers as well as download and dropper links. This is not the first time the 13 exploits have been used by threat actors as they have also been used in

previous malware campaigns. ***The NTIC Cyber Center recommends network administrators block the associated Mirai Indicators of Compromise (IoCs) and implement the appropriate vendor patches if and when they become available. Additionally, we recommend users of internet-connected devices always change any default login credentials prior to use.***

Phishing Emails Masquerade as Microsoft Office 365 File Deletion Alerts

A Microsoft Office 365 phishing campaign masquerades as the "Office 365 Team" disseminating fake alerts to victims. These email alerts try to trick recipients into thinking that a large quantity of files was deleted from their Office 365 accounts and entices them to click on an embedded link labeled *View Alert Details*. When clicked, the malicious link delivers recipients to a fraudulent Microsoft login page crafted to steal Microsoft account credentials. Further inspection of the associated phishing sites reveals that they are signed with Microsoft certificates and hosted on Microsoft's Azure cloud platform to lend credence to the scam. Webpages hosted on Azure can feature landing pages on the domains windows.net and azurewebsites.net. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as alerts from Office 365, avoid opening unexpected emails, and refrain from clicking on links from unknown or untrusted sources. Remember that, for Microsoft and Outlook account logins, legitimate domains for these resources only include microsoft.com, live.com, and outlook.com.***

Magecart Threat Groups Use Iframe-Based Phishing System to Steal Payment Card Data

According to a Malwarebytes security researcher, cybercriminals perpetrating Magecart attacks have employed new methods for stealing payment card information from Magento-powered ecommerce stores. The researcher found that, instead of using traditional JavaScript skimmers, criminals configured scripts on checkout pages to launch rogue iframe pop-up windows that prompt customers for payment card information. This technique may allow Magecart groups to steal payment card information from sites that forward customers to a secure payment service provider instead of processing their own payments. ***The NTIC Cyber Center recommends customers of ecommerce retailers remain vigilant for indications that a checkout page may be compromised, which may include being asked twice to enter payment information or being prompted for payment card details before being forwarded to a secure payment service provider.***

To read more about the threat Magecart poses to ecommerce websites, please see our recent Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Vulnerabilities

Microsoft Windows 10 BYPASS and InstallerBypass

A security researcher known only as SandboxEscaper recently discovered two Windows 10 local privilege escalation vulnerabilities called CVE-2019-0841-BYPASS and CVE-2019-0841-InstallerBypass. BYPASS can circumvent CVE-2019-0841 and lets threat actors to modify an authentication component knows as DACL (discretionary access control list) allowing unauthorized low level users higher level permissions. InstallerBypass works when threat actors place code in the Windows system32 folder and aggregate them with escalated privileges. According to SandboxEscaper, InstallerBypass could be used with malware. There is currently no patch or workaround available. ***The NTIC Cyber Center recommends Windows 10 users monitor systems for unusual and suspicious activity and update Windows 10 if and when a patch becomes available.***

Docker

An unpatched flaw in Docker affects all versions of the platform and allows threat actors read and write access on the host server. The vulnerability is attributed to a process in which Docker manages a portion of symbolic links. In this way, a *FollowSymlinkInScope* function can be exploited using a basic time-to-check-time-to-use (TOCTOU) attack. This affects the *docker cp* function that copies files between containers and local file systems. There is currently no patch or workaround available; however, a patch has been submitted and is currently under code review. ***The NTIC Cyber Center recommends users to monitor systems for unusual and suspicious activity and update Docker if and when a patch becomes available.***

Data Breaches and Leaks

Real estate title insurance and settlement service provider First American Financial Corp. (FAF) accidentally exposed approximately 885 million sensitive documents containing personally identifiable information (PII) dating back from 2003. The PII exposed information of both buyers and sellers, which may have included wire transactions, bank account numbers, Social Security numbers, driver's license images, account statements, and other information. FAF attributed the leak to a design flaw in one of its production applications letting unauthenticated users access the

unencrypted data with only a web browser. It is currently unknown how many people have accessed this information. FAF disabled the external facing component of the application and hired a forensics firm to investigate the extent and impact of the data leak. ***The NTIC Cyber Center recommends FAF customers and clients remain vigilant for phishing attempts perpetrated through email, telephone, or other avenues, and monitoring financial accounts closely, reporting any unauthorized activity to the associated financial institutions. We also recommend immediately placing a security freeze on credit files with credit bureaus Equifax, Experian, and TransUnion.***

Google announced that the company inadvertently stored passwords of some G Suite Enterprise users in an unhashed state since 2005. Google indicates that though the passwords were unhashed, they were stored in an encrypted infrastructure and are not believed to have been improperly accessed or misused. The company has since fixed this issue and issued a notice to administrators of affected G Suite accounts. ***The NTIC Cyber Center recommends G Suite administrators reset affected accounts and passwords and enable two-factor authentication on all accounts that offer it.***

A hacker responsible for stealing over one billion user credentials since early 2019 claims to have posted another cache of breached data, this time from the graphic design service Canva. The data includes the customer names, usernames, email addresses, location, password hashes, and Google tokens of over 139 million Canva website users. ***The NTIC Cyber Center recommends Canva users reset their passwords as soon as possible and monitor their accounts for suspicious activity. Additionally, we encourage the use of lengthy and complex passwords that are unique to every online account to reduce the risk of further compromise in the event of a data breach. We also recommend enabling two-factor authentication as an additional security measure on any account that offers it.***

News aggregation website Flipboard disclosed a data breach that exposed the personal information of over 100 million users. The company believes hackers accessed Flipboard databases from June 2, 2018 to March 23, 2019 and again from April 21-22, 2019 and managed to download content such as users' names, usernames, hashed passwords, email addresses, and digital login tokens used to connect to third-party accounts. Flipboard indicates they have disconnected digital tokens and have forced password resets for all users. ***The NTIC Cyber Center recommends Flipboard users ensure their account passwords are changed and remain vigilant for targeted phishing attempts resulting from the exposure of personal information.***

REDTAIL TECHNOLOGY

Client relationship management software company Redtail Technology issued a notification of a data breach that publicly exposed the personal information belonging to clients of financial advisors who use the company's software. According to the firm, a technical error caused client information to be captured and posted to a publicly accessible file on the web. The data leak, which Redtail identified on March 4, includes client names, addresses, dates of birth, and Social Security numbers. ***As Redtail Technology's products are popular with financial advisors, the NTIC Cyber Center recommends customers of financial advisors remain vigilant for phishing attempts and consider placing a fraud alert or security freeze on their credit file.***

Upcoming Webinars

Bay Dynamics

Orchestrating Data Protection from the Endpoint to the Cloud

Today's organizations face a daunting set of challenges, along with some incredible opportunities, within the context of advancing their existing security infrastructure. As practitioners continue to seek out new techniques for managing the sheer volume of security data at their fingertips, there are tangible benefits found in emerging models for centralized analysis and orchestrated response.

Advanced analytics that integrate existing data and enable automated orchestration of security incidents, along with rapid remediation, offer a huge leap forward in addressing today's biggest hurdles. By taking the output of data loss prevention (DLP), cloud access security broker (CASB), cloud security, and endpoint platforms and applying machine learning (ML), organizations can optimize data protection, making the most of available resources.

Register for this webinar and learn about:

- Integrating security data, analysis, and response
- Addressing emerging cloud requirements
- Orchestrating incident response workflows
- Using ML to build continuous improvement

To register for this free webinar on Wednesday, June 19 at 11:30 am EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Rental scams are a type of social engineering scheme in which perpetrators advertise fake apartment, condominium, home, or vacation rental listings with the intent of defrauding those seeking to lease such properties. These scams frequently target students, prospective residents, and tourists interested in renting short-term or long-term stay properties listed on sites such as Craigslist, AirBnB, VRBO, and others. Rental scams are particularly prevalent during busy summer months when moving and vacation seasons peak and in markets where rental properties are in high demand. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Increase in Vulnerabilities as Report Finds Organizations Are Not Cyber Mature

Analytic Comment: The latest global threat intelligence report from Dimension Data reveals that the average cybersecurity maturity rating of organizations is 1.45 on the company's scale of one through five. The global finance and technology sectors rank the highest scores 1.71 and 1.66, respectively. The American finance sector rates above average at 1.71 compared to the 1.45 global

average, while the technology sector lags behind the 1.45 global average at 1.35, even though it is the most-targeted sector. Since 2017, security vulnerabilities have increased 12.5 percent, breaking previous records. Of all the attack types, web attacks are the most prevalent, composing 32 percent of the total followed by reconnaissance (16 percent), service-specific attacks (13 percent), and brute-force (12 percent). This report highlights the need for all sectors to make security a higher priority through increased security standardization, awareness, implementation, and enforcement as threats become increasingly diverse and global.

DoD Wants Concepts for Protecting IT against Quantum Computing

Analytic Comment: The Defense Information Systems Agency (DISA) is soliciting information from commercial tech companies on cryptographic algorithms and solutions that would protect US Department of Defense (DoD) information technology systems against quantum-computing attacks. DISA fears that, among numerous other concerns, this new technology may allow adversaries to crack public-key cryptography data encryption used in secure online transactions and communications. As the future impacts of quantum-computing are currently unknown, DISA believes that the US DoD must prepare now to ensure information security systems are resistant to large-scale attacks. DISA's concerns about quantum-computing underscore the gravity of this inevitable technological development and its potential repercussions for which all organizations should be preparing.

ICS-CERT Advisories

Emerson Ovation OCR400 Controller

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

June 6, 2019

National Capital Region Cyber Threat Spotlight

National Security Agency Releases Advisory on BlueKeep Vulnerability

The National Security Agency (NSA) released a cybersecurity advisory for vulnerability CVE-2019-0708, dubbed BlueKeep, that affects Microsoft's Remote Desktop Services and allows for the unauthorized execution of arbitrary code on a remote system. It is estimated that nearly one million computers running legacy versions of the Windows operating system, including Windows XP, Vista, 7, Server 2003, Server 2008, and Server 2008 R2, are vulnerable. This flaw is potentially "wormable" and could allow malware to spread quickly through networks without user interaction. The NSA recommends applying the following patches for each respective Windows operating system:

- Windows XP/Windows Server 2003 – Security Patch KB4500331
- Windows Vista/Windows Server 2008 – Security Patch KB4499180 or Monthly Rollup KB4499149
- Windows 7/Windows Server 2008 R2 – Security PatchKB4499175 or Monthly Rollup KB4499164

As BlueKeep has a severity score of 9.8 out of 10, the NTIC Cyber Center recommends users and administrators of affected Windows operating systems apply the available patches as soon as possible. Additionally, we recommend network administrators proactively block TCP port 3389 at

the perimeter firewall to protect unpatched systems within a secured network, enable Network Level Authentication, and disable unneeded Remote Desktop Services in their environment.

Editor's Comment: Although the NTIC Cyber Center shared information about BlueKeep in last week's cyber threat bulletin, we felt that it was prudent to re-emphasize the importance of patching vulnerable Windows operating systems, especially as hackers and researchers are actively developing tools to exploit this vulnerability.

Current and Emerging Cyber Threats

New Phishing Campaign Spoofs Outlook Undelivered Mail Message

A new Microsoft Outlook phishing campaign masquerades as fraudulent alerts to victims. These email alerts contain the subject line “Notifications | undelivered emails to your inbox" and try to trick recipients into clicking a phishing link by making them think they have a queue of undelivered email still residing on Outlook servers. When clicked, the malicious link delivers recipients to a fraudulent Microsoft login page crafted to steal Microsoft account credentials. Further inspection of the associated phishing sites reveals that they are hosted on hijacked websites, potentially making them easier to discern from their legitimate counterparts. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as alerts from Microsoft Outlook, avoid opening unexpected emails, and refrain from clicking on links from unknown or untrusted sources. Remember that, for Microsoft and Outlook account login pages, legitimate domains for these resources only include microsoft.com, live.com, and outlook.com.***

Newly Discovered HiddenWasp Malware Targets Linux Systems

Cybersecurity firm Interzer identified a new strain of malware called HiddenWasp that targets Linux systems. While most Linux-specific malware performs distributed denial of service (DDoS) attacks and cryptomining activity, HiddenWasp is a combination of a Trojan and a rootkit and is designed to take full remote control of an infected system. It shares similar code with other malware such as Mirai and the Azazel rootkit, but currently evades antivirus detection with a zero percent detection rate by all major antivirus platforms. Leading theories suggest threat actors target victims after conducting reconnaissance or by searching for systems that have already been compromised by another variant of the rootkit. Researchers noted similarities between this malware and other Chinese malware families, but their attribution to China is made with low confidence. ***The NTIC Cyber Center recommends network administrators block the associated HiddenWasp indicators of compromise (IoCs) and implement the mitigation strategies listed in the Interzer report.***

OilRig Microsoft Exchange Hacking Tool Discovered

An unknown party leaked a new email hacking tool, dubbed Jason, purportedly used by OilRig, an Iranian nation-state hacking group. Jason can hijack Microsoft Exchange email accounts by brute-forcing online Microsoft Exchange services and is currently not detected by any VirusTotal antivirus detection engines. The tool was leaked within a channel on Telegram, an encrypted communications platform. ***The NTIC Cyber Center recommends Microsoft Exchange users monitor systems for unusual and suspicious activity and update Microsoft Exchange if and when a patch becomes available. We also strongly urge all users to use lengthy, complex, and unique passwords for each account and enable multifactor authentication on any account that offers it to limit the impact of credential compromise.***

BlackSquid Targets Web Servers to Mine Cryptocurrency

Trend Micro researchers discovered BlackSquid malware, a new cryptojacking threat that turns targeted web servers into Monero cryptominers using a variety of security exploits. BlackSquid may contaminate systems through removable network drives, compromised websites, and the exploitation of known vulnerabilities. It can conduct brute-force attacks and spread in a worm-like manner. When Blacksquid compromises a server, it attempts to evade detection and analysis by identifying systems that contain analytical tools, virtual machines, sandboxes, and debuggers, and by terminating the infection process when these tools are discovered. Researchers suggest that Blacksquid is in a testing phase and may be used for other types of attacks in the future. ***The NTIC Cyber Center recommends network administrators block the associated BlackSquid indicators of compromise (IoCs) contained in the Trend Micro report.***

Vulnerabilities

Microsoft Windows Remote Desktop Protocol

The Carnegie Mellon University Software Engineering Institute released an advisory on Tuesday to warn Microsoft Windows users about CVE-2019-9510, a zero-day vulnerability that can allow unauthorized users to gain remote access to a system. By exploiting this vulnerability, attackers can hijack a remote desktop session and circumvent the Windows lock screen, even if multifactor authentication is enabled. Threat actors can achieve this by interrupting the Remote Desktop Protocol (RDP) client connection, triggering a reconnection while the user is away from the computer. When the system reconnects, it circumvents the Windows lock screen, allowing a local threat actor access to an unlocked computer after the RDP session ended. This vulnerability affects

systems running Windows 10 version 1803 and newer, as well as Server 2019, that have RDP enabled. There is currently no known patch available. ***The NTIC Cyber Center recommends Windows users and administrators who use RDP in their environment disconnect all RDP sessions prior to locking their systems to prevent unauthorized users from exploiting this vulnerability.***

Data Breaches and Leaks

Healthcare diagnostics companies Quest Diagnostics and LabCorp both disclosed that a breach of a third-party billing collection provider, American Medical Collection Agency (AMCA), resulted in the exposure of billing details for millions of customers. Quest Diagnostics reports that their breach affected nearly 12 million Quest Diagnostics customers, while LabCorp indicates 7.7 million of their customers are affected. AMCA believes that from August 1, 2018 through March 30, 2019 an unauthorized user obtained access to AMCA systems and may have been able to view information such as customer bank account data, payment card numbers, medical information, and Social Security numbers. As AMCA also provides collection services to Quest Diagnostics contractor Optum360, customers of Optum360 may also be affected. AMCA does not believe any of the breached data exposed laboratory test results or diagnostic information of consumers. ***The NTIC Cyber Center recommends customers of Quest Diagnostics, LabCorp, or Optum360 monitor their account statements, immediately notify their financial institutions of any unauthorized or suspicious activity, and consider placing a fraud alert or security freeze on their credit file with Equifax, Experian, or TransUnion.***

Checkers Drive-In Restaurants released a customer notice disclosing a data breach that occurred at 102 locations of Checkers and Rally's restaurants throughout the United States. The firm believes that that malware installed on point-of-sale systems allowed cyber criminals to steal customer payment card numbers, expiration dates, card verification codes, and cardholder names at certain

restaurants during varying affected time periods. Within the NCR, this data breach may have affected customers of Checkers at 826 Berryville Avenue, Winchester, VA from March 25, 2018 to April 18, 2019. Other affected establishments may be identified here. ***The NTIC Cyber Center recommends that customers who made purchases at affected restaurants during a relevant time period monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.***

AT THE FOREFRONT
UChicago Medicine

An independent security researcher discovered a misconfigured and unprotected ElasticSearch server exposing the personal information of more than 1.6 million University of Chicago Medicine donors. The 34 GB database contained information on prospective and previous benefactors such as full name, date of birth, address, phone number, email address, gender, marital status, wealth information, and communication notes. ***Although the University of Chicago does not believe any individual besides the security researcher accessed the exposed database, the NTIC Cyber Center recommends University of Chicago Medicine affiliates and donors remain vigilant for phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues.***

PYRAMID

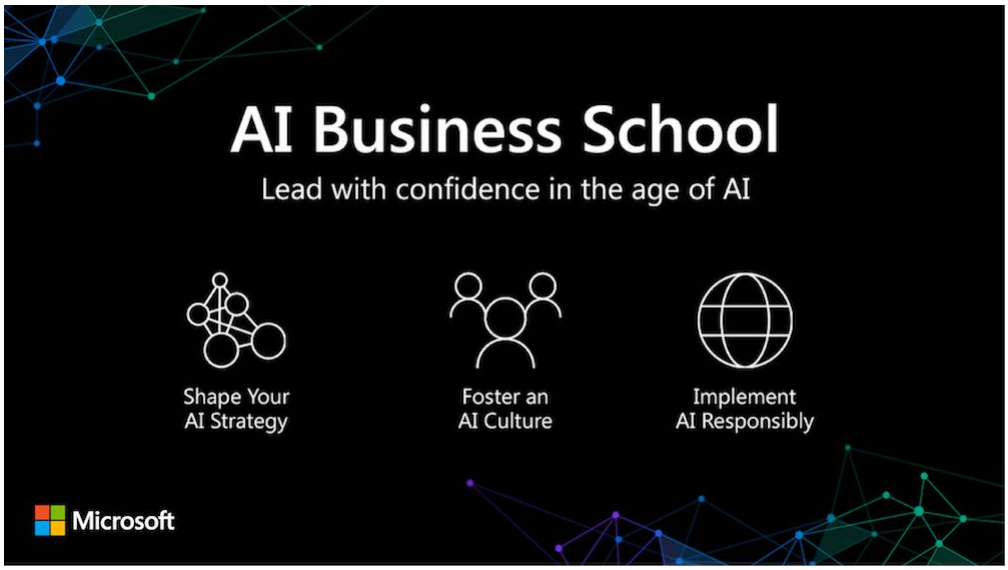
Security researchers discovered an unsecured database owned by the Pyramid Hotel Group, a hotel and resort management company, that has been publicly viewable since April 19, 2019. While the database does not include any customer details, it does include security audit log data for hotels' networks and information on operating systems, security policies, internal networks, and application logs. Additional sensitive information revealed in this data breach includes:

- device names
- IP addresses of inbound connections
- open ports
- malware alerts
- restricted applications
- login attempts
- local computer names and addresses
- application errors
- server names and operating system details
- information identifying cybersecurity policies

- brute-force attack detection
- employees' full names and usernames

The Pyramid Group manages hospitality properties throughout the United States and Europe, representing brands such as Courtyard, DoubleTree by Hilton, Embassy Suites, Hilton, Holiday Inn, Hyatt, Le Meridien, Marriott, Radisson, Residence Inn, Renaissance, Sheraton, and more. Researchers fear the leak of sensitive network information may have allowed threat actors to surveil the networks of any hotel implicated in the exposure, gather information about administrators and users, and formulate attack methodologies based on cybersecurity events alerted in network security logs. As the breach exposed information on network devices that control hotel locking mechanisms, electronic in-room safes, and other physical security management systems, this event may also have implications for the physical security of hotel guests. ***The NTIC Cyber Center recommends network administrators of affected properties secure servers and implement proper access rules to prevent similar breaches of information or unauthorized access to sensitive network data.***

Training Opportunity



Microsoft Offers Online Artificial Intelligence Course for Government Employees

On Tuesday, May 28, Microsoft launched a free online course to help government leaders, policy makers, and administrators learn more about how technologies infused with artificial intelligence (AI) can help their stakeholders, constituents, and citizens. Using AI, government organizations can find ways to improve public safety and reduce the time people spend waiting in line for services.

According to Microsoft's website, this curriculum will include:

- A video lecture from Peter Zemsky, Eli Lilly chaired professor of innovation and strategy at INSEAD graduate business school, on why and how governments can identify the right opportunity to use AI
- A case study illustrating how the city of Espoo, Finland, is working to modernize life for its residents
- A demo showcasing how governments can use intelligent bots to help citizens access resources

To access Microsoft's AI Business School for Government, click here.

Upcoming Webinars

riskrecon™

Managing Risk Exposure in a Hyper-Connected World: Revelations from the Internet Risk Surface Report

The old demarcation lines of cybersecurity responsibility have been erased. In this new landscape, risk surface is the unforeseen undercurrent of high velocity digital business.

"Risk Surface Management" is a revolutionary shift in third-party risk management. It's an approach to self-reporting on third-party risk - the risk that exists as a result of the connections between you and every company with whom you do business.

RiskRecon is proud to present a webinar on risk surface and the ***Internet Risk Surface Report***, which will reveal the true expanse of enterprise risk and forecasting solutions for managing risk surface in a hyper-connected and hyper-exposed world.

Register for this webinar and you will learn:

- Exactly what risk surface is and where it exists in relation to your organization's digital assets
- What your responsibility is for your organization's sensitive data
- Common components of risk surface
- Best practices for assessing the risk of your third- and fourth-party vendors

To register for this free webinar on Wednesday, June 26 at 1:30 pm EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Student loan forgiveness scams, also known as student loan debt relief scams, are a type of social engineering scheme in which the perpetrator elicits money from victims through fraudulent student debt relief services. Perpetrators emotionally manipulate those eager, or struggling, to pay off their student loan debts by offering to forgive payments, consolidate loans, or refinance for a service charge. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Industry is Not Prepared for the IIoT Attacks that Have Already Begun

Analytic Comment: Results of a recent survey conducted by cybersecurity firm Irdeto indicate that 80 percent of industry organizations in China, Germany, Japan, the United Kingdom, and the United States have experienced a cyber attack against their Industrial Internet of Things (IIoT) devices in the last 12 months. 83 percent of those respondents, which include security professionals in connected health, connected transport, connected manufacturing, and IIoT device and technology manufacturing organizations, express concern that they will experience a future cyber attack against these devices. This survey demonstrates that industry organizations are largely unprepared for the

increased challenges of integrating IIoT devices within their environment. Additionally, Irdeto speculates that, as IIoT devices proliferate within industry networks and reliance on connectivity provided by these devices increases, the costs associated with cyber attacks on industry organizations could increase dramatically.

Baltimore Estimates Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts

Analytic Comment: Baltimore's budget office estimates that costs resulting from last month's Robbinhood ransomware attack on the city are likely to total at least $18.2 million. The city has spent $4.6 million on recovery efforts so far with an additional $5.4 million projected to be needed by the end of the year. In addition to funds spent directly on recovery efforts, the city estimates having incurred an additional $8.2 million as a result lost or delayed revenue. The city reports having restored email access for some employees, but is still in the process of rebuilding other affected systems. Insights into the city's challenges in the wake of the attack demonstrate the tremendous costs associated with both remediation and lost income as well as the disruptive and lasting impacts of ransomware on organizations.

Patches and Updates

Apple AirPort Extreme and AirPort Time Capsule

Chrome for Android

Cisco

NVIDIA GeForce Experience

Quest Kace System Management (K1000) Appliance

ICS-CERT Advisories

AVEVA Vijeo Citect and CitectSCADA

Emerson Ovation OCR400 Controller

Geutebrück G-Cam and G-Code

PHOENIX CONTACT FL NAT SMx

PHOENIX CONTACT PLCNext AXC F 2152

We welcome your feedback.

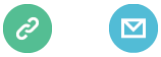
Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.



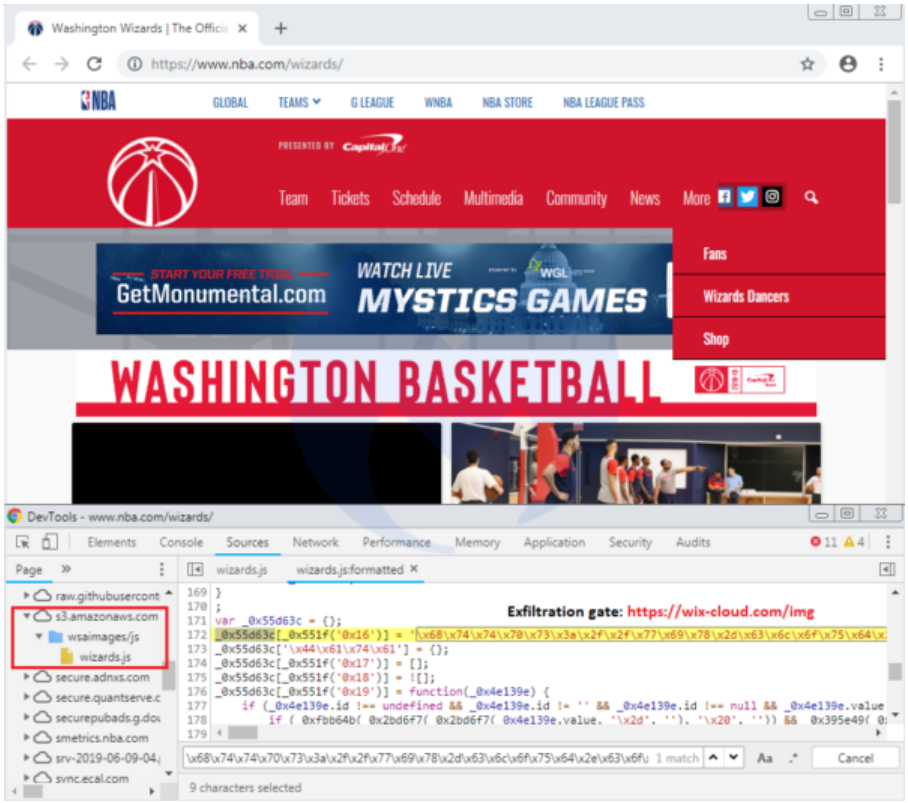
NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

June 13, 2019

National Capital Region Cyber Threat Spotlight



(Image Source: Malwarebytes)

New Magecart Skimming Tactic Impacts Washington Wizards Webpage

MalwareBytes researchers report that Magecart cyber threat groups, traditionally known for conducting payment skimming attacks on ecommerce websites, have widened their scope to target any websites that load external resources from Content Delivery Networks (CDNs). Magecart groups continue to compromise CDNs by injecting resources such as JavaScript libraries with skimming code, but the groups have extended these techniques to skim non-ecommerce websites as well to exfiltrate user input data from

sources such as account login fields.

This new tactic suggests that Magecart groups may be taking a more opportunistic approach to data theft by casting a wider net through CDN compromise rather than targeting specific websites. Many organizations rely on CDN-hosted JavaScript libraries to reduce loading times or to provide data analytics for websites and, for this reason, CDNs hosted on improperly secured cloud storage buckets potentially provide a larger attack surface for threat actors than individual websites embedded with vulnerable ecommerce platforms. The effects of this shift in tactics have been observed locally as Malwarebytes researchers recently discovered that the webpage for the Washington Wizards basketball team, hosted on the National Basketball Association's website, loaded a compromised JavaScript library featuring Magecart data skimming code. Fortunately, this website does not contain user input fields or process merchandise orders; the franchise's shop is hosted on a different domain that is not believed to have been affected. Researchers also identified other impacted organizations, including a news portal, a lawyer's office, a software company, and a small telecommunications operator, with websites loading similarly compromised resources configured to steal user input data.

Based on these observations, the NTIC Cyber Center assesses with high confidence that Magecart attacks are a persistent threat not only to websites built using vulnerable ecommerce platforms, but also to websites that use CDNs to optimize website performance and availability.

To read more about the threat of Magecart attacks and for mitigation strategies, please see our recent Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Federal Agency Announcements

Internal Revenue Service Reminds Taxpayers to Remain Vigilant of Tax Scams

The Internal Revenue Service (IRS) issued a reminder to US taxpayers that tax-related phone and email scams continue year-round, even after tax-filing season has ended. This reminder also urges taxpayers to remain vigilant for two new variations of these tax-related scams. In one version, scammers threaten to suspend or cancel victims' Social Security numbers if they do not return their phone calls or pay a specified fee. In the other version, scammers mail a fraudulent lien or levy notification letter through the US Postal Service to victims accusing them of owing delinquent taxes to the "Bureau of Tax

Enforcement," a non-existent agency. ***The NTIC Cyber Center would like to remind all members to maintain awareness of potential scams, tax-related and otherwise, designed to steal victims' money and personal information.***

To learn more about IRS tax scams and how to recognize them, please read our product titled ***Securing Our Communities: IRS Tax Scams***. To learn about other scams impacting the National Capital Region, please see our Security Our Communities product series on our website.

FBI Warns of Cyber Actors Exploiting "Secure" Websites in Phishing Campaigns

The US Federal Bureau of Investigation (FBI) recently published a Public Service Announcement (PSA) warning that cyber threat actors are exploiting "secure" websites — websites that display a green lock symbol and Hypertext Transfer Protocol Secure (HTTPS) in the URL field of a web browser — in phishing campaigns to trick victims into thinking the malicious websites are safe to use. They achieve this by obtaining third-party website certificates for phishing pages that spoof websites of legitimate organizations. If unsuspecting victims enter sensitive information into the site, the cyber threat actors behind the campaign will steal that information and likely use it to gain unauthorized access to victims' accounts, commit identity theft, or they will sell it to other criminals on hacker forums and illicit online marketplaces. ***The NTIC Cyber Center recommends all members review the FBI's PSA for prevention and mitigation strategies, remain vigilant for potential phishing campaigns that use this technique, and carefully scrutinize website domain names prior to entering any personal or sensitive information into the site.***

Current and Emerging Cyber Threats

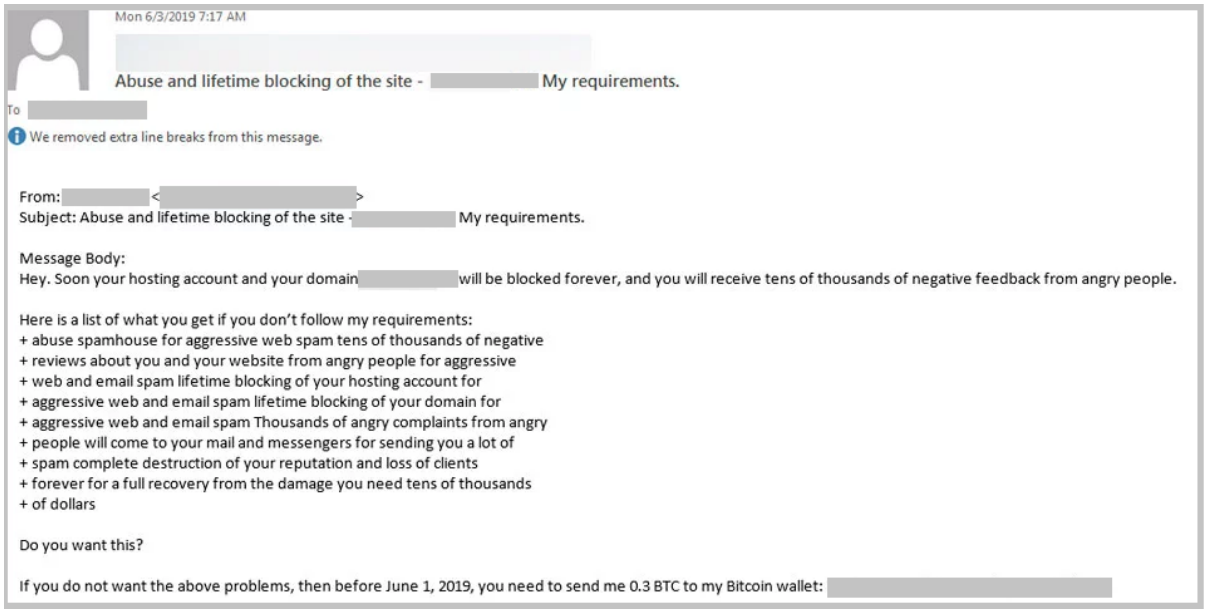
Phishing Campaign Requests Victims' Recovery Phone Numbers

A new phishing campaign sends emails that masquerade as "Server Notifications" and contain the subject line "New Account Verification!" that threaten recipients with account deletion if they do not add a

recovery phone number to their email accounts. In the body of the emails, recipients are prompted to click an embedded link labeled *Add Recovery Number Now* that will deliver them to a spoofed webmail login page designed to capture account credentials. Further inspection of the phishing sites revealed that they are hosted on compromised WordPress websites. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as alerts from their email service providers, avoid opening and acting upon unexpected emails, and refrain from clicking on links from unknown or untrusted sources. We also recommend never entering any account credentials or other sensitive information into a website that launches after clicking a link in an email or text message. Instead, visit the website directly by entering the address in the URL field of the browser before entering any sensitive information.***

Cyber Extortion Scheme Targets Website Administrators

Bleeping Computer reports that a new email-based cyber extortion scheme is targeting website administrators, threatening to ruin their websites' online reputations and place their domains on blacklists if they do not pay the perpetrators 0.3 Bitcoin (approximately $2,400). The extortion emails list the consequences victims will supposedly suffer if they do not submit payment by a specified date. The email's subject line contains the words *Abuse and lifetime blocking of the site* and *My requirements* and includes the target's domain name. Below is an example of the extortion email used in this campaign:



Mon 6/3/2019 7:17 AM

Abuse and lifetime blocking of the site - [redacted] My requirements.

To [redacted]

We removed extra line breaks from this message.

From: [redacted] <[redacted]>
Subject: Abuse and lifetime blocking of the site - [redacted] My requirements.

Message Body:
Hey. Soon your hosting account and your domain [redacted] will be blocked forever, and you will receive tens of thousands of negative feedback from angry people.

Here is a list of what you get if you don't follow my requirements:
+ abuse spamhouse for aggressive web spam tens of thousands of negative
+ reviews about you and your website from angry people for aggressive
+ web and email spam lifetime blocking of your hosting account for
+ aggressive web and email spam lifetime blocking of your domain for
+ aggressive web and email spam Thousands of angry complaints from angry
+ people will come to your mail and messengers for sending you a lot of
+ spam complete destruction of your reputation and loss of clients
+ forever for a full recovery from the damage you need tens of thousands
+ of dollars

Do you want this?

If you do not want the above problems, then before June 1, 2019, you need to send me 0.3 BTC to my Bitcoin wallet: [redacted]

(Image credit: BleepingComputer.com)

The NTIC Cyber Center recommends targets of this scheme refrain from submitting any payment to the perpetrator and monitor websites and associated email accounts for any suspicious activity or compromise. Additionally, we recommend all website administrators secure their domain registration accounts and web hosting control panels with multifactor authentication, if available, and consider using a domain privacy service to protect ownership information and reduce the risk of additional

targeting. If you are impacted by this or another cyber extortion scheme, file a report with your local police department and submit a complaint to the FBI's Internet Crime Complaint Center (IC3).

New Mirai Botnet Malware Variant Employs Eight Exploits

Palo Alto Networks Unit 42 research group discovered a new variant of the Mirai botnet malware that exploits vulnerabilities in various Internet-of-Things (IoT) devices including wireless presentation systems, television set-top boxes, and smart home controllers. The Mirai malware family originally compromised IoT devices exclusively using default credentials to gain unauthorized access, but newer variants use publicly available exploits to spread and compromise vulnerable devices. Researchers deduce that this new feature allows Mirai to gauge bot counts and maximize the number of bots gained through Mirai exploitations. ***The NTIC Cyber Center recommends changing all default credentials on IoT devices and their associated administrator control panels as well as applying available security patches and firmware updates immediately after connecting them to a network. We also recommend placing IoT devices behind a firewall, blocking any unneeded ports that would allow external and unauthorized access, and monitoring the network for suspicious activity. If devices have publicly known vulnerabilities, but no updates or patches are available, we recommend immediately decommissioning the devices, if possible. For a list of Indicators of Compromise (IoCs) associated with this threat, please review Unit 42's report here.***

GoldBrute Botnet Targets Windows Systems with Remote Desktop Protocol Enabled

A new botnet, dubbed GoldBrute, is currently scanning the internet for exposed and unprotected Remote Desktop Protocol (RDP)-enabled Windows machines and creating a list of these vulnerable systems. According to a researcher from security firm Morphus Labs, GoldBrute currently has only one command-and-control server, currently located on a New Jersey-based cloud hosting provider, and does not appear to contain a mechanism for maintaining persistence on exploited systems. As GoldBrute's purpose has not yet been identified, the researcher believes that the threat actor behind the botnet may intend to sell the collected information on hacker forums or marketplaces or to sell access to the botnet itself. ***The NTIC Cyber Center recommends all network and system administrators disable all unneeded instances of RDP in their environments, implement strong authentication protocols and IP whitelisting on systems that do need RDP enabled, and block outbound connections from TCP/UDP port 8333. For more information about this threat, including IoCs, please see BleepingComputer's report here.***

RIG Exploit Kit Delivers Buran Ransomware through Malicious Advertisements

The RIG Exploit Kit is currently distributing a new ransomware variant, Buran, through online malvertising (malicious advertising) campaigns. When victims visit websites hosting the associated malicious advertisements, they will be redirected to the RIG exploit kit, which will attempt to exploit vulnerabilities in victims' web browsers, deliver the ransomware payload, and execute it. The ransomware generates a ransom note text file named *!!!your files are encrypted!!!* and appends a unique identifier as an extension on encrypted files. There is currently no publicly available decryption tool for this variant. ***The NTIC Cyber Center recommends users and administrators keep all systems and software up-to-date with the latest security patches, implement a robust data backup strategy, and use a reputable ad blocker when browsing the web.***

To reduce your risk of a ransomware infection, we encourage you to visit our website and download the NTIC Cyber Center Ransomware Mitigation Guide and the NTIC Cyber Center Guide for Cyber Incident Response Planning.

Vulnerabilities

Microsoft Windows 10 Zero-Day Vulnerability Impacts Edge Browser

An exploit developer known as SandboxEscaper recently discovered a Microsoft Windows 10 zero-day local privilege escalation (LPE) vulnerability that, if abused, could be used to obtain administrator rights on normal user accounts, install programs, and to access, modify, and delete data on systems and network shares. The vulnerability is created when someone using a normal user account deletes files and folders associated with the Microsoft Edge browser in the user profile's *AppData* folder. Although the proof of concept exploit has only been demonstrated using Microsoft Edge, SandboxEscaper claims that other software packages can create the same LPE vulnerability. ***The NTIC Cyber Center recommends Windows 10 users monitor their computers for unusual and suspicious activity and update their operating system if and when a patch becomes available.***

Exim Mail Transfer Agent

A critical remote command execution vulnerability found in Exim, a mail transfer agent that runs on Unix platforms, puts over three million machines in the United States at risk of exploitation by allowing unauthenticated remote attackers to gain root privileges and execute arbitrary commands on mail servers. This vulnerability impacts Exim versions 4.87 to 4.91. ***The NTIC Cyber Center recommends all Exim server administrators update to version 4.92 as soon as possible.***

Data Breaches and Leaks

US Customs and Border Protection (CBP) confirmed a data breach that exposed digital photos of travelers and vehicles crossing the US border. The stolen data affects less than 100,000 people from "a few specific lanes at a single border" during an unspecified time frame and does not include airline travel data, passports, or other travel documents. CBP states that the breach resulted from a compromised subcontractor who violated CBP security protocols and transferred traveler and vehicle photos to an external network. ***The NTIC Cyber Center recommends all network administrators implement a reputable data loss prevention solution to detect and prevent the unauthorized exfiltration of sensitive information.***

Evite, a social-planning website, disclosed a data breach that compromised user information collected prior to 2013. According to Evite, an unauthorized party gained access to an inactive data storage file beginning February 22, 2019. This file contained names, usernames, email addresses, passwords, and possibly dates of birth, phone numbers, and mailing addresses if provided by Evite users. The company states that no financial account information or Social Security numbers were compromised in this breach. ***The NTIC Cyber Center recommends all Evite users change their account passwords immediately. If Evite account holders used the same login credentials for other websites and online services, we recommend changing those as well to mitigate against credential stuffing attacks resulting from this breach. We also recommend affected Evite users remain vigilant for phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues.***

Upcoming Webinars

GOVINFO SECURITY®

Ensure Enterprise-Grade Security for Your Mobile Apps

5G promises to be a game changer for mobile. Technology has leaned forward to enable massive processing power at blistering speeds, yet the true value of mobile as not just a communication device, but a compute platform, has yet to be realized. Why?

The number one gating factor for true edge compute on mobile is security, and that's a hard thing to get into a mobile app.

Ensuring enterprise-grade security in your custom or third party corporate app does not have to be complicated, nor should it stretch the limits of your development team.

Discover how to easily secure custom mobile apps with enterprise-grade security controls without having to rely on hours of DevOps and SecDevOps time and expense.

Register for this webinar and you will learn how leading organizations are:

- Keeping sensitive corporate information out of the wrong hands with app-level security controls that don't get in the way of an intuitive mobile user experience
- Accelerating the development of secure custom apps without coding
- Realizing the power of mobile to extend their enterprise workforce, reach customers and speed business processes

To register for this free webinar on Tuesday, June 25 at 1:30 pm EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Disaster scams are a type of social engineering scheme in which perpetrators target and defraud victims of natural disasters, severe weather events, or other catastrophic occurrences. These scams attempt to further victimize those struggling to recover from incidents such as floods, hurricanes, wildfires, and tornadoes, although scammers are known to exploit victims in the wake of nearly any emergency situation. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

DHS Needs Help Peeking into State and Local Networks, Cybersecurity Official Says
Analytic Comment: The US Department of Homeland Security (DHS) seeks deeper interoperability with local municipalities in order to keep pace with the ever-evolving cyber threat landscape. Some local municipalities impacted by cyber attacks have declined DHS assistance in the past, which means that valuable and timely cyber threat information may not have been shared between agencies. To strengthen the United States as a whole against cyber-attacks, federal, state, and local governments need to work together and incorporate comprehensive information sharing strategies to quickly harden networks and systems against the latest threats and exploits.

Election Security Is Still Hurting at Every Level
Analytic Comment: The Stanford Cyber Policy Center recently released a report highlighting US election security inadequacies. These challenges range from electronic voting machines without audit backups and outdated voting machines to inconsistent security regulations and tainted international relations. This report highlights the need for government officials to hasten their election security pursuits as the US presidential election is less than 18 months away. Implementing comprehensive and consistent IT security policies, redundancies, and cyber incident response plans can help government agencies tackle these challenges and more effectively secure the US election security posture.

Google's Triada Backdoor Demonstrates Vulnerabilities in the Mobile Supply Chain
Analytic Comment: In 2017, hackers compromised Android phones with Triada malware, a rooting Trojan that created a backdoor on infected devices. Initially, Triada malware came bundled in apps created by third-party vendors, but eventually, Triada was discreetly included in the Android system image itself after original equipment manufacturers (OEMs) installed tainted third-party code for additional features. This example of supply chain compromise underscores the importance of conducting security audits throughout the development and manufacturing process to reduce the risk of delivering a potentially malicious product to customers.

Patches and Updates

Adobe
Android
Intel
Microsoft

Cisco IOS XE

Exim

GitLab

MyBB

VMware

ICS-CERT Advisories

DICOM Standard in Medical Devices

Optergy Proton Enterprise Building Management System

Panasonic Control FPWIN Pro

Siemens CP, SIAMTIC, SIMOCODE, SINAMICS, SITOP, and TIM (Update B)

Siemens Industrial Products with OPC UA (Update B)

Siemens LOGO!8 Devices

Siemens SCALANCE X

Siemens SCALANCE X (Update A)

Siemens SCALANCE X Seitches, RUGGEDCOM WiMAX, RFID 181-EIP, and SIMATIC RF182C (Update B)

Siemens SIMATIC Ident MV420 and MV440 Families

Siemens Siveillance VMS

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

June 20, 2019

National Capital Region Cyber Threat Spotlight

CISA Warns of DHS Email Phishing Scam

The Cybersecurity and Infrastructure Security Agency (CISA) warns of a current email phishing campaign designed to trick recipients into opening malicious attachments disguised as Department of Homeland Security (DHS) notifications. The Agency reports that campaign-associated emails spoof alerts from DHS's National Cyber Awareness System (NCAS) and contain attachments that trigger malicious downloads. The NTIC Cyber Center recommends users remain vigilant for phishing attempts and malicious emails disguised as DHS notifications or NCAS alerts, avoid clicking on links or opening attachments from unknown or untrusted sources, and alert their organization's IT security team if they receive a suspicious email. ***Furthermore, as CISA indicates that legitimate NCAS alerts will never contain email attachments, the NTIC Cyber Center encourages recipients of NCAS correspondence to scrutinize and verify the legitimacy of all emails before opening.***

Current and Emerging Cyber Threats

Malicious Mobile Apps Attempt to Collect Two-Factor Authentication Codes

ESET researchers discovered malicious mobile apps employing a new social engineering technique to bypass notification access permission settings and collect SMS-based two-factor authentication

(2FA) codes displayed on Android devices. If installed, the malicious apps request permission to read and dismiss notifications displayed by other apps and click any buttons contained within those notifications. The apps then display a fraudulent login screen designed to capture user credentials such as usernames, email addresses, and passwords, which are sent to the attacker behind the campaign. If affected, Android users attempt to log into an online account that sends an SMS-based 2FA code to the device, the malicious apps record and send that information to the attacker as well. Currently, these malicious apps appear to only target Turkish cryptocurrency account credentials, but researchers determined that 90 percent of Android devices are vulnerable to this type of compromise, so it is likely that this attack vector will soon be widely used to target other types of accounts and users across the globe. ***The NTIC Cyber Center encourages all mobile device users to exercise caution before installing any app and to pay close attention to required permission settings. If the permissions required do not match the advertised functionality of the app, do not install it. After installing any new app, monitor the device for unusual behavior such as excessive power consumption, excessive data usage, overheating, unexpected pop-ups, or device malfunction and uninstall problematic apps immediately, performing a factory reset of the device if necessary.***

Cryptomining Campaign Uses EternalBlue and EternalChampion Exploits to Compromise Victims

Security researchers at Trend Micro discovered a large-scale cryptomining campaign that uses the EternalBlue and EternalChampion server message block (SMB) exploits to compromise vulnerable Windows systems and infect them with malware designed to steal victims' computing resources and generate a profit for the attackers behind the campaign. The researchers observed this campaign victimizing organizations across a wide range of sectors, taking an opportunistic approach to selecting targets rather than a more strategic approach. ***The NTIC Cyber Center recommends all network and system administrators ensure that all software, including operating systems, are patched and up-to-date and decommission any unsupported or End-of-Life (EOL) systems and software. We also recommend monitoring systems and servers for unusual and excessive CPU usage and proactively blocking the associated IoCs provided in Trend Micro's report.***

Malicious Android Apps Abuse Push Notifications and Redirect Victims to Scam Sites

Dr. Web security researchers discovered a new Android Trojan embedded in apps available on the Google Play store that redirects users to scam sites. This malware, dubbed Android.FakeApp.174, is distributed via fraudulent apps designed to resemble legitimate and popular apps. Once installed on

an Android device, the malware launches a website in the Google Chrome mobile web browser that asks the victim to enable push notifications for "verification purposes." If enabled, it spams victims with numerous push notifications designed to redirect them to phishing pages and other fraudulent websites. ***The NTIC Cyber Center recommends all Android users remain vigilant for this type of device behavior after installing any new mobile app and refrain from enabling push notifications at the request of unfamiliar websites and apps. We also recommend thoroughly reading user reviews and ratings prior to downloading and installing any new app to help determine its legitimacy.***

Echobot Botnet Uses 26 Exploits and Targets Oracle WebLogic and VMware SD-WAN

Akamai researchers discovered that the new Echobot botnet, created using a variant of the Mirai malware family, uses 26 exploits to infect vulnerable Internet-of-Things (IoT) devices, more than the previous 18 found by Palo Alto Networks Unit 42 research group. Echobot's targets include network-attached storage (NAS) devices, routers, network video recorders (NVRs), IP cameras, IP phones, and wireless presentation systems. In addition to these IoT devices, Echobot also targets enterprise applications such as Oracle WebLogic and VMware SD-WAN. ***The NTIC Cyber Center recommends changing all default credentials on IoT devices and their associated administrator control panels as well as applying available security patches and firmware updates immediately after connecting them to a network. We also recommend placing IoT devices behind a firewall, blocking any unneeded ports that would allow external and unauthorized access, and monitoring the network for suspicious activity. If devices have publicly known vulnerabilities, but no updates or patches are available, we recommend immediately decommissioning the devices, if possible. More information and the IoCs associated with Echobot are available in the Akamai report*** *here*.

New Phishing Campaign Steals OneDrive Account Credentials

An independent security researcher discovered a new phishing campaign that sends emails masquerading as mail server notifications and entices victims to click an embedded malicious link by claiming an encrypted message needs to be manually retrieved from the server. These emails contain the subject line "Encrypted Message Received" and the embedded link redirects victims to a fraudulent OneDrive for Business page that displays a button labeled "Open." When victims click the button, they are redirected to a second page designed to steal OneDrive account credentials. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as notifications from their email service providers, avoid opening and acting upon unexpected emails, and refrain from clicking on links from untrusted sources. We also recommend never entering any account credentials or other sensitive information into a website that originates***

from a link in email or text message. Instead, visit the website directly by entering the address in the URL field of the browser before entering any sensitive information.

Vulnerabilities

Yubico YubiKeys

Security key company Yubico discovered a flaw in some YubiKey devices that impacts calculations used in the devices' cryptography operations. The company indicates that the flaw, which results in reduced randomness of the first set of values generated upon device startup, affects versions 4.4.2 and 4.4.4 of YubiKey FIPS Series devices. This flaw has been remedied in the latest firmware version, 4.4.5, and no other Yubico devices or firmware versions are currently impacted. Although Yubico does not believe any security incidents have occurred as a result of the devices' reduced functionality, the company is offering owners of affected devices a free upgrade through their replacement portal. ***The NTIC Cyber Center encourages users of YubiKey FIPS Series devices to decommission affected devices, remove them from their network environment, and follow Yubico's instructions for obtaining a replacement device.***

TP-Link Technologies Wi-Fi Extenders

IBM X-Force threat intelligence researchers discovered a flaw in TP-Link Technologies Wi-Fi extender firmware that, if exploited, could allow remote threat actors to gain unauthorized access to and execute code on affected devices and associated networks. ***The NTIC Cyber Center recommends all users of affected TP-Link Wi-Fi extenders place these devices behind a firewall, block any unneeded ports that would allow external and unauthorized access, and monitor networks for suspicious activity. Additionally, we recommend visiting the TP-Link Download Center to obtain security patches and firmware updates for affected Wi-Fi extenders.***

Data Breaches and Leaks

BioReference LABORATORIES

carecentrix

A breach reported earlier this month of third-party billing collection provider American Medical Collection Agency (AMCA) is now believed to have affected over 20 million patients. In addition to the 11.9 million customers of Quest Diagnostics and the 7.7 million customers of LabCorp previously reported, nearly one million additional customers of three more entities may have had their data compromised in this breach. Additional victims include customers of BioReference Laboratories (422,600 patients), Carecentrix (500,000 patients), and Sunrise Laboratories (unknown number of patients). As a result, customer information such as patient names, dates of birth, address, phone numbers, dates of service, provider names, balance information, payment card information, bank account information, Social Security numbers, and medical procedures have been exposed to unauthorized access. AMCA has since filed for bankruptcy protection in the wake of this massive data breach. ***The NTIC Cyber Center recommends customers of BioReference Laboratories, Carecentrix, or Sunrise Laboratories monitor their account statements, immediately notify their financial institutions of any unauthorized or suspicious activity, and consider placing a fraud alert or security freeze on their credit file with Equifax, Experian, or TransUnion.***

Online and mobile food ordering service EatStreet disclosed a security breach that affects customers and participating restaurants. According to a company notification, a hacker allegedly obtained access to EatStreet databases from May 3 to May 17 and exfiltrated the data of an unknown number of users. EatStreet reports that customer data stolen may include customer names, credit card numbers, expiration dates, card verification codes, billing addresses, email addresses, and phone numbers. Restaurant and delivery service information stolen may include names, phone numbers, email addresses, bank accounts, and routing numbers. Security researchers believe that the infamous hacker Gnosticplayers, known for stealing collectively over one billion user credentials in various data breaches to date, is responsible for the attack and has gathered EatStreet data of over six million users. Within the National Capital Region, locations where EatStreet food ordering service is available and whose user populations may be affected by this data breach include: College Park, MD; Hyattsville, MD; Rockville, MD; Alexandria, VA; Arlington, VA; Fairfax, VA; and Washington, DC. ***The NTIC Cyber Center recommends EatStreet users, both customers and restaurants, monitor their financial account statements closely, report any unauthorized or suspicious activity to their financial institutions immediately, and remain vigilant for phishing attempts perpetrated through email, telephone, or other avenues.***

Industry Report

proofpoint®

Proofpoint 2019 Domain Fraud Report

Every year, millions of web domains are registered by people looking to defraud businesses, their employees and customers. Using social engineering tactics, threat actors register domains that impersonate trusted brands. From these domains, they launch phishing attacks or other scams.

This report outlines Proofpoint's latest research on domain trends, including the tactics and activity of fraudulent domains.

Download the report now to learn:

- How threat actors create fraudulent domains
- What characterizes fraudulent and legitimate domains
- Which keywords and top-level domains (TLD) are trending
- How fraudulent domains use email to launch attacks

Upcoming Webinars

GOVINFOSECURITY®

Why Third-Party Vendors Often Become the Weakest Link to Your Network Security

Cybersecurity continues to be a significant area of concern, with a higher frequency of multi-million dollar, potentially deadly security breaches, 63 percent of which can be attributed to a third party.

In this webinar Justin Strackany, Chief Customer Officer at SecureLink, and Tony Howlett, Chief Information Security Officer at SecureLink, will discuss why vendor privileged access can open your organization up to unlimited risk and best practices for managing third-party vendor access in a secure and efficient way.

Attend the webinar to learn:

- Lessons from recent third-party vendor-related data breaches
- Why privileged access should be managed differently for vendors vs. employees

- Tools and strategies to ensure third-party accountability without burdening overworked staff

To register for this free webinar on Thursday, June 27 at 1:30 pm EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

DNA testing scams, also known as DNA screening scams or genetic testing scams, are a type of social engineering scheme in which the perpetrator masquerades as a medical health professional or health sales representative concealing his or her true intentions to fraudulently bill healthcare service providers or elicit personally identifiable information (PII) via DNA testing services. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

The Highly Dangerous "Triton" Hackers Have Probed the US Grid
Analytic Comment: According to the critical infrastructure security firm Dragos, a Russian hacker group called Xenotime has recently begun scanning the US energy grid. This group became infamous in early 2018 for using their signature malware, Triton, to sabotage an Aramco facility in Saudi Arabia by exploiting a vulnerability in the facility's Triconex safety instruction systems, impacting the equipment's ability to detect leaks, explosions, or other hazardous events. This report highlights the importance of cybersecurity, particularly threat hunting, in the energy and critical infrastructure sectors.

Instagram Shows Kids' Contact Details in Plain Sight

Analytic Comment: A San Francisco-based data scientist discovered that a large number of Instagram users listed as 13 years of age or younger have Instagram accounts that are improperly secured and expose their personal contact information such as phone numbers and email addresses. This data exposure commonly results from converting Instagram accounts from “personal” to “business” as business accounts have less-restrictive privacy settings. The public exposure of this personal data puts minors at risk of social engineering schemes such as phishing and vishing or unwanted contact from strangers. This discovery underscores the importance of teaching children about cybersecurity and privacy best practices as well as the need for understanding the potential consequences of sharing too much information online.

Patches and Updates

Cisco

Google Chrome

Mozilla Firefox & Firefox ESR

Mozilla Thunderbird

Oracle WebLogic

Samba

ICS-CERT Advisories

WAGO Industrial Managed Switches 852-303, 852-1305, & 852-1505

BD Alaris Gateway Workstation

Johnson Controls exacqVision Enterprise System Manager

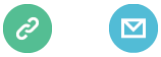
We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.



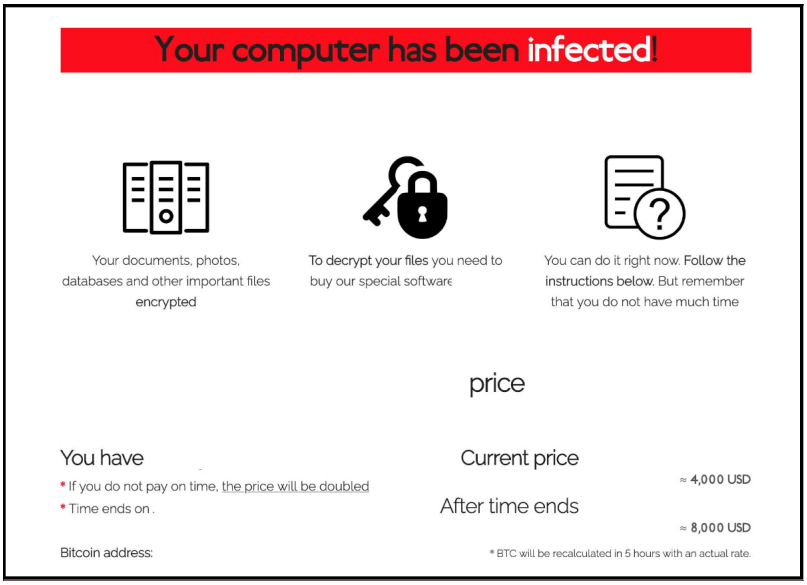
NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

June 27, 2019

National Capital Region Cyber Threat Spotlight



Sodinokibi Ransomware Campaign Update

On Monday, June 24, 2019, the NTIC Cyber Center alerted members about a new ransomware campaign, dubbed Sodinokibi, that leveraged a vulnerability in Oracle WebLogic servers and exploited various compromised Managed Service Provider (MSP) accounts to maximize infection rates and potential profits. Since the release of our Cyber Alert, the cyber threat actor or group behind this campaign included additional attack vectors including exploit kits and malvertising, or malicious online advertisements, to infect victims with Sodinokibi. ***As this appears to be an aggressive and rapidly evolving ransomware campaign, the NTIC Cyber Center would like to emphasize the importance of maintaining a robust and comprehensive data backup strategy to reduce downtime and recovery expenses that could result from a ransomware incident. Additionally, we recommend using a reputable ad-blocker to reduce the risk of a ransomware***

infection perpetrated via malicious advertisements. For a full list of prevention and mitigation strategies, please download our Ransomware Mitigation Guide available on our website.

CISA Warns of Increase in Iranian 'Wiper Attacks'

The US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Director Christopher Krebs released a statement on Saturday warning of an increase in wiper attacks against US businesses and government agencies by the Iranian government and proxy actors. A wiper attack is a cyber attack that leverages malware to destroy data on a computer or entire network, leaving victims with no way of recovering lost files. Director Krebs indicates that Iranian actors have perpetrated wiper attacks using vectors such as spear phishing, credential stuffing, and password spraying. ***The NTIC Cyber Center recommends Internet users remain vigilant for phishing attempts and malicious emails, avoid clicking on links or opening attachments from unknown or untrusted sources, and alert IT security teams of suspicious emails. We also strongly encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication on any account that offers it to limit the impact of credential compromise. Furthermore, in light of the destructive nature of wiper attacks, we recommend maintaining regular system backups that are stored securely off the network.***

Current and Emerging Cyber Threats

Malicious Macro-Enabled Word Documents Distribute New Ransomware LooCipher

Security researchers identified a new ransomware, called LooCipher, likely distributed via spam emails containing malicious Word documents. When the document is opened and macros are enabled, the host computer downloads the LooCipher ransomware from a Tor server and launches the executable file. LooCipher then encrypts files, appends them with the .lcphr extension, and displays a ransomware note demanding that approximately $330 be sent to a Bitcoin address within a limited time period. At this time, it is not known if LooCipher is decryptable. ***Since exploiting macro functionality to deliver malicious payloads is a common attack vector, the NTIC Cyber Center recommends users disable Microsoft Office macros by default and avoid opening documents from unknown and untrusted sources. We also recommend maintaining regular***

system backups that are stored securely off the network and keeping endpoint antivirus software updated with the latest virus definitions.

Chinese APT 10 Group Targeting Telecommunications Providers

Cybersecurity firm Cybereason identified a global cyber campaign targeting telecommunications providers that is believed to be the work of a Chinese-affiliated advanced persistent threat (APT) group, APT 10, also known as Stone Panda. Cybereason believes APT 10's campaign was long-term, with the threat actor having penetrated targeted telecommunications networks for roughly six months before the firm discovered the breach. Researchers believe APT 10's attack consisted of four waves: stealing credentials and mapping out the target networks; conducting additional reconnaissance and exfiltrating data from critical servers; exfiltrating additional data moving laterally through networks; and launching similar attacks from different Indicators of Compromise (IoCs). According to the firm's report, APT 10 attempted to steal active directory data, usernames and passwords, billing data, call detail records, credentials, email servers, geo-location of users, and personally identifiable information. Cybereason believes telecommunications data is of significant value in intelligence and counterintelligence operations as it could be used to identify sources, destinations, and duration of calls; glean device and vendor details; or to track the whereabouts and device details of targeted individuals. ***The NTIC Cyber Center recommends network and system administrators, especially those within telecommunications organizations, consider implementing a web application firewall, block access to unused ports and services, require the use of multifactor authentication on all employee and customer accounts, track and regularly audit enterprise user account creation and changes, and keep all software and operating systems patched and updated.***

"Free Prize" Phishing Campaign Steals Steam Users' Credentials

Researchers at Malwarebytes Labs identified a new phishing campaign targeting users of Steam, a popular game distribution platform, and masquerading as an offer for a free "prize." The offer appears as a message within Steam urging users to follow a Twitter redirection link to play an online roulette game. After users interact with the game, they are directed to a phishing site that prompts for Steam user credentials in order to claim an earned "prize." ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as free prize giveaways from Steam and refrain from clicking on links from unknown or untrusted sources. We also recommend never entering any account credentials or other sensitive information into a website that launches after clicking a link in an email or text message. If you believe you have been targeted by this phishing scam, notify Steam customer support immediately.***

Vulnerabilities

Multiple Vulnerabilities in Linux and FreeBSD Kernels

The information security team at Netflix discovered several Transmission Control Protocol (TCP) Selective Acknowledgement (SACK) vulnerabilities in Linux and FreeBSD that would allow perpetrators to hinder system speeds or create a denial-of-service (DoS) condition. Of these vulnerabilities, CVE-2019-11477, dubbed SACK Panic, poses the greatest risk as it can send TCP Selective Acknowledgements (SACKs) to a vulnerable system resulting in remote DoS attacks. CVE-2019-11478, dubbed SACK Slowness, delivers malicious TCP SACKs to vulnerable systems engrossing resources resulting in hindered system speeds or DoS conditions. CVE-2019-5599, dubbed FreeBSD 12, operates in a similar manner to CVE-2019-11478 but uses recent acknowledgment (RACK) instead. CVE-2019-11479, dubbed Excess Resource Consumption Due to Low Maximum Segment Size (MSS) Values, restricts TCP connection segment size resulting in hindered system speeds. ***For more information about vendor announcements, patches, and workarounds, the NTIC Cyber Center recommends visiting the Carnegie Mellon University Software Engineering Institute's website.***

Microsoft Excel Power Query

Security researchers discovered a method threat actors could potentially use to abuse Microsoft Excel Power Query, a software feature designed to assist Excel files with locating, combining, and manipulating data prior to importing it from external sources. Recent versions of Excel include this tool, but Power Query is also available for older versions of Excel through an add-in that can be downloaded from Microsoft's website. According to researchers, threat actors could use Power Query to launch a Dynamic Data Exchange (DDE) attack by automatically delivering malicious content from an external source that executes on a victim's computer after he or she opens a specially crafted Excel file. As this is a legitimate feature of Excel, Microsoft does not intend to release a patch to address this issue. However, Microsoft released Security Advisory 4053440 to advise customers on how to properly secure Microsoft Office applications such as Excel against DDE attacks. ***The NTIC Cyber Center recommends all Microsoft Excel users and administrators review Microsoft's Security Advisory 4053440 and implement the recommended mitigation strategies. We also encourage all users to refrain from opening attachments from unknown or untrusted sources.***

Data Breaches and Leaks

Dominion National, a dental and vision benefits and insurance firm in Arlington, VA, recently disclosed a security incident involving unauthorized third-party access to company servers. The firm believes a third-party actor may have had access to company servers as early as August 2010. Information stored on servers includes names, addresses, emails, dates of birth, Social Security numbers, taxpayer identification numbers, bank account and routing numbers, member ID numbers, group numbers, and subscriber numbers, though Dominion National indicates there is no evidence that any of this data was accessed, acquired, or misused. Dominion National is currently mailing notification letters to potentially affected customers. ***The NTIC Cyber Center encourages customers of Dominion National to remain vigilant for an increase in phishing attempts and to contact Dominion National's incident response line at 877-503-8923 with any additional questions.***

Security researchers at vpnMentor discovered an unsecured MongoDB database exposing the prescription and medical data of over 78,000 users of Vascepa, a medication for reducing triglycerides. Researchers report that the database, whose owner has yet to be identified, was Internet accessible and configured without a password. Patient data exposed includes patient names, phone numbers, addresses, email addresses, prescribing doctor, gender, pharmacy location, and more. ***The NTIC Cyber Center recommends Vascepa users remain vigilant for increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

Upcoming Webinars

Data Breach Today
Prevention. Response. Notification.

The New #1 Cyber Threat - Attacks on the Applications that Power Your Business

In today's hyper-connected organizations, you depend on externally facing web, mobile, and API-based applications to connect with customers, partners, suppliers, and employees. These strategically important applications support business processes and enable you to create an extended, efficient digital ecosystem.

Unfortunately, these same applications have become primary targets for two vastly different, but equally dangerous, types of cyberattacks. Successful application breaches can lead to financial fraud, stolen IP, and business disruption.

Cequence Security recently completed two separate research projects with Ponemon Institute and Osterman Research, which provide insights into these attacks and defense strategies at nearly 900 organizations across the US.

Register for this live webinar and learn:

- What the two cyberattacks are and how they're dangerous;
- How they're impacting your peers;
- What you can do to protect your hyper-connected organization.

To register for this free webinar on Wednesday, July 10 at 1:30 pm EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Money mule scams are phony employment opportunities that criminals advertise to recruit individuals to launder money obtained through illicit activity. People who accept these opportunities are called money mules. Whether knowingly or unknowingly, money mules assist criminals in transferring funds derived from phone or Internet-enabled fraud scams, drug trafficking, human trafficking, or other crimes. Ultimately, money mules help criminals obscure trails of financial transactions and perpetuate illegal activity. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Business Decision Makers Focus on the Wrong Security Issues

Analytic Comment: A study by Symantec found that business leaders and security experts frequently disagree on which cloud-related security issues pose a greater risk. Roughly seven percent of business leaders believe that account takeover through internal corporate cloud accounts are a risk when in reality, 42 percent of dangerous behavior indicates cloud account compromise and 64 percent of all cloud security incidents are account takeovers. One way that threat actors penetrate these accounts is through flaws in Software as a Service (SaaS) apps. Additionally, Bring Your Own Devices (BYOD), and the policies that govern their integration and use, also present risks that can be identified and exploited by threat actors. Implementing and enforcing strict BYOD policies to ban devices that have not been sanctioned to access the corporate network may help mitigate risks and address challenges facing organizations concerned with cloud security.

50% of Manufacturers Experienced Data Breaches in Past Year

Analytic Comment: A study by Sikich found that 50 percent of manufacturing firms report having experienced a data breach in 2018, and, of those respondents, 11 percent report experiencing a "major" breach. The study also found that manufacturing firms with revenue under $500 million per

year do not make adequate investments in cybersecurity. Although corporate cybersecurity can be expensive, the disastrous effects of cyber attacks are likely to outweigh the costs of properly implemented prevention strategies. Manufacturing firms are encouraged to make cybersecurity a core priority to ensure they are prepared to defend against the increasing risk of data theft, ransomware, and other cyber threats.

Patches and Updates

Apache Tomcat

Apple Airport

Cisco Data Center Network Manager

Dell

Microsoft Outlook for Android

Mozilla Firefox and Firefox ESR

ICS-CERT Advisories

PHOENIX CONTACT Automation Worx Software Suite

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

July 3, 2019

Ahead of the Independence Day holiday tomorrow, we have decided to release our Weekly Cyber Threat Bulletin a day early to help keep you up-to-date with the latest cybersecurity trends, news, and mitigation strategies specially selected to help protect you and your network from current and emerging cyber threats. We here at the National Capital Region Threat Intelligence Consortium want to take a moment to thank you, our readers, for entrusting us to bring you the latest in cyber threat intelligence each and every week. While you head out to enjoy your favorite Independence Day festivities, we would like to extend our wishes for a happy, healthy, and safe celebration!

National Capital Region Cyber Threat Spotlight

DIA and Joint Chiefs of Staff Warn of Imposter Twitter Accounts

The US Defense Intelligence Agency (DIA) and the Joint Chiefs of Staff report an increase in fraudulent Twitter accounts impersonating Joint Staff leadership that attempt to defraud unsuspecting Twitter users out of money. The DIA reminds social media users that official government accounts will never request money or send friend requests. ***The NTIC Cyber Center recommends that all social media users remain vigilant for fraudulent accounts and refrain from communicating with – or sending money to – anyone you do not know personally. We also encourage reporting accounts that are suspected of impersonating government officials, celebrities, and other high-profile individuals. Instructions on how to report Twitter accounts that are in violation of the platform's rules and terms of service can be found here.***

Current and Emerging Cyber Threats

EternalBlue Sextortion Email Campaign Discovered

Security researchers warn of a email sextortion campaign that claims attackers have stolen compromising and personal videos of victims. The email, entitled "Security Alert. Your Account Was Compromised. Password Must Be Changed," falsely indicates that attackers leveraged the EternalBlue software exploit on victims' computers to install a Remote Access Trojan (RAT) and record videos of victims visiting websites hosting adult content. The campaign threatens email recipients with the release of the alleged video recordings unless the victim remits payment of $600 in Bitcoin. To add an element of credibility to the scam, the sextortion perpetrators have included victims' old email passwords likely obtained from previous and publicly available data breaches. ***The NTIC Cyber Center reminds recipients of these or similar sextortion scam emails to ignore the bogus claims included in this correspondence. For more information on sextortion scams, please reference the NTIC Cyber Center's Sextortion Scams blog post.***

Malicious Android Gaming App Steals User Information

Mobile security firm Wandera discovered a malicious Android game app that steals user information such as Facebook and Google credentials, phone numbers, verification codes, birth dates, cookies, tokens, and recovery email addresses. This malicious app masquerades as a fully functional game known as Scary Granny ZOMBYE Mod: The Horror Game 2019 (Scary Granny) and imitates a legitimate and popular Android game called Granny. The user-granted permissions during the installation process allow Scary Granny to gain persistence and deliver deceptive ads. Scary Granny does not start conducting malicious activity until two days after installation, however. The app eventually displays a fraudulent Google login page requesting user login credentials which the app then uses to collect user data from the device. The malicious Scary Granny app was removed from the Google Play Store on June 27th. ***The NTIC Cyber Center recommends Android users keep device operating systems up-to-date. Before installing any app, exercise caution and research both the app itself and the developer. Once an app is installed, monitor the app's requests for permission authorizations and data activity. Beware of any applications that request permissions that do not match the advertised app functionality. Users who suspect that their devices have been compromised should perform a factory reset and restore devices to manufacturer default settings. Additionally, users impacted by this or other malicious Android apps are strongly encouraged to change their account credentials and monitor accounts for suspicious or unauthorized activity.***

Malvertising Campaign Pushes Ransomware Using Greenflash Sundown Exploit Kit

Malwarebytes researchers uncovered a ransomware campaign delivered through a rare exploit kit named Greenflash Sundown that relies on a newly expanded malicious advertising – or malvertising – program. The developers of the exploit kit compromise existing websites' advertisements rather than create their own malicious ads. The current resurgence of Greenflash Sundown relies on a large network of compromised websites, including a popular video conversion site, which is visited by more than 200 million individuals per month. The compromised sites promptly redirect visitors to the exploit kit through malware hidden in a Graphics Interchange Format (GIF) file, which pushes three malicious software packages including SEON ransomware, the information-stealing Trojan called Pony, and a cryptocurrency-mining malware. Originally, the campaign almost entirely targeted victims in East Asia but, recently, it expanded its scope to target victims in Europe and North America. ***The NTIC Cyber Center recommends regularly backing up data and patching systems and devices to reduce the risk of a ransomware attack, and using a reputable ad blocker to mitigate against malvertising campaigns.***

New Dridex Banking Malware Variant Discovered

Researchers at the cybersecurity firm eSentire discovered a new variant of Dridex malware that steals bank account information from victims' computers. Like previous forms of Dridex, this variant commonly gains initial access by abusing macro functionality in documents attached to spear phishing emails. This variant currently uses a technique called application whitelisting to evade approximately 27 percent of antivirus software systems. ***Since exploiting macro functionality to deliver malicious payloads is a common attack vector, the NTIC Cyber Center recommends users disable Microsoft Office macros by default and avoid opening documents from unknown and untrusted sources. We also recommend maintaining regular system backups that are stored securely off the network and keeping endpoint antivirus software updated with the latest virus definitions. In addition, we recommend administrators review the Indicators of Compromise (IoCs) associated with this malware variant listed here.***

Vulnerabilities

Numerous Medtronic Insulin Pumps Vulnerable to Exploitation

Medical device provider Medtronic is recalling numerous Medtronic MiniMed™ insulin pump models due to potential vulnerability concerns. Although there have not been any reported incidents related to these vulnerabilities, the company believes that there is the potential for exploitation and that these flaws could allow unauthorized persons to modify insulin pump settings to increase, decrease, or stop insulin flow, causing dangerous fluctuations in the blood sugar levels of device users. Medtronic currently estimates that approximately 4,000 patients may be affected and is working with partners to identify and replace vulnerable devices. ***The NTIC Cyber Center recommends MiniMed™ insulin pump users check Medtronic's list of affected devices to see if their device or software is vulnerable. Users of affected devices should work with their medical health provider to request a replacement immediately and should avoid sharing pump serial numbers or connecting pumps to unfamiliar machines and networks. For additional information, contact Medtronic at 1-866-222-2584 or visit Medtronic's website.***

Data Breaches and Leaks

Security researchers at cybersecurity firm UpGuard, Inc. discovered an unsecured Amazon Web Services cloud server belonging to information management company Attunity that exposed the internal files of clients including Ford Motor Co. and TD Bank. Comprised of more than one terabyte of data, the information revealed in the leak includes Ford IT architecture details and internal project plans; TD Bank invoices, agreements, and details on technology solutions; and Attunity email backups, network information, and employee login credentials and personal information. Researchers have seen no indication that threat actors accessed the information while it remained exposed, and impacted clients do not believe that customers' personal or financial information was affected. ***The NTIC Cyber Center recommends Attunity clients and customers scan all incoming emails for phishing attempts, monitor networks for suspicious activity, and remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

PCM THE RIGHT TECHNOLOGY, DELIVERED™

Cloud data management provider PCM Inc. disclosed a security incident that allowed third party actors to access the email and file sharing systems of some of the company's clients. The company believes that third party actors used stolen Microsoft Office 365 administrative credentials to gain access to client accounts, where they then sought to steal information that could be used to conduct gift card transaction fraud. Security researchers believe this attack bears resemblances to a security incident that affected Indian IT firm Wipro in April of 2019, when attackers breached company systems in search of information associated with gift cards. ***The NTIC Cyber Center recommends PCM clients and customers scan all incoming emails for phishing attempts, monitor networks for suspicious activity, and contact PCM for specific indicators of compromise (IoCs) and adversary tactics, tools, and procedures (TTPs) associated with this breach.***

Medicare Supplement.com

Comparitech researchers discovered an unsecured MongoDB database belonging to health insurance marketing website, MedicareSupplement.com, that contained approximately five million records of personal information and health details. Data exposed in this breach includes the full names, addresses, email addresses, dates of birth, genders, phone numbers, and IP addresses of registered website users. At this time, it is not known how long the database was exposed or if a third party accessed the information contained within it. ***The NTIC Cyber Center recommends affected users remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

Upcoming Webinars

Data Breach Today
Prevention. Response. Notification.

Managing Risk Exposure in a Hyper-Connected World: Revelations from the Internet Risk Surface Report

The old demarcation lines of cybersecurity responsibility have been erased. In this new landscape, risk surface is the unforeseen undercurrent of high velocity digital business.

"Risk Surface Management" is a revolutionary shift in third-party risk management. It is an approach to self-reporting on third-party risk - the risk that exists as a result of the connections between you and every company with whom you do business.

RiskRecon is proud to present a webinar on risk surface and the Internet Risk Surface Report, which will reveal the true expanse of enterprise risk and forecasting solutions for managing risk surface in a hyper-connected and hyper-exposed world.

Register for this webinar and you will learn:

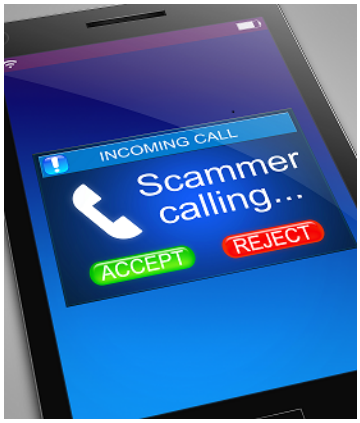
- Exactly what risk surface is and where it exists in relation to your organization's digital assets;
- What your responsibility is for your organization's sensitive data;
- Common components of risk surface;
- Best practices for assessing the risk of your third- and fourth-party vendors.

To register for this free webinar on Tuesday, July 9 at 1:30 pm EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

A ***neighbor number scam***, also called ***neighbor spoofing*** or ***caller ID spoofing***, is a technique that scammers use to deliberately falsify telephone caller ID information to conceal



their identifying information. Masquerading as a neighbor or otherwise legitimate local caller, scammers prey on those who answer these calls in any number of ways. Becoming familiar with neighbor number scam calls can help prevent you from falling victim to financial fraud and identity theft. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Microsoft to Require Multi-Factor Authentication for Cloud Solution Providers

Analytic Comment: In an effort to mitigate phishing attacks targeting Office 365 account credentials, Microsoft will now require all of its Cloud Solution Partners (CSPs) to use multi-factor authentication to secure their accounts. Many organizations use Microsoft-partnered CSPs to manage their Office 365 accounts, which creates risk and potentially leaves them vulnerable to breaches if CSP accounts become compromised. Microsoft's new mandatory security requirements reflect a shift toward "security by default" to help protect customers as well as the reputation of software companies and service providers.

Patches and Updates

Chrome

VMware

ICS-CERT Advisories

ABB CP635 HMI

ABB CP651 HMI

ABB PB610 Panel Builder 600

Advantech WebAccess/SCADA

Medtronic MiniMed 508 & Paradigm Series Insulin Pumps

Quest KACE Systems Management Appliance

Schneider Electric Modicon Controllers

SICK MSC800

We welcome your feedback.

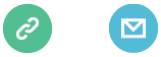
Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

July 11, 2019

National Capital Region Cyber Threat Spotlight

FBI Warns of Sextortion Scams Targeting Minors

The Federal Bureau of Investigation (FBI) issued a statement warning of the dangers of sextortion, a cybercrime in which criminals threaten to distribute incriminating content if victims do not comply with demands. According to a story on FBI's website, the Bureau has recently noted a significant increase in sextortion cases, especially those involving the targeting of minors. Perpetrators of these crimes commonly use gaming platforms, social media outlets, or dating and video chat applications to conduct sextortion schemes. Through these avenues, they lure young victims into producing explicit content in exchange for game credits, payment, or other rewards. They then threaten to widely distribute the content if the victim refuses to produce additional explicit photos or videos. ***The NTIC Cyber Center recommends that parents, educators, and others concerned with the increase in sextortion crimes review the FBI's resources for combating this dangerous trend. In addition, we recommend reviewing the NTIC Cyber Center's blog post on sextortion for additional information and mitigation strategies.***

US Coast Guard Issues Cybersecurity Recommendations in Safety Alert

The US Coast Guard recently released a safety alert offering cybersecurity recommendations for commercial vessels. The alert comes in response to a cyber incident that impacted a vessel in February 2019, affecting the ship's network and degrading the functionality of the onboard computer system. The Coast Guard, along with an inter-agency team, concluded that, while essential vessel control systems were not impacted by the incident, the vessel lacked proper cybersecurity measures that exposed critical control systems to cyber threats. Due to the increasing reliance on Internet-enabled control and navigation systems, the US Coast Guard has issued recommendations including segmenting networks, requiring the use of unique network profiles for each employee, scrutinizing external media, employing antivirus software solutions, and keeping all systems updated with the latest patches. ***The NTIC Cyber Center recommends reviewing and implementing the recommended cybersecurity practices contained within US Coast Guard's complete Safety Alert 06-19.***

Current and Emerging Cyber Threats

Phishing Campaign Spoofs Microsoft OneNote Audio Message Notifications

A new phishing campaign uses fraudulent Microsoft OneNote audio message notification emails to entice recipients into navigating to phishing pages. The email correspondence features the subject line "New Audio Note Received" and contains a security banner claiming the email has been "scanned by McAfee Ultimate 2019 Antivirus Scanning Service for Microsoft." When users click on a link to retrieve the audio message, they are ultimately delivered to a fraudulent Microsoft login page designed to steal user account credentials. To lend credence to this scam, attackers have registered the phishing domains on the fraudulent site sharepoint[.]com, which has no affiliation with Microsoft, and have obtained Microsoft certificates that bolster appearances of legitimacy. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as alerts from Microsoft OneNote, avoid opening unexpected emails, and refrain from clicking on links from unknown or untrusted sources. In addition, users are advised that legitimate Microsoft and Outlook account login pages are hosted on the microsoft.com, live.com, microsoftonline.com, and outlook.com domains only.***

Magecart Attacks Breach 962 Ecommerce Stores

Security researchers discovered a large-scale Magecart payment-skimming campaign stealing customer personal and financial information from 962 breached ecommerce stores. By adding malicious data-stealing JavaScript code to websites, attackers were able to steal names, phone numbers, addresses, and credit card details of customers of stores ranging from small to enterprise-sized. Though details regarding exact attack vectors are still unknown, researchers believe that the websites of at least some affected merchants may have suffered from PHP object injection vulnerabilities.

Magecart attacks are proliferating; according to one researcher "for every Magecart attack that makes headlines, we detect thousands more that we don't disclose." Furthermore, Magecart groups continue to diversify their attacks and have been observed extending their techniques to steal information other than payment details, such as login credentials and other sensitive information, from non-ecommerce sites as well. ***As Magecart attacks continue to pose a large risk to both ecommerce and non-ecommerce platforms, the NTIC Cyber Center recommends website visitors remain vigilant for indications that a webpage may be compromised. These may include being asked twice to enter payment or login information or being prompted for payment card details before being forwarded to a secure payment service provider. In addition, customers making purchases on ecommerce platforms should routinely monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.***

To read more about the threat of Magecart attacks and for mitigation strategies, please see our recent Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Phishing Campaign Delivers Two Types of Malware Through Macro-Enabled Excel Sheets

Researchers at Codefense discovered a new phishing campaign that delivers both the Dridex banking malware variant and the Remote Manipulator System Remote Access Tool (RMS RAT) through macro-enabled Microsoft Excel files. This campaign's emails are disguised as eFax messages and contain Excel attachments within ZIP file archives. When enabled, macros within the Excel files download the Dridex banking trojan to steal credentials from browsers and the RMS RAT to control infected computers, steal passwords through keyloggers, activate computers' microphones or webcams, or transfer files. ***Since exploiting macro functionality to deliver malicious payloads is a common attack vector, the NTIC Cyber Center recommends users disable Microsoft Office macros by default. In addition, we advise users to remain vigilant for phishing emails disguised as eFax messages and refrain from opening attached documents from unknown***

or untrusted sources.

Fileless Malware Campaign Delivers Astaroth Trojan

Researchers at Microsoft Security Intelligence discovered a fileless malware campaign that drops the Astaroth information stealing Trojan. The malware campaign is comprised of a spear phishing email containing a link that leads victims to an LNK file, which, when double-clicked, directs system tools already present on the target system to force the download of the Astaroth Trojan. The Astaroth Trojan steals sensitive information such as user credentials from victims by using a keylogger module, intercepting operating system calls, and monitoring clipboards. The technique of abusing the functionality of legitimate system tools (instead of downloading and running files) to deliver malware is known as "living off the land" and allows attackers to masquerade malicious activity as routine system processes. ***The NTIC Cyber Center recommends users remain vigilant for phishing emails and refrain from clicking on links from unknown or untrusted sources.***

Vulnerabilities

Numerous Models of Arlo Security Cameras Vulnerable to Exploitation

Researchers at Tenable discovered two vulnerabilities in several models of Arlo wireless security cameras that could allow threat actors to obtain sensitive information or take control of a targeted camera. The first vulnerability, CVE-2019-3949, allows threat actors with physical access to a device to log in as the root user with default credentials and execute arbitrary commands. The second vulnerability, CVE-2019-3950, allows threat actors to take control of a camera through the LAN-connected internal camera network interface. Arlo has released patches addressing these bugs in the latest firmware updates for affected devices, which include Arlo Base Station models VMB3010, VMB4000, VMB3500, VMB4500 and VMB5000. ***The NTIC Cyber Center recommends users of affected Arlo wireless security cameras confirm that the latest security patches have been successfully installed via automatic firmware updates.***

Zoom Video Conferencing App Vulnerable on Mac Devices

A security researcher discovered a vulnerability within Zoom, an app that enables video conferences through cloud systems, that allows websites to launch video calls and access webcams without permission on Mac computers. Because the vulnerable app version installs a persistent local web server onto Mac computers to enable video conferencing functionality, simply uninstalling Zoom from systems does not mitigate security concerns related to this vulnerability. However, on July 9, Zoom issued a software patch that deletes the persistent local web server, allows users to fully

uninstall Zoom software from systems, and resolves security issues that allow rogue video calls to launch on vulnerable systems. ***The NTIC Cyber Center recommends that Zoom users update the app through the Zoom client pop-up prompt, through a download at zoom.us/download, or by opening the Zoom app window, clicking zoom.us in the top left corner of the screen, and then clicking "Check for Updates." In addition, we encourage Zoom users to set "Turn off my video when joining a meeting" as a default in the program's setting pane to avoid unintentional third-party webcam access.***

Data Breaches and Leaks

The Maryland Department of Labor announced that the sensitive information of 78,000 residents of the state may have been accessed by an unknown party. According to the announcement, the breached information includes full names, dates of birth, Social Security numbers, city or county of residence, graduation dates, and record numbers from files dating from 2009, 2010, and 2014. Though the information was left accessible on two Internet-facing servers, the Maryland Department of Information Technology does not believe that unauthorized users downloaded or extracted any of the information from the databases. ***The NTIC Cyber Center recommends affected residents remain vigilant for increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure. Affected residents can obtain more information about this incident and register for free credit monitoring services by contacting Maryland Department of Labor's hotline at 410-767-5889 or through e-mail at dataincident.labor@maryland.gov.***

Upcoming Webinars

INTSIGHTS

CYBERSECURITY

How to Hunt Threats on the Dark Web to Prevent Cyberattacks

The dark web is a sprawling underground network of secrecy where cybercriminals plan and coordinate cyberattacks against organizations. Monitoring the dark web can provide cybersecurity teams with valuable intelligence for how, when, and where a cyberattack might be launched, but this is no simple task. You need to know what to look for and how to engage on the dark web in order to identify threats without drawing suspicion.

Join IntSights for a live webinar on July 17th at 9:00 AM EDT or 1:00 PM EDT for:

- Key dark web sources you need to be monitoring
- How to covertly establish access behind enemy lines
- Common examples of dark web threats
- How to operationalize your dark web monitoring program

To register for this free webinar on Wednesday, July 17 at 9:00 AM EDT or 1:00 pm EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Advance fee fraud, also known as an ***upfront fee fraud***, is a social engineering scheme in which perpetrators try to elicit money from victims through a fraudulent business proposition. Scammers may propose an investment, offer a loan, or present a lucrative business opportunity with the "promise" of delivering a benefit or compensation in the future. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

China is Forcing Tourists to Install Text-Stealing Malware at its Border
Analytic Comment: In the Xinjiang province of China, authorities are requiring that foreign visitors download an Android app that can access text messages, calendar entries, contact lists, call

logs stored on the device. In addition to capturing this data, the app searches for files containing Islam-related material including religious Islamic texts and academic books on Islam. The app has caused concern among both international privacy activists and cybersecurity firms, some of which have updated their antivirus software to flag the app as malware. This revelation highlights the cyber risk posed to devices when visiting foreign nations, especially those hostile to US interests. When traveling abroad, it is strongly advised to leave personal and professional devices at home and only carry one-time use devices that contain no sensitive or personal data, if needed.

Thirty Percent of Employees Have Lost a Work Device While on Vacation
Analytic Comment: According to a Snow Software report, 30 percent of working Americans surveyed reported losing work-related devices while on vacation and, of those, only 49 percent contacted their company to report the device as missing. Common locations for misplacing devices include restaurants, hotels, public transportation, airplanes, airports, and rental cars. Though the ability to access work devices while on vacation can be advantageous, employees and organizations should be aware of the potential for data exposure and other security concerns when devices are lost or stolen.

Patches and Updates

Adobe

Android

Cisco 1

Cisco 2

Intel

Juniper Networks

Microsoft

Mozilla Firefox and Firefox ESR

WP Statistics

ICS-CERT Advisories

Emerson DeltaV Distributed Control System

GE Aestiva and Aespire Anesthesia

Rockwell Automation PanelView 5510

Schneider Electric Zelio Soft 2

Siemens CP1604 and CP1616 (Update A)

Siemens CP, SIMATIC, SIMOCODE, SINAMICS, SITOP, and TIM (Update C)

Siemens Industrial Products with OPC UA (Update C)

Siemens Spectrum Power

Siemens SIMATIC PCS7, WinCC, TIA Portal (Update A)

Siemens SIPROTEC 5 and DIGSI 5

We welcome your feedback.

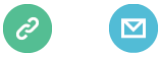
Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.



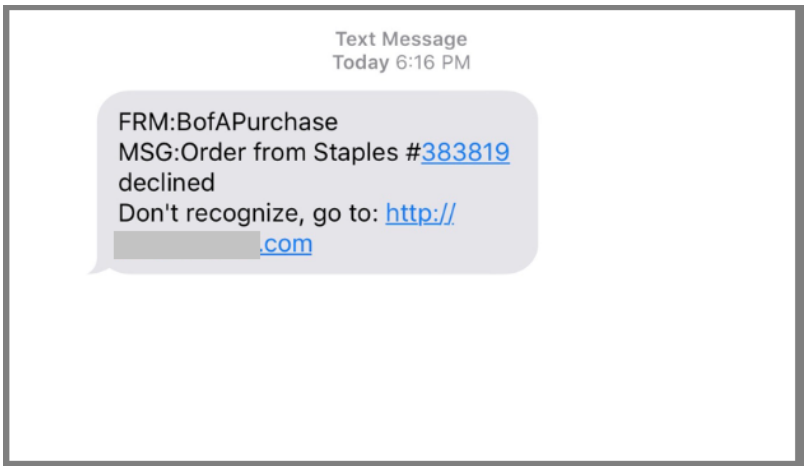
NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

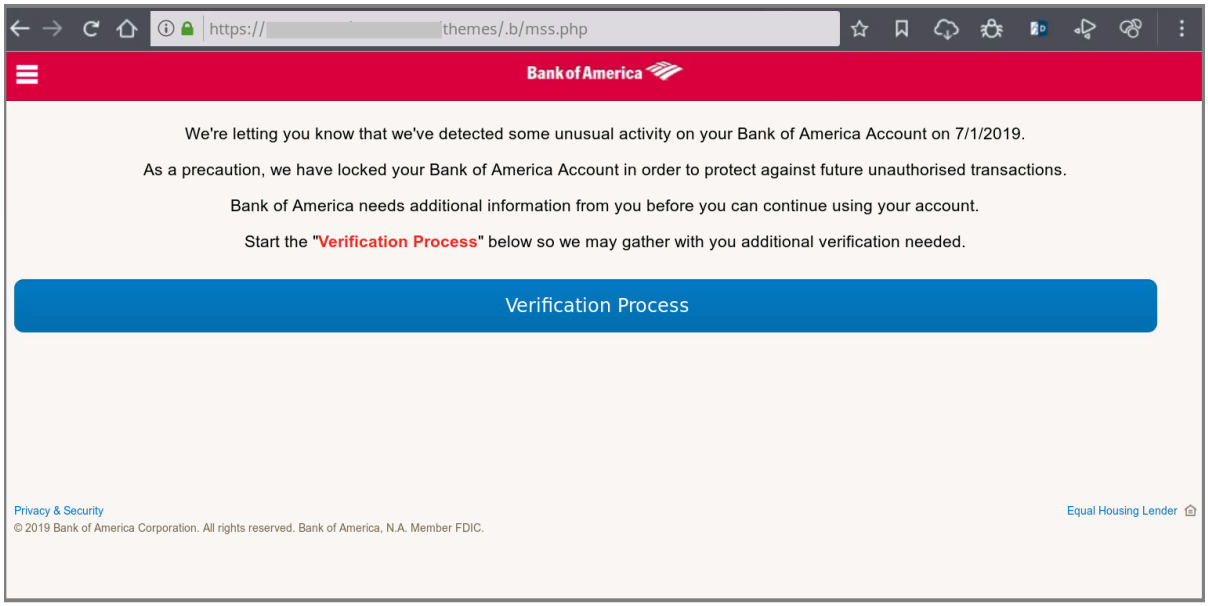
Weekly Cyber Threat Bulletin

TLP:WHITE

July 18, 2019

National Capital Region Cyber Threat Spotlight





SMiShing Scheme Reported

The NTIC Cyber Center recently received a report of a new text message-based phishing campaign, also known as SMiShing, impacting residents within the National Capital Region. This SmiShing campaign entices recipients to click a link sent via text message by masquerading as a declined order alert from Bank of America. Once clicked, the link redirects victims to a phishing page claiming that their Bank of America account has been locked. If victims proceed with the verification process on the phishing page, they will be asked to "confirm" their identity by entering the following information into the fraudulent website: credit or debit card details, ATM PIN, Social Security number, date of birth, phone number, email address, and email account password. Once the attackers collect this information, they can use it to hijack victims' accounts and commit identity theft and financial fraud. ***The NTIC Cyber Center recommends maintaining awareness of this and similar SMiShing threats and never clicking on links in unexpected or unsolicited text messages. We encourage our readers to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of similar SmiShing schemes.***

Current and Emerging Cyber Threats

Miori - A New Variant of the Mirai Botnet

Trend Micro researchers observed a new variant of the Mirai botnet, Miori, using unique protocols to communicate with its Command and Control (C&C) servers to target Internet of Things (IoT) devices. While most Mirai variants rely on binary-based protocols to communicate with their C&C servers, Miori uses a text-based protocol. Consequently, rather than displaying the log-in feature found in most samples of Mirai, this variant requires a specific text string for connection. Researchers also found that Miori can scan for and target vulnerable telnet hosts through the ThinkPHP Remote Code Execution. Within the Miori variant examined, researchers also located a message containing a URL of the site that allegedly sells the malware's code for $110. ***The NTIC Cyber Center recommends reducing the potential impacts of this malware by changing all default credentials on IoT devices and their associated administrator control panels as well as applying available security patches and firmware updates immediately after connecting them to a network. We also recommend placing IoT devices behind a firewall, blocking any unneeded ports that would allow external and unauthorized access, and monitoring the network for suspicious activity. If devices have publicly known vulnerabilities, but no updates or patches are available, we recommend immediately decommissioning the devices, if possible. For more information and the Indicators of Compromise (IoCs) associated with Miori, we encourage readers to reference the Trend Micro report here.***

New Ransomware Variant Targets QNAP NAS Devices

Anomali researchers discovered a new ransomware family called eCh0raix that targets QNAP Network Attached Storage (NAS) devices made by the Taiwanese company QNAP Systems, Inc. ECh0raix compromises QNAP devices, which provide cloud-accessible storage and backups to personal and

enterprise users, by brute-forcing weak credentials or exploiting known vulnerabilities. ECh0raix then encrypts files using the AES encryption algorithm and appends them with the *.encrypt* extension. According to the researchers, eCh0raix is used in targeted attacks and does not appear to be designed for mass distribution. There is currently no publicly available decryption key available for this ransomware. ***The NTIC Cyber Center advises administrators of QNAP NAS devices to restrict external access to devices, keep them updated with the latest security patches, and use strong passwords to secure access. In addition, administrators should reference the Anomali report for more information and IoCs associated with eCh0raix ransomware.***

Agent Smith Malware Infects over 25 Million Android Devices

Researchers at cybersecurity firm Check Point discovered a variant of mobile malware, dubbed Agent Smith, that has already infected over 25 million Android devices. Masquerading as a Google-related app, Agent Smith silently replaces installed apps on devices with malicious clones and delivers advertisements that earn revenue for the app's creator. Check Point researchers believe Agent Smith may be distributed through malware-laced applications disguised as free games, utility applications, or adult entertainment applications on the third-party Android application store 9Apps. Researchers express concern that, while the app is currently being used for the financial gain of attackers, it could easily be repurposed to perpetrate banking credential theft, eavesdropping, or other malicious activity. ***The NTIC Cyber Center recommends Android users avoid downloading apps from third-party application platforms. In addition, before installing any app, exercise caution and research both the app itself and the developer. Users who suspect that their devices have been compromised should perform a factory reset and restore devices to manufacturer default settings.***

Vulnerabilities

RingCentral and Zhumu

An independent security researcher discovered that a recently reported flaw in Zoom video conferencing software also affects two additional apps, RingCentral and Zhumu. Because these apps also use Zoom’s vulnerable software infrastructure, any Mac user who has ever installed either of them is at risk of downloading code that would enable threat actors to launch the video conferencing app and access their computers' webcams. Though RingCentral has issued a patch for devices running the app, users who have already uninstalled RingCentral remain vulnerable. Zhumu has not yet released a patch. ***The NTIC Cyber Center advises that, since Apple has issued a silent update to patch this vulnerability for current and former users of RingCentral or Zhumu, no further customer action is required.***

WordPress Plugin Ad Inserter

Security researchers found a critical vulnerability in Ad Inserter, a WordPress plugin, that enables attackers to remotely execute PHP code. This vulnerability, which may affect up to 200,000 WordPress-powered websites, allows attackers to acquire a nonce, or one-time communication block, and use it to circumvent WordPress security features. Ad Inserter has since developed a patch that addresses the vulnerability in their latest update, and WordPress has issued a statement discouraging the use of nonces for authentication, authorization, or access control. ***The NTIC Cyber Center recommends that administrators of WordPress sites using the Ad Inserter plugin update the plugin to the latest version, version 2.4.22, and refrain from using nonces as security features.***

Data Breaches and Leaks

A recent Maryland General Assembly audit report found that the Maryland Department of Education inappropriately stored the personal information, including social security numbers, of 1.4 million students and 230,000 teachers. The report indicates that the records were stored in plaintext format and not in encrypted format, as required by laws governing Maryland state agencies. The audit also reports that some Maryland systems had not been updated since 2008. The Maryland Department of Education has since agreed to encrypt sensitive information and upgrade all systems by September 30, 2019. ***Though there is no indication that third parties accessed this information, the NTIC Cyber Center recommends Maryland students and teachers remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text message, or other avenues as a result of this data exposure.***

A researcher from Security Discovery found that GE Aviation, a subsidiary of General Electric, accidently leaked its internal software configurations through an exposed Jenkins server. According to the researchers, the exposed server contained source code, plaintext passwords, configuration details, and private keys belonging to GE Aviation's internal infrastructure. Though GE's security team removed public access to the server after receiving the researcher's disclosure, it is not known if the server was accessed by third parties or for how long it remained exposed. GE indicates that the credentials found on the server mapped to internal network systems and that no customer or significant GE data was impacted by this breach. ***The NTIC Cyber Center reminds administrators of Jenkins instances to review***

accessibility settings to ensure that sensitive information is not publicly exposed.

A database belonging to education provider K-12 Inc. suffered a breach and exposed the sensitive information of over 19,000 students who used the company's A+nyWhere Learning System software package. The database contained over 7 million records and included the names, genders, birthdates, email addresses, and school names belonging to students in over 500 school districts. ***Though K-12 Inc. does not believe this information was accessed by third parties, the NTIC Cyber Center recommends students using the K-12 A+nywhere Learning System remain vigilant for an increase in phishing attempts perpetrated through email, social media, or other avenues as a result of this data exposure.***

A publicly accessible Amazon Web Services server belonging to Vitagene Inc., a DNA testing company for genetics and nutrition, may have been left unsecured, exposing client data records for several years. Data stored on this server includes customers' full names, birth dates, contact information, and genetic data. Vitagene Inc. indicates that credentials and financial data were not affected and that records with exposed names did not include genetic information. Vitagene Inc. has since blocked external access to the database and plans on notifying affected customers of the incident. ***The NTIC Cyber Center recommends affected users remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

Clinical Pathology Laboratories (CPL) recently reported that the data of 2.2 million patients was exposed as a result of the breach that impacted the American Medical Collection Agency (AMCA), a third-party billing collection provider, last month. With the latest addition of CPL customers included, the AMCA breach so far has affected over 22 million patients of numerous healthcare providers. Data exposed in this breach includes the full names, birth dates, service dates, balance information, and treatment price information of CPL customers, with an additional 34,500 customers also impacted by a breach of credit card or banking information. ***The NTIC Cyber Center recommends customers of CPL monitor their account statements, and immediately notify their financial institutions of any unauthorized or suspicious activity, and consider placing a fraud alert or security freeze on their credit file with Equifax, Experian, or TransUnion.***

A security researcher discovered an unsecured database server belonging to AavGo, a hotel operation service provider. The exposed data, comprised of over eight million entries, includes guest names, emails, phone numbers, hotel location, room types, dates of stay, and customer complaints. The database was allegedly left online without a password for three weeks. ***As hotel chains such as Holiday Inn Express and Zenique Hotels are among those that use AavGo's services, the NTIC Cyber Center recommends patrons of these chains remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

US mobile network provider Sprint announced that threat actors successfully breached an unknown number of accounts through the "add a line" website on Samsung[.]com. Sprint is sending letters to impacted customers informing them that, on June 22, the company discovered that hackers gained unauthorized access to user accounts and may have viewed information including phone numbers, device types, device IDs, monthly recurring charges, subscriber IDs, account numbers, account creation dates, upgrade eligibility, first and last names, billing addresses, and add-on services. Sprint reports that they have forced a reset of customer PINs to prevent further unauthorized access. ***The NTIC Cyber Center recommends that affected Sprint customers reset their account PINs when prompted and remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

Upcoming Webinars

A Hacker's Perspective: Where Do We Go from Here?

For 25 years or more, we have fought the battle of passwords and patches while, all around us, the world has developed, data has exponentially increased, attack surfaces are everywhere and technology had quite simply forced the human race to consider the evolution cycle in single lifespans as opposed to millennia.

During the last 25 years we have done little to protect the charges we are responsible for, we have failed to secure systems, allowed financial attacks, infrastructure attacks, and now attacks directly against humans. At what point will we be able to stem the bleeding and actually take charge of our realm? Have we left it too late, or are we still able to claw back out of the abyss and face our adversary in a more asymmetrical defensive manner? Can we actually provide safety and security to our charges or will we continue to fail? And, critically, how do we communicate this, and educate a population that is content to watch from the sidelines, while they are being digitally eviscerated.

To register for this free webinar on Monday, July 22 at 1:00 PM EDT, click here.

Secure the Core | Creating Resilient Business Applications

Did you know that public exploits for business applications have increased 100 percent since 2015? Today, over 77 percent of the world's transactional revenue touches an enterprise resource planning (ERP) system, making these applications an attractive target for cyber criminals looking to profit from the highly sensitive and regulated data that resides in them.
Through our research, focused on business applications over the past 10 years, we have discovered that nine out of 10 SAP customers have critical risk in their environment. Another bountiful attack surface exists in Oracle E-Business Suite (EBS) applications, where our researchers find a bug every two days.

Join us in this session to learn more about:

- Precise trends on the state of business application security;
- Insights into what some of the most trusted brands are doing to secure these critical systems.
- How to better protect your organization.

To register for this free webinar on Tuesday, July 30 at 11:30 AM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Have you ever seen a friend's social media post promoting a product at such an incredible discount, you *almost* couldn't resist clicking the advertisement and making a purchase? Not so fast! You may have encountered a ***fake social media ad scam***. Fake social media ad scams are social engineering schemes in which perpetrators use compromised social media accounts to post links to phishing websites disguised as product advertisements. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

US Mayors Group Adopts Resolution Not to Pay Any More Ransoms to Hackers

Analytic Comment: The United States Conference of Mayors unanimously adopted a resolution to not make any more ransom payments to hackers following ransomware infections. The Conference of Mayors, which includes 1,400 mayors of cities across the US with populations over 30,000, indicates that since 2013, 170 different city, county, or state systems have experienced a ransomware attack, with 22 of those attacks occurring in 2019. This resolution underscores the notion that paying ransom perpetuates the increasing threat of ransomware and encourages threat actors to launch more attacks. Furthermore, since paying the ransom does not guarantee that systems will be completely restored, this resolution provides appropriate procedural guidance when dealing with ransomware incidents.

BlueKeep Vulnerability a "Bleak" Situation for Local Governments, Tenable CTO Says

Analytic Comment: The BlueKeep vulnerability affecting Microsoft's Remote Desktop Protocol continues to pose risks to state and local governments using outdated operating systems. Although Microsoft has issued updates patching this vulnerability on legacy systems, many local governments using these systems have failed to apply these patches. Since BlueKeep is a wormable exploit, any ransomware with worm-like capabilities, such as WannaCry, can use this exploit to compromise vulnerable systems quickly. The ongoing threat posed by the BlueKeep vulnerability highlights the need for state and local governments to be diligent about keeping systems patched and updated to minimize the risk of ransomware attacks.

Urgent Cyber Warning for Hospitals over Threat of "WannaCry Repeat"

Analytic Comment: A recent threat report warns that the healthcare sector has not taken sufficient steps to protect against the threat of a future ransomware attack similar to WannaCry. Breached health records, vulnerable medical health devices, and understaffing of cybersecurity personnel continue to pose challenges for this industry. Additionally, new technologies such as artificial intelligence (AI) and interconnected health devices also heighten risks. These issues underscore the need for increased cybersecurity resources within the public health sector, as another WannaCry-type attack would prove disastrous given the current state of cybersecurity within this industry.

Patches and Updates

Chrome

Cisco

Drupal

Jira

Microsoft

Oracle

ICS-CERT Advisories

AVEVA Vijeo Citect and Citect SCADA Floating License Manager

Delta Industrial Automoation CNCSoft ScreenEditor

Philips Holter 2010 Plus

Schneider Electric Floating License Manager

Schneider Electric Interactive Graphical SCADA System

Siemens SIMATIC RF6XXR

Siemens SIMATIC WinCC and PCS7

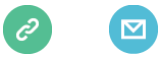
Siemens TIA Administrator (TIA Portal)

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

July 25, 2019

National Capital Region Cyber Threat Spotlight

Malicious LinkedIn Messages Leveraged in Iranian Cyber Espionage Campaign

FireEye security researchers warn of an Iranian cyber espionage campaign currently targeting users of the LinkedIn social networking platform with malicious phishing messages. Researchers believe that APT34, an Iranian advanced persistent threat group, used LinkedIn to craft fraudulent accounts and send documents that delivered malware designed to steal data and login credentials from unsuspecting victims. In this campaign, APT34 created a LinkedIn profile for a fictitious Cambridge University researcher and used it to target victims through the social media website's messaging platform. Though the group targeted individuals in a variety of industries, their primary efforts appear to be focused on financial, energy, and government sector entities in an effort to cultivate access to strategic geopolitical or economic information.

FireEye cautions that social networking sites offer a simple and effective platform for cyber threat actors to deliver malware, especially against organizations that rely on email defenses to mitigate intrusions. Additionally, as APT34 and other cyber threat actor groups have demonstrated, these sites also increasingly provide an attractive platform for foreign adversaries wishing to engage in cyber espionage.

The NTIC Cyber Center reminds social networking users to exercise caution when engaging with unknown individuals on these platforms, to avoid opening emails and attachments from unknown or untrusted sources, and to remain vigilant for indications of espionage activity perpetrated via social networking sites. For additional information on this ongoing and pervasive threat, please reference the NTIC Public Safety Center's recent advisory, "Beware of Espionage Efforts on Professional Networking Sites."

Federal Partner Announcements

CISA Releases Infographic on 5G Risks

The US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) released an infographic detailing risk factors associated with the upcoming rollout of 5G communications. CISA notes that, although the 5G network will increase the security, speed, and capacity of wireless communications, it will likely contain vulnerabilities that impact its own security and resilience. ***The NTIC Cyber Center recommends members review the DHS CISA infographic for information on the risks and benefits associated with 5G technology and communication networks.***

CISA Issues Resources for Combatting Foreign Interference

The US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) announced the release of several reference resources as part of the Agency's #Protect2020 initiative to secure elections and election infrastructure from foreign interference. These resources are intended to build partners' resilience to interference and misinformation—activities that undermine the interests of the United States, the security of our election process, and more. ***The NTIC Cyber Center advises partners and members to review these resources to develop and maintain awareness of mitigation strategies for combatting the threats of foreign influence and misinformation ahead of the 2020 election season.***

Current and Emerging Cyber Threats

Fraudulent Chrome and Firefox Updates Deliver Trickbot Malware

Attackers have created a fake Office 365 website that uses spoofed Chrome and Firefox browser updates to trick visitors into installing the Trickbot information-stealing Trojan malware. Though the fraudulent updates seem legitimate and feature convincing branding, they force the download of an executable that installs the Trickbot Trojan on users' systems. Once installed, Trickbot can remain undetected by the computer's task manager; communicate with a remote command and control server; and steal saved passwords, auto-filled form information, and browser history. ***The NTIC Cyber Center advises Internet users to remain vigilant for malicious activity perpetrated through fraudulent Office 365 websites or spoofed browser updates. In addition, we recommend only obtaining browser updates through auto-update features within the browser or via the browser developer's official website.***

Malicious App Mobonogram Infects Android Devices

Security researchers at Symantec discovered an Android messaging app called Mobonogram that runs hidden services and browses malicious websites in the background without user consent. Malware found in the Mobonogram app is configured to reboot automatically after two hours if it detects its processes are killed. This app, which is advertised as an unofficial version of the Telegram messaging app, was downloaded 100,000 times before it was removed from the Google Play app store. Security researchers also report finding a similar malicious app, called Whatsgram, on the Google Play store that was published by the same developers, RamKal Developers. ***The NTIC Cyber Center recommends Android users refrain from downloading Mobonogram or Whatsgram. In addition, before installing any app, exercise caution and research the app and the app's developer. Once an app is installed, monitor the app's requests for permission authorizations and data activity. Users who suspect that their devices have been compromised should perform a factory reset and restore devices to manufacturer default settings.***

New Extenbro Trojan Blocks Antivirus Software on Infected Machines

Security researchers have identified a Trojan dubbed Extenbro that serves adware and prevents infected machines from accessing software security updates and security-related websites. By using Domain Name Server (DNS) changing to block a machine's access to legitimate security websites, Extenbro effectively disables anti-malware and anti-adware security software running on infected machines. Extenbro adds two additional DNS servers and is configured to maintain persistence upon reboot even if these servers are deleted. ***The NTIC Cyber Center encourages administrators to***

reference Malwarebytes Labs's blog post on Extenbro for IoCs and information on how to remove Extenbro from infected machines.

Phishing Campaign Targets American Express Customers

Cofense Phishing Defense Center researchers discovered an email phishing campaign targeting American Express customers. The campaign's malicious emails masquerade as system maintenance alerts from American Express and threaten account suspension if victims do not click the embedded link. When clicked, the malicious link forwards recipients to a landing page that spoofs the American Express customer login page and phishes for user credentials. Emails in this phishing campaign feature an HTML element that can prevent email security filters from detecting the malicious URL and hide the URL when recipients hover over the suspicious link. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as alerts from American Express, avoid opening unexpected emails, and refrain from clicking on links from unknown or untrusted sources.***

Vulnerabilities

Ellucian Banner

The U.S. Department of Education issued a security alert concerning the ongoing exploitation of a vulnerability in Ellucian Banner, a student management platform, that has affected 62 unnamed higher education institutions to date. The vulnerability, CVE-2019-8978, allows threat actors to hijack sessions, create new accounts, and cause denial-of-service attacks. The Department of Education indicates that over 600 fraudulent student accounts were reportedly created in a 24-hour period, and the Department expresses concern that threat actors could further manipulate the Banner system to influence aspects of administration including student financial aid. The following Ellucian Banner products are impacted by this vulnerability: Ellucian Banner Web Tailor (versions 8.8.3, 8.8.4, 8.9) and Banner Enterprise Identity Services (versions 8.3, 8.3.1, 8.3.2, 8.4.) ***The NTIC Cyber Center recommends administrators of educational institutions using vulnerable Ellucian products contact Ellucian for guidance on patching or upgrading affected systems. In addition, the Department of Education requests that institutions using vulnerable Ellucian products immediately contact both FSASchoolCyberSafety@ed.gov and CPSSAIG@ed.gov with the name of the institution as well as the name, telephone number, and email address of an institutional point of contact for guidance on mitigating risks posed by these vulnerabilities.***

ProFTPD

Security researcher Tobias Mädel discovered a vulnerability within ProFTPD, an open-source File Transfer Protocol (FTP) service with cross-platform functionality that can support Windows and UNIX-like systems. The vulnerability, identified as CVE-2019-12815, allows threat actors, both authenticated and anonymous, to execute arbitrary code and perform information disclosure attacks. The vulnerability is attributed to a bug in the SITE CPFR and SITE CPTO commands that bypass "Limit WRITE" DenyAll directives, allowing unauthorized users to copy or modify files without permission. CVE-2019-12815 affects all ProFTPD versions up to and including the latest version, 1.3.6, although a temporary workaround is available for 1.3.6. ***The NTIC Cyber Center recommends administrators keep all systems and software up-to-date with the latest security patches and disable the mod_copy module as a workaround for servers running version 1.3.6.***

Upcoming Webinars

Realizing the Strategically Essential Value of Good Third-Party Cybersecurity Risk Management

Really good third-party cybersecurity risk management is essential to enterprise success. Done well, it enables an organization to realize, at the speed of business, the benefits of outsourced systems and services. Done poorly, it results in the business missing out on strategically important opportunities or, even worse, results in data breaches and operational outages.

So, what does good third-party cybersecurity risk management look like? Well, look no further than the patterns used to manage internal enterprise information security risk. How do you do this? With good risk processes operated on a foundation of good data, analytics, and automation. In this webinar, we will show you how to realize the strategically essential value of good third-party cybersecurity risk management.

To register for this free webinar on Wednesday, July 31 at 1:30 PM EDT, click here.

Ransomware Hostage Rescue Guide

It is estimated that a business falls victim to a ransomware attack every 40 seconds, adding up to a projected $11.5 billion in damages for this year. As ransomware attacks become more targeted and

damaging, your organization faces increased risk that can have your networks down for days or even weeks.

So, how can your organization avoid getting held hostage? Join Erich Kron, CISSP, and Security Awareness Advocate at KnowBe4 as he looks at scary features of new ransomware strains, gives actionable info that you need to prevent infections, and provides tips on what to do when you are hit with ransomware.

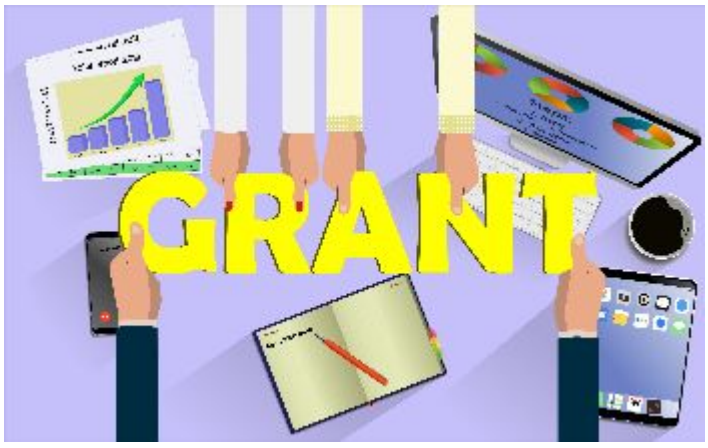
In this webcast he will cover:

- What new scary ransomware strains are in the wild
- Am I infected?
- I'm infected, now what?
- Proven methods of protecting your organization?
- How to create a "human firewall"

To register for this free webinar on Tuesday, August 13 at 11:30 PM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.



Government grant scams are a type of social engineering scheme in which perpetrators use the promise of grant funding to steal money and/or elicit personally identifiable information (PII) from victims. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

BEC Scams Cost US Firms $300m Each Month

Analytic Comment: According to a report from the US Department of Treasury's Financial Crimes Enforcement Network (FinCEN), business email compromise (BEC) scams are on the rise, costing US victims an average of $301 million per month in 2018 compared to a reported $110 million in 2016. BEC scams are social engineering schemes in which threat actors send emails disguised as legitimate corporate correspondence to trick recipients into sending money or divulging sensitive information. In addition to becoming more costly, these scams are also more numerous; around 1100 instances were reported per month in 2018, contrasting with 500 per month in 2016. FinCEN also reports that 73 percent of all scams involved transfers of money into US bank accounts instead of overseas accounts, a statistic that reflects scammers' ongoing reliance on money mule networks to launder illicitly-obtained funds. FinCEN's report underscores the need for organizations to maintain awareness of the increasing prevalence and dangers of BEC scams. For more information on BEC scams, please read our Securing Our Committees (SOC) blog post here.

US Troops Using Russia-Connected FaceApp Urged to Be Cautious

Analytic Comment: Several US Military organizations have issued statements warning military members of the dangers associated with FaceApp, a mobile app that can make users appear older in photographs. FaceApp is a product of a Russian-owned company and has already been downloaded 12.7 million times. The US European Command (USEUCOM) and the US Marine Corps have both released statements that included samples of FaceApp's user agreement, which authorizes the app owners a "perpetual, irrevocable, royalty-free, worldwide license to use, reproduce, modify, distribute and display user content and any name or username in all media formats." The US Air Force issued a similar message to its Facebook followers, citing counterintelligence, privacy, and operational security (OPSEC) concerns. These warnings serve as a reminder that, although new apps and technology may offer fun and tempting features, there may be numerous dangers and risks associated with their use.

Patches and Updates

Apple

ICS-CERT Advisories

GE Aestiva and Aespire Anesthesia (Update A)

Mitsubishi Electric FR Configurator2

NREL EnergyPlus

We welcome your feedback.

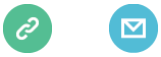
Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

August 1, 2019

National Capital Region Cyber Threat Spotlight

Capital One Data Breach Impacts 100 Million Customer Accounts

Capital One Financial Corporation announced a data breach that compromised the personal and sensitive information of 106 million Capital One bank customers in the US and Canada. This data, stolen from customer accounts and credit card applications, includes customer names, addresses, phone numbers, email addresses, dates of birth, credit scores, account balances, and credit limits. Additionally, 80,000 bank account numbers, 140,000 Social Security numbers of American customers, and 1 million Social Insurance numbers of Canadian customers were reportedly compromised in this data breach.

According to the Federal Bureau of Investigation (FBI), the hacker allegedly responsible for the breach gained unauthorized access to improperly secured Amazon Web Services cloud servers, known as Simple Storage Service (S3) buckets, and exfiltrated 30 gigabytes of data belonging to Capital One. In addition to stealing Capital One data, the accused hacker may have accessed and stolen data belonging to other major organizations as well. The FBI does not believe the compromised Capital One customer information has been disseminated or used for fraudulent purposes as of this time.

The NTIC Cyber Center encourages all Capital One customers to immediately place a fraud alert or security freeze on their credit file with Equifax, Experian, and TransUnion. In addition, we recommend that victims of this breach monitor their financial account statements closely, report any

unauthorized or suspicious activity to their financial institutions, and remain vigilant for phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure. Capital One will be offering free credit monitoring and identity protection services to affected customers. For questions or concerns, call the Capital One service line at 1-800-227-4825.

Federal Partner Announcements

2019 CISA Cybersecurity Summit

The Cybersecurity and Infrastructure Security Agency (CISA) invites government and infrastructure stakeholders from around the world to participate in the 2019 CISA Cybersecurity Summit. The Summit will feature presentations focused on emerging technologies, vulnerability management, incident response, risk mitigation, and other current cybersecurity topics. The Summit provides the opportunity for federal, state, local, tribal, and territorial government agencies, as well as private sector organizations, to highlight successes and opportunities for collective action.

- **Dates:** September 18 - 20, 2019
- **Location:** National Harbor, MD

Registration: More details about the agenda, programming, and registration will become available here. Organizations are also invited to submit presentation proposals to cybersummit@hq.dhs.gov.

Steps to Safeguard against Ransomware Attacks

CISA, the Multi-State Information Sharing & Analysis Center (MS-ISAC), National Governors Association (NGA), and the National Association of State Chief Information Officers (NASCIO) have released a Joint Ransomware Statement with recommendations for state and local governments to build resilience against ransomware:

1. **Back up systems—now (and daily).** Immediately and regularly back up all critical agency and system configuration information on a separate device and store the backups offline, verifying their integrity and restoration process. If recovering after an attack, restore a stronger system than the one lost, fully patched and updated to the latest version.

2. **Reinforce basic cybersecurity awareness and education.** Ransomware attacks often require the human element to succeed. Refresh employee training on recognizing cyber threats, phishing, and suspicious links—the most common vectors for ransomware attacks. Remind employees of how to report incidents to appropriate IT staff in a timely manner, which should include out-of-band communication paths.
3. **Revisit and refine cyber incident response plans.** Have a clear plan to address attacks when they occur, including when internal capabilities are overwhelmed. Make sure response plans include how to request assistance from external cyber first responders, such as state agencies, CISA, and MS-ISAC, in the event of an attack.

CISA encourages organizations to review the Joint Ransomware Statement and the following ransomware guidance:

- MS-ISAC Security Primer on Ransomware
- CISA Tip Sheet on Ransomware
- NGA Disruption Response Planning Memo
- NASCIO Cyber Disruption Planning Guide

Additionally, the NTIC Cyber Center provides a full list of ransomware prevention and mitigation strategies, along with a guide for cyber incident response planning, available on our website.

Current and Emerging Cyber Threats

Watchbog Malware Scans for BlueKeep Vulnerability

A variant of the cryptocurrency-mining botnet malware, Watchbog, scans for systems vulnerable to BlueKeep, a vulnerability that would allow the unauthorized execution of arbitrary code on a remote system. Once the machine has been infected, this malware will parse through a list of vulnerable IP addresses and deliver it to the its associated command-and-control (C2) server. Leading theories suggest the Watchbog scan will be used to compile a list of vulnerable devices for future attacks or sold to third parties. ***The NTIC Cyber Center recommends network administrators who have not yet patched systems to protect them against the BlueKeep vulnerability do so as soon as possible. A free tool has been created to help administrators scan for systems vulnerable to BlueKeep and is available via links provided in the Bleeping Computer article here. We also recommend blocking the associated Watchbog Indicators of Compromise (IoCs) available on the Intezer website. Lastly, we recommend network administrators proactively block TCP port 3389 at the perimeter firewall to protect unpatched systems within a secured network and disable unneeded Remote Desktop Services in their environment.***

Phishing Campaign Uses WeTransfer Alerts to Bypass Filters

Researchers at Cofense Phishing Defense Center discovered a new phishing campaign that abuses WeTransfer "shared file" notifications to deliver malicious links to victims. The attackers behind this campaign use WeTransfer, a cloud-based file transfer platform, to host malicious files and email fraudulent notifications to unsuspecting victims in an effort to bypass email security filters. To lend credence to the campaign, the attackers will customize the notifications and claim there are invoices ready for review. If victims click the "Get your files" button embedded in the emails, they will be redirected to another page hosting an HTM or HTML file. If the victim opens the malicious file, it will open a phishing landing page in the browser that's designed to steal login credentials for various online platforms. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as alerts from WeTransfer, avoid opening unexpected emails, and refrain from clicking on links from unknown or untrusted sources.***

Lenovo Iomega NAS Devices Targeted in Ransom Scheme

Remote threat actors are targeting publicly exposed Lenovo Iomega network-attached storage (NAS) devices, deleting their files, and leaving ransom notes named *YOUR FILES ARE SAFE!!!.txt* that demand between 0.01 and 0.05 Bitcoin to return the stolen data. Although it is currently unknown how the threat actors are gaining access, Iomega NAS devices do have publicly accessible web interfaces that allow users remotely access their files and, if not properly secured, these interfaces could allow unauthorized access to data stored on the NAS. Further inspection reveals that the data in this campaign is deleted rather than encrypted and, therefore, could possibly be recovered using file recovery software. Reports indicate that other unsecured NAS devices such as QNAP and Synology are under attack as well. ***The NTIC Cyber Center recommends securing NAS devices with complex and unique login credentials, placing it behind a firewall, and ensuring that it is only accessible via a virtual private network (VPN) to help protect stored data from unauthorized access. We also strongly advise against reusing the same login credentials across multiple accounts to reduce the risk of compromise in credential stuffing attacks. To read more about how to protect yourself from credential stuffing attacks, please read our product titled "*** *Credential Stuffing Attacks – A Growing Yet Easily Mitigated Threat* ***."***

New Ransomware Variant Targets Android Devices

ESET Mobile Security researchers discovered a new ransomware variant that targets devices running the Android operating system, dubbed *Android/Filecoder.C*, that has been active since July 12, 2019. *Android/Filecoder.C* spreads primarily through text messages, or SMS messages, that contain malicious links. When clicked, these links will download a malicious Android application package (APK) file onto the device and prompt the victim to begin installation. If installed, the malware begins encrypting files and propagates itself by sending malicious links to everyone in the victim's contact list. The threat actors behind this campaign are also spreading *Android/Filecoder.C* through online forums such as Reddit and XDA Developers. ***The NTIC Cyber Center recommends Android users keep device operating systems up-to-date. Before installing any app, exercise***

caution and research both the app itself and the developer. Once an app is installed, monitor the app's requests for permission authorizations and data activity. Beware of any applications that request permissions that do not match the advertised app functionality.

Vulnerabilities

Multiple VPN Applications

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of vulnerabilities affecting multiple VPN applications. A remote attacker could exploit these vulnerabilities to take control of an affected system. CISA encourages administrators to review the following security advisories and apply the necessary updates:

- Palo Alto Security Advisory PAN-SA-2019-00200
- FortiGuard Security Advisory FG-IR-18-384
- Pulse Secure Security Advisory SA44101

Das U-Boot

Semmle, a code analysis platform provider, publicly disclosed 13 vulnerabilities in the Das U-Boot open-source universal boot loader. When U-Boot is used for networking to retrieve next stage boot resources, threat actors can exploit the vulnerabilities to conduct remote code execution. ***The NTIC Cyber Center recommends users review the 13 vulnerabilities, monitor systems for unusual and suspicious activity, and update the U-Boot boot loader if and when a patch becomes available. If vulnerable, discontinue the use of any U-Boot networking functionality and mount filesystems via the Network File System (NFS).***

Wind River VxWorks RTOS

Researchers from Armis, an Internet-of-Things (IoT) security firm, have discovered a collection of 11 zero-day vulnerabilities dubbed "Urgent/11" in the VxWorks real time operating system (RTOS). If exploited, these vulnerabilities could allow threat actors to cause denial-of-service (DoS) conditions, logical errors, information leaks, remote code execution, and remote system takeover. VxWorks is reportedly used in more than two billion devices including routers, modems, and firewalls and operate in a variety of industries such as healthcare, manufacturing, and security. There are currently no recorded incidents of the vulnerabilities being exploited in the wild and patches are available. ***These vulnerabilities affect the following VxWorks versions 6.5-6.9, 7 (SR540 and SR610) and Versions of VxWorks using the Interpeak standalone network stack. The***

NTIC Cyber Center recommends administrators to keep all systems and software up-to-date with the latest security patches and properly segment their network to isolate the system from external and unauthorized access.

Data Breaches and Leaks

Credit reporting agency, Equifax, agreed to pay a multimillion-dollar settlement as a result of the data breach it suffered in 2017. The breach affected over 140 million consumers and led to the compromise of their personal information such as names, birth dates, Social Security numbers, credit card numbers, and driver's license numbers. As a result, victims could be eligible for a cash payment of up to $125 or free credit monitoring. To find out if you are eligible for compensation, visit the Equifax Data Breach Settlement website and follow the instructions provided. The deadline for filing a claim is January 22, 2020. Please note that the US Federal Trade Commission (FTC) is warning victims about fake settlement websites that have begun appearing online and urges consumers to only file through the official settlement website. ***The NTIC Cyber Center recommends victims seeking compensation only file a claim using links provided on the FTC website.***

A security researcher discovered an unsecured Elasticsearch database containing information related to the internal network and computers of the Honda Motor Company. The data includes details on internal computers such as machine hostname, MAC address, IP address, operating system version, patches applied, and the status of Honda's endpoint security software. ***Though Honda does not believe the information any third parties other than the researcher accessed company information, the NTIC Cyber Center recommends administrators of Elasticsearch databases reference instructions for configuring Elasticsearch cluster security to reduce the risk of unauthorized access.***

A security researcher recently accessed a cloud server belonging to cybersecurity company Comodo using a publicly exposed email address and password. The server credentials, which were found in a public GitHub repository, allowed the researcher to access and view Comodo internal files and documents containing sales information, biographies, contact information, photographs, customer contracts, calendars, and more. ***The NTIC Cyber Center reminds administrators to properly secure access to GitHub repositories or any other resources that, if publicly viewable, could place sensitive information, proprietary code, or account credentials at risk of exposure or theft. We also recommend organizations regularly check their public repositories for sensitive information that has been inadvertently uploaded or stored.***

Upcoming Webinars

StaySafeOnline.org
Powered by National Cyber Security Alliance

What Are Phishing, Vishing, and Smishing and How Can I Protect My Small Business?

You may have heard of the term phishing, but do you really know what it means and how you can protect yourself from this type of cyber threat? What about other threats such as smishing and vishing? Join the National Cyber Security Alliance and Infosec on August 13 and we'll break down these terms and outline steps you can take to protect yourself from cyber criminals.

To register for this free webinar on Tuesday, August 13 at 2:00 PM EDT, click here.

helpsystems

The Rise of Insider Threats and How to Prevent Them

Whether it's a negligent employee or the result of espionage, insider threats are now on almost every cybersecurity expert's list of top concerns. This anxiety about insider threats and their management was recently illustrated with the new Insider Threat Report by Cybersecurity Insiders, sponsored by HelpSystems. For instance, 70 percent of cybersecurity professionals surveyed believe that insider attacks have become more frequent in the past year alone. Even more alarming is the fact that 62 percent of organizations experienced at least one insider attack in the last year, and that over 80 percent of respondents listed the average remediation cost at over $100,000 per incident. With these worrisome statistics, it's more important than ever to take action. Join Bob Erdman,

Senior Cybersecurity Product Manager at HelpSystems and Mike Lynch, Senior Sales Engineer at Core Security for actionable advice on how to keep insider threats out of your organization. Learn about important, achievable strategies, including:

- Implementing the right tools
- Focusing on swift detection and deterrence
- Effectively managing user privileges
- Increasing protection of most vulnerable data
- Maintaining policies to ensure proper configuration
- Additional employee training to increase awareness

To register for this free webinar on Tuesday, August 20 at 11:00 AM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Payroll diversion scams, also known as direct deposit diversions, are social engineering scams in which perpetrators send deceptive emails to human resources or finance departments to divert direct

deposit payments to a bank account they control. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

15 Signs You've Been Hacked -- and How to Fight Back

Analytic Comment: Even regularly maintained antivirus or anti-malware solutions have difficulty keeping pace with malicious signatures, often failing to quickly detect and block new and emerging threats. However, in the absence of accurate antivirus or anti-malware alerting, there may be several signs indicating that a computer has been compromised. These may include ransomware messages, spoofed antivirus messages, unwanted browser toolbars, redirected internet searches, popups, unexpected software installations, and more, with each symptom requiring a unique approach to mitigation and system restoration. Computer users should familiarize themselves with these symptoms and recognize the signs of infection in the event virus protection solutions fall short.

Over 23 Million Stolen Credit Cards Are Being Traded on the Dark Web

Analytic Comment: Cybersecurity firm Sixgill revealed in their recent Underground Financial Fraud report that American credit and debit card data comprise the majority of stolen card data on the dark web as compared to the rest of the world. Sixgill analyzed 23 million credit cards and discovered that the United States accounts for 64.49 percent of the total available financial data. The report also reveals that criminals are increasingly using encrypted platforms to trade this type of data over centralized marketplaces. This underscores the importance of regularly reviewing financial account statements for unauthorized charges and immediately reporting suspicious account activity to the appropriate financial institutions.

Patches and Updates

Chrome

ICS-CERT Advisories

CAN Bus Network Implementation in Avionics

Prima Systems FlexAir

Wind River VxWorks

We welcome your feedback.

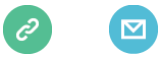
Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

August 8, 2019

National Capital Region Cyber Threat Spotlight

Private Sector Organizations Issue Bulletin on Magecart Online Skimming Threats

The PCI Security Standards Council and the Retail & Hospitality ISAC issued a joint bulletin warning of the continuing threat of online skimming attacks. These threats, known as Magecart attacks, primarily target ecommerce websites, though security researchers have recently observed these attacks infecting non-ecommerce sites as well. By injecting malicious code into vulnerable plugins or third-party software libraries, Magecart attackers can compromise numerous websites simultaneously to steal customer data such as names, billing addresses, email addresses, phone numbers, credit card details, usernames, and passwords. Magecart attacks have resulted in the theft of payment card details and personal information of millions of victims to date, and they continue to pose significant risks to websites that are not configured with effective security controls.

The NTIC Cyber Center recommends administrators review the suggested best practices, which include regularly testing web applications for vulnerabilities, implementing file integrity monitoring or change-detection software, performing periodic penetration testing to identify weaknesses, and keeping antimalware solutions and security patches up to date, among other recommendations.

To read more about the threat of Magecart attacks and for additional mitigation strategies, please see our recent Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Federal Partner Announcements

SWAPGS Spectre Side-Channel Vulnerability

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of a vulnerability (CVE-2019-1125) known as SWAPGS, which is a variant of Spectre Variant 1—that affects modern computer processors. This vulnerability can be exploited to steal sensitive data present in a computer systems' memory.

Spectre is a flaw an attacker can exploit to force a program to reveal its data. The name derives from "speculative execution"—an optimization method a computer system performs to check whether it will work to prevent a delay when actually executed. Spectre affects almost all devices including desktops, laptops, and cloud servers.

CISA encourages users and administrators to review the following guidance, refer to their hardware and software vendors for additional details, and apply an appropriate patch when available:

- Microsoft: Windows Kernel Information Disclosure Vulnerability
- Red Hat: Spectre SWAPGS gadget vulnerability
- Google: Spectre Side Channels

CISA Warns of El Paso and Dayton Tragedy-Related Scams and Malware Campaigns

CISA warns of possible malicious cyber activity perpetrated in the wake of recent tragic events in El Paso, TX and Dayton, OH. The agency advises users to beware of threats including emails containing malware or links to phishing sites, fraudulent requests for donations, or scams conducted through social media pleas, calls, texts, or door-to-door solicitations.

CISA suggests the following preventative measures to avoid becoming a victim of malicious activity:

- Use caution when opening email attachments, and do not click on links in unsolicited email messages. Refer to CISA's Tip on Using Caution with Email Attachments.
- Review CISA's Tip on Staying Safe on Social Networking Sites.

- Refer to CISA's Tip on Avoiding Social Engineering and Phishing Attacks.
- Review the information from the Federal Trade Commission on Before Giving to a Charity.

To learn more about malicious schemes surrounding tragic events and the mitigation strategies recommended for combatting them, please reference the NTIC Cyber Center's blog posts on charity scams and disaster scams.

IRS Reminds Tax Professionals: Beware of Phishing Emails

The Internal Revenue Service (IRS) has issued a news release warning tax professionals of the continued threat of phishing emails. Phishing emails are one of the most common ways cyber criminals steal sensitive data. Educating personnel on the risks posed by phishing emails is part of the Taxes. Security. Together. Checklist, which IRS created to help tax professionals protect sensitive taxpayer data.

NIST Publishes Multifactor Authentication Practice Guide

The National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) has published NIST Cybersecurity Practice Guide: Multifactor Authentication for E-Commerce. The guide provides e-commerce organizations multifactor authentication (MFA) protection methods they can implement to reduce fraudulent purchases.

The NTIC Cyber Center recommends all members review the NIST Guide as well as our recent Cyber Advisory titled Credential Stuffing Attacks - A Growing Yet Easily Mitigated Threat to learn more about how multifactor authentication can help reduce the risk of online account compromise.

Industry Report

The Evolution of Cyber Attacks in 2019

Threat actors continue to improve their cyber weapons, quickly adopting new methods and adapting their attacks to emerging technologies. While cryptomining attacks are on the decrease, banking malware has seen a 50 percent increase since 2018. The *2019 Mid-Year Trends Report* provides a comprehensive overview of cryptominers, ransomware, botnets, banking Trojans, and data breaches. This cyber security report also includes:

- An in-depth look at attack trends in cloud, mobile, email, and software supply chains
- Major cyber breaches during the first half of 2019
- Key insights into major worldwide malware types

The report is available for free via the Check Point website here.

Current and Emerging Cyber Threats

New Spear Phishing Campaign Spreads LookBack Malware

Security researchers uncovered a new spear phishing campaign conducted against three US organizations within the utility sector that spoofs the domain of the National Council of Examiners for Engineering and Surveying (NCEES). These spear phishing emails masquerade as notices of failed examinations by the NCEES and contain Word documents configured with malicious macros that, when enabled, install a new Remote Access Trojan (RAT) dubbed LookBack. LookBack is a sophisticated RAT that can take screenshots, remotely operate a computer's cursor, view process, system, and file data, and execute additional commands, such as file deletion. LookBack also has a command and control (C2) server and channel. It is believed that the LookBack campaign is state-sponsored, although attribution has yet to be determined. ***The NTIC Cyber Center recommends remaining vigilant against phishing attempts and refraining from opening documents attached to suspicious or unexpected emails.***

SystemBC Malware Uses SOCKS5 Proxies to Hide Malicious Traffic

Researchers at cybersecurity firm Proofpoint recently discovered SystemBC, a malware variant distributed via the Fallout and RIG exploit kits that hides its network traffic by passing it through compromised computers that act as SOCKS5 proxy servers. It also uses Hypertext Transfer Protocol Secure (HTTPS) connections to encrypt network traffic to associated C2 servers. This allows SystemBC to deliver other malware variants to infected machines, evade firewall detection, bypass Internet content filters, and hide their IP addresses. Proofpoint suggests that SystemBC is likely being sold on Dark Web marketplaces. ***The NTIC Cyber Center recommends all network and system administrators ensure that all software, including operating systems, webserver plugins, content management systems, and antivirus software applications are patched and up-to-date and***

decommission vulnerable legacy systems, if possible. We also recommend restricting administrative privileges on user accounts and blocking the associated SystemBC Indicators of Compromise (IoCs) available on the Proofpoint website.

Sextortion Campaign Targets Database of Compromised Email Addresses

Researchers at Cofense Labs discovered an active sextortion campaign using spam botnets to target a database of more than 200 million compromised email accounts. The spam emails used to target victims contain login credentials pulled from data breach dumps to lend credence to the threat actor's claims that the victims' accounts and computers are compromised. Cofense estimates that victims have paid more than $1.5 million to sextortion scammers so far this year. ***The NTIC Cyber Center would like to remind our members to ignore sextortion scam attempts. We also encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication on any account that offers it to limit the impact of credential compromise. For more information on sextortion scams, please review our product titled Securing Our Communities: Sextortion Scams.***

Data Breaches and Leaks

Online clothing marketplace Poshmark recently disclosed a breach of user data stored in company servers. According to Poshmark's security notice, an unauthorized third party acquired customer profile information such as full name, username, city of residence, email address, size preferences, social media profile information, and encrypted passwords. The company believes that no customer financial or physical address information was accessed and, because hashed passwords were uniquely salted with a one-way encryption, the exposed passwords are nearly impossible to use to access customer accounts. Nevertheless, the company has recommended that users change their passwords as a security precaution. ***The NTIC Cyber Center recommends that Poshmark users enable multifactor authentication on any account that offers it, monitor their accounts for suspicious activity, and remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text message, or other avenues as a result of this data exposure.***

A security researcher discovered numerous unprotected and publicly accessible Jira servers exposing data about internal projects and users. The servers, owned by organizations including Google, Yahoo, NASA, Lenovo, 1Password, Zendesk, and several government entities and educational institutions, revealed information such as project development details and names, roles, and employee email addresses. The researcher believes that the inadvertent exposure was caused by misconfigured server access options and settings that control visibility of filters and dashboards in projects. ***The NTIC Cyber Center advises administrators of Jira servers to review accessibility and security settings of servers to ensure sensitive or proprietary information is not exposed publicly.***

Online custom clothing and merchandise retailer CafePress suffered a breach of data that exposed the information of over 23.2 million user accounts. According to a researcher who reported the incident to Have I Been Pwned, a website that tracks breaches of websites globally, the CafePress breach compromised records such as customer names, email addresses, physical addresses, and phone numbers, as well as encrypted passwords of roughly half of the affected users. ***The NTIC Cyber Center recommends CafePress customers reset their account passwords, enable two-factor authentication on any account that offers it, and remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text message, or other avenues as a result of this data exposure.***

StockX, a sneaker and fashion apparel trading platform, disclosed a data breach that compromised 6.8 million records. Data affected includes customer names, shipping addresses, email addresses, usernames, hashed passwords, and purchase histories. According to the company, no customer financial information was compromised. StockX has issued a password reset for all customers and they have implemented a system-wide security update, credential rotation on all servers and devices, and a lockdown of their cloud computing perimeter. ***The NTIC Cyber Center recommends StockX customers change their StockX login credentials when prompted and to remain vigilant for increase in phishing attempts perpetrated through email, social media, or other avenues as a result of this data exposure.***

Upcoming Webinars

Access & Authentication: Better Together for IT & End Users

Ensuring your employees have the right level of access to their work and nothing more has never been easy. It's even more challenging now for IT to ensure that a user is who they say they are with users bringing more apps, devices, and networks into the workplace. Combining access and authentication solutions to one unified solution provides visibility and security that can't be achieved with disparate tools.

Join the LastPass team as they discuss new market research on how businesses are handling access and authentication today and provide insight into how these solutions are increasing company security, including:

- The role of access and authentication technologies like single sign-on, password management, and multifactor authentication in small and medium-sized businesses
- Why doing one without the other can leave your business at risk of breach
- Best practices for getting started with access and authentication

To register for this free webinar on Thursday, August 22 at 11:30 AM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Have you ever received an unsolicited phone call or email from someone offering to help fix a computer problem? How about a pop-up or error message indicating your device was infected and urging you to contact a support person who could help? If so, you were a target of a ***tech support scam***. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

What We Can Learn from the Capital One Hack

Analytic Comment: As more information about the Capital One breach becomes available, it has become clear that the hacker relied on relatively well-known methods rather than novel or sophisticated techniques to gain unauthorized access to the trove of sensitive customer data. An investigation of the breach revealed that a misconfigured Web Application Firewall provided the hacker with an opportunity to exploit a Server Side Request Forgery vulnerability and send specially crafted requests to a back-end server on the Amazon Web Services platform. The requests ultimately allowed the hacker to access data stored on that server. This breach highlights the importance of properly configuring, securing, auditing, and monitoring any cloud instance that contains sensitive data or is critical to business operations.

Cyberattacks Against Industrial Targets Double Over the Last 6 Months

Analytic Comment: According to a report from IBM X-Force Incident Response and Intelligence Services (IRIS), cyber attacks conducted with the sole purpose of destroying and incapacitating systems have doubled over the past six months and half of the organizations affected by these attacks are in the manufacturing sector. Additionally, the report indicates that, although nation-state actors commonly use destructive malware variants in attacks, non-government affiliated cyber criminals have begun to adopt the same or similar destructive tactics as well. As this report highlights, it is imperative for organizations to implement and maintain a robust data backup plan to help mitigate against these increasingly debilitating cyber attacks.

Patches and Updates

Cisco Releases Security Updates

Cylance Antivirus Vulnerability

VMware Releases Security Updates for Multiple Products

ICS-CERT Advisories

3S-Smart Software Solutions GmbH CODESYS V3 -1

3S-Smart Software Solutions GmbH CODESYS V3 -2

Advantech WebAccess HMI Designer

Fuji Electric FRENIC Loader

LCDS LAquis SCADA LQS File Parsing

Rockwell Automation Arena Simulation Software

We welcome your feedback.

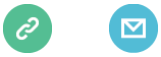
Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

August 15, 2019

National Capital Region Cyber Threat Spotlight

Highlights and Key Takeaways from DEFCON 27

Last week, NTIC Cyber Center team members attended DEFCON – a four-day annual cybersecurity and hacking conference – to learn about the latest vulnerabilities, exploits, and research conducted by cybersecurity experts across the globe. The theme of this year's DEFCON conference was "The Promise of Technology" and included a lineup of presentations and activities specifically designed to, according to conference organizers, "reflect the real costs of technology" and "strengthen those things that help us do good, and weaken the things that enable us to do bad." In previous years, hackers and cybersecurity experts sharing their research at DEFCON participated in such unofficial contests as "Spot the Fed," whereby attendees were encouraged to identify potential law enforcement officers and intelligence officials sent to conduct surveillance and possibly arrest subjects of interest. However, this year, the aim of the conference shifted with the goal of bringing the cybersecurity and government communities together to help solve complex technological problems all of us face as a result of our increasingly interconnected world.

To read more about what the NTIC Cyber Center learned during DEFCON 27, please see our post titled The NTIC Cyber Center Goes to DEFCON: Highlights and Key Takeaways.

Industry Report

BlackBerry Cylance 2019 Threat Report

BlackBerry Cylance Research and Intelligence published its annual threat report for 2019, which contains the top OS X and Windows-based threats encountered by their customers, notable advanced persistent threat (APT) activity, and year-over-year analysis. Readers will also find sections detailing attacks on Office365 services, credential-based hacks, and current consumer sentiment regarding cybersecurity solutions. This report also features in-depth examination of Emotet, a former banking Trojan upgraded into a modular attack platform, examines novel and complex threat obfuscation techniques, and offers specific cybersecurity-related predictions for the upcoming year.

The report is available for free via the BlackBerry Cylance website here.

Current and Emerging Cyber Threats

Robocall-Blocking Apps Discovered Sending Data to Third Party Data Collection Firms

A researcher from cybersecurity firm NCC Group discovered several popular robocall-blocking mobile apps sending data to third party data analytics companies without users' consent. According to the researcher, apps such as TrapCall, Truecaller, and Hiya collect and exfiltrate data such as phone numbers, device types, device models, software versions, and other information. Some apps collect and send user information as soon as the application is first opened and before users consent to any privacy policies. ***The NTIC Cyber Center recommends that users seeking robocall-blocking solutions exercise caution and research both the app itself and the developer before downloading any app. Once an app is installed, monitor the app's requests for permission authorizations and data activity. Beware of any applications that request permissions that do not match the advertised app functionality.***

For more information on robocall-blocking solutions, see the NTIC Cyber Center's blog post entitled, "Scam Call Solutions."

Android Clicker Trojans Distributed in Apps on Google Play Store

Researchers at antivirus firm Dr. Web discovered clicker Trojans bundled in numerous Android apps distributed on the Google Play Store. These Trojan variants, known as *Android.Click.312.origin* and *Android.Click.313.origin*, can perform functions such as clicking links, opening web pages, subscribing users to paid services, directing users to sites generating online traffic revenue, and other fraudulent activity. The malware also collects user information such as OS version, device manufacturer and model, country of residence, Internet connection type, and time zone. Clicker Trojans were found embedded in over 33 apps, collectively downloaded over 100 million times on the Google Play Store, including audio players, barcode scanners, dictionaries, and other seemingly ordinary utilities. ***The NTIC Cyber Center recommends Android users keep device operating systems up-to-date. In addition, before installing any app, exercise caution and research both the app itself and the developer. Once an app is installed, monitor the app's requests for permission authorizations and data activity. Beware of any applications that request permissions that do not match the advertised app functionality.***

New "Saefko" RAT Found For Sale on Dark Web

Researchers at Zscaler ThreatLabZ discovered a new Remote Access Trojan (RAT) called Saefko being sold on the Dark Web. This RAT launches every time a user logs into an infected machine and identifies activities involving credit cards, business, social media, gaming, cryptocurrency, and shopping by accessing a victim's Chrome browser history. Saefko then provides system information to a command-and-control (C2) server, collects screenshots, videos, and keystrokes, and can download additional malware onto infected systems. ***To protect from the dangers of RATs and other malware, the NTIC Cyber Center recommends Internet users remain vigilant for malicious emails, avoid clicking on links or opening attachments from unknown or untrusted sources, and alert IT security teams of suspicious emails. We also recommend blocking the associated Saefko Indicators of Compromise (IoCs) included in Zscaler's blog post.***

Vulnerabilities

Avaya VoIP Phones

A security researcher recently discovered two vulnerabilities affecting several models of Avaya VoIP phones. The first vulnerability, reported as a bug in an open-source software in 2009, enables an attacker to hijack affected devices and steal audio data. The second, identified in the same software in 2011, allows attackers to execute remote code on affected devices. Though these vulnerabilities have been patched in the original open-source software, the firmware of affected Avaya devices was found to be still using outdated versions of these third party software components. Vulnerable Avaya devices include Avaya 9600 series IP phones, J100 Series IP phones,

and B100 series conference phones (B189). ***The NTIC Cyber Center advises administrators of affected Avaya VoIP phone systems to update device firmware with the latest H.323 software release as soon as possible.***

Steam

A security researcher disclosed details of a zero-day vulnerability identified in the popular video gaming platform Steam. If exploited, this vulnerability allows a threat actor to leverage flaws in write access permissions for registry keys and launch executable files with elevated administrative privileges on a target system. As Steam's developer, Valve, has failed to acknowledge or release a patch for this issue, the vulnerability remains a threat to the 100+ million users of Steam and any computer installed with the program. ***The NTIC Cyber Center recommends Steam users remain vigilant for changes in system behavior and consider disabling the program until the developer issues a patch for the vulnerability.***

Multiple Software Drivers

Security researchers at Eclypsium identified numerous vulnerabilities in the software drivers of devices from over twenty well-known hardware vendors. These vulnerabilities, which affect drivers used in BIOS or the firmware of graphics cards, network adapters, hard drives, and other devices, can be exploited to disable hardware or escalate privileges on Microsoft Windows operating systems including Windows 10. Because the BIOS and drivers often load before an operating system, malware planted in vulnerable drivers may escape detection from operating system security solutions. ***To mitigate the threats posed by vulnerable device drivers, the NTIC Cyber Center encourages users and administrators of Windows systems to scan regularly for outdated system and component firmware and apply the latest device driver patches and updates as soon as they become available.***

Data Breaches and Leaks

State Farm notified affected customers of a data breach that compromised select usernames and passwords of State Farm online accounts. The company believes the breach occurred as a result of a credential stuffing attack, in which threat actors used combinations of usernames and passwords leaked in previous data breaches to gain access to accounts of customers who had reused the same credentials elsewhere online. Though State Farm has not identified any indications of fraudulent

activity perpetrated as a result this attack, the company nevertheless has changed affected account passwords to prevent further compromise or abuse and implemented additional controls to mitigate future attacks. ***The NTIC Cyber Center encourages the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication on any account that offers it to avoid falling victim to credential compromise.***

For more information on credential stuffing attacks, please reference the NTIC Cyber Center's product entitled** Credential Stuffing Attacks – A Growing Yet Easily Mitigated Threat**.

Upcoming Webinars

Hard Truths about Account Takeover and Strategies to Defend Your Enterprise

Protecting your enterprise from breaches and account takeovers has never been a bigger challenge. New tools make it possible for even unsophisticated actors to perform advanced, widespread attacks that put your organization at risk. According to the 2019 Verizon Breach Report, stolen credentials are the leading attack vector - yet in a recent study by Symantec, only 7 percent of respondents rated account takeover as a top threat to their cloud infrastructure.

Regardless of the thoughtful measures and policies you have in place, the hard truth is that no policy can protect you from human behavior. In this webinar, SpyCloud Head of Product Strategy Chip Witt will demonstrate how malicious actors take advantage of loopholes in your account takeover prevention plans. For example, your employees may be reusing compromised passwords to access corporate systems or signing up for third-party services like LinkedIn or Fantasy Football using their work credentials.

Register for this webinar to learn about:

- The anatomy of an account takeover attack
- Real-world examples of how employee password reuse can threaten your enterprise
- Potential holes in your account takeover plan
- What you can do to strengthen your security posture, including alignment to the National Institute of Standards and Technology (NIST)

To register for this free webinar on Thursday, August 29 at 11:30 AM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Like-farming, also known as like-harvesting, is a social engineering technique that fraudsters employ to increase online engagement and boost the popularity of social media posts and pages. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Critical US Election Systems Have Been Left Exposed Online Despite Official Denials

Analytic Comment: After conducting interviews with multiple cybersecurity experts, reporters from Vice News believe that election systems in several counties and states were left exposed to the Internet, in some cases for longer than a year. Since third-party vendors are often responsible for maintaining oversight of election systems, officials may not have been aware that these systems were left exposed and at risk of serious damage or manipulation. This article highlights the fact that, although election systems are theoretically secure, errors in configuration protocols can render their security features all but irrelevant.

Emergency Declarations Improve Cyberattack Recovery, Report Says

Analytic Comment: An analytical report from Moody's Investors Service concludes that, during a state-targeted cyber attack, a statewide emergency declaration increases the likelihood of recovery and reduces the risk of lasting and damaging effects. According to the report, last month's decision from Louisiana Governor John Bel Edwards to declare a state of emergency in the wake of ransomware attacks in several school districts minimized the attack's negative impacts and exemplified best practices. The declaration allowed the National Guard, the Louisiana State Police, Louisiana's Office of Technology Services, and Louisiana State University to coordinate response efforts, to quickly recover backup data and prevent the lowering of the state's credit score. The

report's findings underscore the importance of proper preparation for cyber incident response and the need for governments across the country to clarify procedures and policies related to emergencies stemming from cyber attacks.

Hackers Can Use Netflix Account to Steal Banking Info

Analytic Comment: A security analyst presenting at this year's DEFCON conference detailed how simply having a Netflix account may put a customer at risk of banking or identity theft. In her talk, the analyst discussed a cyber threat tactic by which attackers could use their knowledge of regularly scheduled payment transactions, such as those charged by online subscription services, to verify recent transactions with a bank's customer service department. Since this information is frequently requested by numerous financial institutions to verify bank account ownership, attackers could use this technique to spoof account ownership and gain access to victims' banking accounts. Social media users who openly reveal information about subscriptions to online services may be among the most vulnerable to this kind of manipulation. Ultimately, this attack vector highlights the need for individuals to maintain awareness of their own privacy, to avoid oversharing on social media platforms, and regularly review account privacy settings to limit the exposure of sensitive or personal information.

Patches and Updates

Adobe Releases Security Updates for Multiple Products

Cisco Releases Security Updates for Multiple Products

Google Releases Security Updates for Chrome

Intel Releases Security Updates

Microsoft Releases August 2019 Security Updates

Microsoft Releases Security Updates to Address Remote Code Execution Vulnerabilities

Multiple HTTP/2 Implementation Vulnerabilities

ICS-CERT Advisories

Delta Industrial Automation DOPSoft

Mitsubishi Electric smartRTU and INEA ME-RTU

OSIsoft PI Web API

Siemens SCALANCE X Switches

Siemens SIMATIC PCS7, WinCC, TIA Portal (Update B)

Siemens SIMATIC WinCC and PCS7 (Update A)

Siemens SIPROTEC 5 and DIGSI 5 (Update A)

Siemens Spectrum Power (Update A)

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Email your name, job title, organization, phone number, and preferred email address to NTICCyberCenter@dc.gov and we will add you to our distribution list.

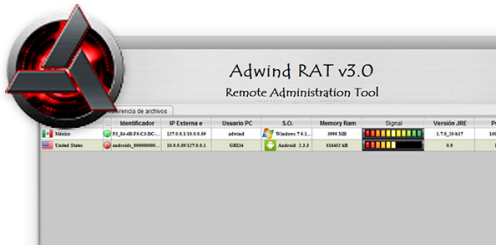
NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

August 22, 2019

National Capital Region Cyber Threat Spotlight



Adwind RAT Targeting Utility Sector

According to researchers at cybersecurity firm Cofense, cyber threat actors are actively targeting utility sector organizations with malicious spam (malspam) campaigns that distribute the Adwind Remote Access Trojan (RAT). Adwind is capable of performing a variety of malicious tasks on infected machines, including logging keystrokes, stealing browser credentials and VPN certificates, accessing webcams and microphones, and mining for cryptocurrency. Researchers indicate that the most common initial attack vector has been spam emails containing infected attachments or links that direct victims to a malicious payload. ***The NTIC Cyber Center recommends users remain vigilant for malspam campaigns, avoid opening and unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. We also recommend administrators reference and block the associated Indicators of Compromise (IoCs) contained in Cofense's report.***

Announcement

Call for Presentations

In preparation for our upcoming one-day cybersecurity-focused conference that will take place in Washington, DC during DC Cyber Week this October, the NTIC Cyber Center is now accepting presentation proposals. The goal of this conference is to educate our stakeholders within the National Capital Region about the latest cyber threats impacting their sectors and provide actionable intelligence they can use to protect themselves and their organizations.

Proposal guidelines:

- Topics should focus on current and emerging cyber threats and highlight best practices and lessons learned.
- As this conference will be open to the public, information included within presentations must be at the unclassified level.
- Presentations should be no longer than one hour and include an opportunity for a question and answer session with the audience.
- We welcome speakers from both the public and private sectors, provided the information contained within presentations can apply to a broad audience. No financial compensation will be provided to any speaker and presentations cannot be used to promote commercial products or services.
- PowerPoint slides must be submitted to the NTIC Cyber Center two weeks prior to the conference date for content review.

If you are interested in submitting a presentation proposal, please email us at NTICCyberCenter@dc.gov. The call for presentations will close on **Friday, September 20, 2019 at 5:00PM**. After this deadline, we will review all submitted proposals and notify those selected via email.
General attendee registration will open in the next few weeks. Please keep checking www.ncrintel.org/cyber for updates.

Current and Emerging Cyber Threats

Lateral Phishing Attacks a Dangerous and Growing Threat

Researchers at UC Berkeley, UC San Diego and security firm Barracuda analyzed the tactics and outcomes of 180 lateral phishing attacks, attacks that target victims using a compromised email

account from within their own organization. In the majority of attacks, threat actors disguised correspondence as notifications for shared documents or account issues in efforts to forward victims to fraudulent login pages. Attackers also deleted emails sent and received in order to avoid detection by the compromised account's owner. Researchers warn of the dangers of the growing threat of lateral phishing campaigns, not only for enterprise users, but for personal email account users as well. ***The NTIC Cyber Center encourages the use of multifactor authentication on any account that offers it and advises email users to avoid opening unexpected emails. If you believe you have been targeted in a lateral phishing campaign, notify your organization's IT security team immediately.***

Phishing Campaign Using Google Drive Notification Emails Identified

Security researchers at Cofense identified a phishing campaign targeting an organization in the energy sector with legitimate Google Drive notification emails containing links to phishing sites. These emails spoof correspondence from CEOs, complete with convincing company names and logos, and urge recipients to open a link to a fraudulent login page that prompts for user credentials. The use of a legitimate business service such as Google Drive allows threat actors to bypass email security filters and ensure malicious emails reach end users. ***The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as alerts from Google Drive and avoid opening unexpected emails. We also recommend referencing and blocking the associated Indicators of Compromise (IoCs) included in Cofense's blog post.***

Adware Found in 85 Gaming and Photography Android Apps

Security researchers at Trend Micro identified adware known as AndroidOS_Hidenad.HRXH in at least 85 gaming and photography apps available on the Google Play Store. These malicious apps, which were collectively downloaded over eight million times, allow threat actors to distribute full screen ads, alter ad frequency, and disable the skipping of ads on infected devices. AndroidOS_Hidenad.HRXH uses time stamps, network time, and java reflection to avoid detection techniques and maintain persistence. Trend Micro has alerted their findings to Google, who has removed the adware-laced apps from the Google Play Store. ***The NTIC Cyber Center recommends Android users exercise caution before installing any app and to pay close attention to required permission settings. If the permissions required do not match the advertised functionality of the app, do not install it. After installing any new app, monitor the device for unusual behavior such as excessive power consumption, excessive data usage, unexpected pop-ups, and uninstall problematic apps immediately, performing a factory reset of the device if necessary.***

Malicious Apple Lightning Cable Allows for Remote Takeover

A security researcher known as MG created and sold malicious Apple lightning cables that grant attackers unauthorized remote access into any Mac computer into which the cable is connected. The malicious cable, dubbed the "O.MG Cable," appears legitimate but has been modified to include components that can allow an attacker to use various payloads, scripts, and commands to wirelessly take control of a targeted computer from up to 300 feet away. The cable's creator marketed this item for $200 during the latest DEFCON conference, where he completely sold out of available inventory. ***The NTIC Cyber Center cautions users and administrators to beware of malicious Apple lightning charging cables or other third-party accessories and to avoid connecting unapproved, untrusted, or unauthenticated cables or devices into USB ports.***

Vulnerabilities

Lenovo ThinkPad Laptops

Lenovo warns of three vulnerabilities, one which remains unpatched, affecting the company's ThinkPad model laptops. A high-severity vulnerability, identified as CVE-2019-9506 and included in Microsoft's August Patch Tuesday, affects Bluetooth systems and allows attackers to perform information-disclosure or escalation-of-privileges attacks. Another vulnerability, rated as medium-severity and identified as CVE-2019-6171, is a Lenovo-specific bug that affects numerous ThinkPad laptops sold from 2015-2016 (see bulletin for list of affected devices). This bug, which remains unpatched, allows attackers to gain elevated access to computer resources or data and take control of a targeted system. A third vulnerability, low-severity CVE-2019-0128, exists in the Intel chipset device software and may allow escalation-of-privilege. ***The NTIC Cyber Center advises users and administrators of ThinkPad devices to review the vulnerability bulletins and to implement patches and updates immediately or as soon as they become available.***

Data Breaches and Leaks

Comparitech researchers discovered an unsecured MongoDB database belonging to the hotel franchise Choice Hotels that contained approximately 5.6 million records of customer information.

In the database, researchers identified a ransom note demanding approximately $4,000 in exchange for the return of 700,000 customer records believed to have been accessed and stolen by hackers. Data compromised in this breach includes the full names, addresses, email addresses, and phone numbers of guests of Choice Hotel establishments possibly including Ascend, Cambria, Clarion, Comfort, EconoLodge, MainStay Suites, Rodeway Inn, Sleep Inn, Suburban, Quality Inn, and Woodspring Suites. ***The NTIC Cyber Center recommends customers of Choice Hotels remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

A security researcher identified an exposed database owned by movie ticket subscription service MoviePass containing 161 million records of customer data. Within these records, researchers identified 58,000 customer payment records including MoviePass debit card numbers, used to make movie purchases at cinemas, and customer personal credit card details, including card numbers, expiration dates, names, and addresses. In addition to exposing payment records, the database also featured customer username and password combinations recorded during failed login attempts. ***The NTIC Cyber Center recommends MoviePass customers monitor their account statements, immediately notify their financial institutions of any unauthorized or suspicious activity, and remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

Upcoming Webinars

Data Breach®
Prevention. Response. Notification. TODAY

Insider Threat Program Realities - New Research Findings

Join Enterprise Strategy Group (ESG) and Dtex Systems to get a detailed look at a newly released ESG Research Insights Report, "Insider Threat Program Realities." Based on the survey of 300 security and IT professionals in the US, the report underscores the continued struggle most organizations face when it comes to defending against insider threats. Despite exponential increases in the number of insider-related incidents and mindshare dedicated to insider risks, 62 percent of respondents say that insider threat detection has become more difficult in the last two years.

Come take and in-depth look at the survey findings and explore the factors responsible for the growing number of complexities, as well as receive guidance on how to effectively manage all types of insider threats.

Topics will include:

- Current challenges with insider threat detection, largely due to outdated solutions, immature programs, and insufficient investments
- The need for a strong data foundation with a focus on quality, not quantity, of data
- How to identify data-driven, purpose-built solutions capable of pinpointing modern insider threats

To register for this free webinar on Tuesday, August 27 at 1:30 PM EDT, click here.

Data Breach Today
Prevention. Response. Notification.

Top Social and Digital Threats Facing Financial Institutions

The threats facing financial institutions are not new: from data breaches and information leakage, spearphishing and customer scams, to financial fraud, bad actors are set on stealing your revenue, damaging your brand, and weakening your customer trust. But as we expand avenues for engagement, the attack surfaces have changed. Bad actors now rely on social media to impersonate your brand and top executives in order to gain access to your information and customers. Cyberattackers use dark web forums to plan attacks and share vulnerabilities. Early warning and visibility into the networks that these actors use to conduct attacks is critical.

In this webinar, ZeroFOX's Chief Security Officer, Dr. Sam Small, will be joined by another financial services expert to discuss the top digital threats facing their organizations, tactics they've seen used most often on social and digital platforms to target their customers, employees and brand, and steps organizations can take to protect themselves against these risks. Sam will present the latest ZeroFOX Threat Research on the top digital threats the ZeroFOX Alpha Team has identified within the financial services industry.

Register for this live webinar to:

- Understand the modern digital threat landscape and where bad actors live, such as deep and dark web forums, code sharing sites and social media sites
- Gain knowledge of the top digital risks facing the financial industry and the tactics bad actors use to conduct attacks on your organization and customers

- Hear directly from financial services experts on the top digital threats facing financial organizations and how to effectively and proactively address them

To register for this free webinar on Thursday, September 12 at 11:30 AM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

A ***car wrapping scam*** is a type of bogus check scheme in which perpetrators target people seeking to place advertisements or company logos on their personal vehicles to earn money. These scammers often use fraudulent online job postings or spam email to promote their illicit money-making schemes, which offer to pay drivers to cover their vehicles with graphics printed on sheets of vinyl, a process known as car wrapping. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

3,813 Breaches Were Reported Through June 30, Exposing Over 4.1 Billion Records
Analytic Comment: According to Risk Based Security's 2019 Data Breach Report, data breaches continue to occur at an alarming rate. In the first half of 2019 alone, 3,813 data breaches exposed over 4.1 billion records globally, representing an increase of 54 percent in the number of breaches and 52 percent in the number of records exposed compared to reports from the first half of 2018. Unauthorized third-party access to systems and services remains the predominant cause of data breaches, with phishing attacks identified as the most common first step in gaining access. The proliferation of breaches and exposed records highlights the need for organizations to implement preventative measures to mitigate against the ongoing threat of data theft and loss.

Cleaning Up After Ransomware Attacks Isn't Easy

Analytic Comment: Recent profiles of ransomware attacks affecting two healthcare organizations illustrate the challenges associated with ransomware response and recovery efforts. One organization faced losses of electronic medical records while another suffered disruptions to business operations including patient appointment scheduling systems. Inaccessibility of systems can make treating patients and collecting payments extremely difficult, requiring data to be documented manually until systems are back up and running. Difficulties associated with restoration efforts underscore the importance of taking critical steps, including patching systems and performing frequent backups, to prevent falling victim to a ransomware attack.

Patches and Updates

Kubernetes

Microsoft Remote Desktop for Android

ICS-CERT Advisories

Fuji Electric Alpha5 Smart Loader

Johnson Controls Metasys

Siemens SCALANCE Products

Siemens SINAMICS

Zebra Industrial Printers

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

August 29, 2019

National Capital Region Cyber Threat Spotlight

Ostap Malware Campaign Serves Up Trickbot and Ransomware

First discovered in 2016, Ostap is a JavaScript loader designed to deliver banking Trojans such as Dridex, Tinba, and Ursnif, as well as point-of-sale (PoS) malware on infected machines. More recently, however, researchers observed Ostap delivering Trickbot, a modular banking Trojan that often acts as a dropper for other malware such as ransomware. Ostap is a sophisticated malware variant that is capable of detecting antivirus software, network monitoring applications, and virtual environments to prevent analysis. It also replaces targeted documents on a system with custom JavaScript files if the final payload fails to download, each displaying the file extension *.jse*. Ostap is primarily distributed via malicious email attachments and disguised as invoices to prompt victims to open them and execute the malware. It then uses JavaScript to download the final payload to the system. ***The NTIC Cyber Center recommends all network administrators review Esentire's and Trend Micro's reports on Ostap and proactively block the associated indicators of compromise (IoCs).***

Federal Partner Announcements

IRS Warns of New Email Scam

The Internal Revenue Service (IRS) has issued a warning about a new email scam in which malicious cyber actors send unsolicited emails to taxpayers from fake (i.e., spoofed) IRS email addresses. The emails contain a link to a spoofed IRS.gov website that displays fake details about the targeted recipient's tax refund, return, or account. The emails instruct the recipient to access their refund information by entering a provided password on the spoofed website. By entering the password, the victim unintentionally downloads malware that could enable the malicious cyber actors to take control of the affected system or obtain sensitive information. The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review the IRS news release and the CISA Tip on Avoiding Social Engineering and Phishing Attacks for more information.

For additional information on tax-related scams, please reference the NTIC Cyber Center's blog post titled Securing Our Communities: IRS Tax Scams.

FISMA Annual Report to Congress

The Office of Management and Budget (OMB) has published its Fiscal Year (FY) 2018 Annual Report to Congress on the implementation of the Federal Information Security Modernization Act of 2014 (FISMA). The document includes data reported by agencies to OMB and the Cybersecurity and Infrastructure Security Agency (CISA). The report highlights government-wide cybersecurity programs and initiatives, and agencies' progress to enhance federal cybersecurity over the past year and into the future. Notably, in FY 2018, agencies reported 31,107 incidents, a 12 percent decrease from FY 2017.

CISA encourages organizations to review the Fiscal Year 2018 Annual Report for more information.

Current and Emerging Cyber Threats

Phishing Campaign Targets Instagram Users

A new phishing campaign attempts to convince Instagram account holders to click on malicious links paired with fraudulent two-factor authentication (2FA) codes to gain unauthorized access to their accounts. Threat actors send spoofed Instagram messages to victims that contain a sign-in link and a decoy 2FA code urging them to sign in as soon as possible. When clicked, the link leads to a fraudulent Instagram login page with a .CF top-level domain with a valid HTTPS certificate and

green padlock to give credence to the scheme. ***The NTIC Cyber Center recommends never using a link contained in an email to visit and sign into an online account and to enable 2FA on every account that offers it. Users who suspect that their accounts have been compromised may regain access by filing a report with Instagram.***

Web Services Dynamic Discovery Protocol Abused in DDoS Attacks

Security researchers discovered a new distributed denial-of-service (DDoS) attack vector performed by abusing the Web Services Dynamic Discovery (WS-DD, WSD, or WS-Discovery) protocol, which is used for communication and inter-device discovery. WS-DD can "discover" other neighboring devices that use a specific standard to communicate using the Simple Object Access Protocol (SOAP) messaging format over the User Datagram Protocol (UDP) transport protocol. Due to the nature of UDP, threat actors may spoof destination packets. Additionally, WS-DD's output is much larger than its input, threat actors with few resources can launch larger scale attacks towards target devices. WS-DD can be found in devices such as printers, Internet Protocol (IP) cameras, digital video recorders (DVRs) and “smart” home appliances. One security researcher identified a WS-DD DDoS campaign that consisted of 130 attacks, some of which reached over 350 gigabits per second (Gbps). ***The NTIC Cyber Center recommends network administrators proactively block TCP port 3702 at the network perimeter.***

Vulnerabilities

Pulse Connect Secure VPN Software

Security researchers observed automated scanning activity targeting Pulse Secure “Pulse Connect Secure” virtual private network (VPN) servers vulnerable to CVE-2019-11510, an arbitrary file-reading vulnerability. Researchers believe threat actors are actively exploiting this vulnerability to download files, read usernames and passwords associated with VPN servers, and launch further attacks to gain access inside private networks. According to researchers, approximately 14,500 hosts worldwide are currently running vulnerable Pulse Connect Secure software, with roughly 5,000 of the hosts existing in the US including organizations such as US military organizations, federal, state, and local government agencies, public universities and schools, hospitals and health care providers, electric and gas utilities, major financial institutions, and numerous Fortune 500 companies. ***The NTIC Cyber Center encourages administrators of Pulse Secure VPN systems to immediately ensure that installed versions of “Pulse Connect Secure” server software are not vulnerable to CVE-2019-11510 and, if necessary, to reference Pulse Secure’s guidance on updating to fixed versions.***

Lenovo Solution Center

Researchers at Pen Test Partners discovered a privilege escalation vulnerability in the Lenovo Solution Center (LSC), a diagnostic software that is preinstalled on most Lenovo computers. This vulnerability, CVE-2019-6177, allows threat actors to execute arbitrary code and escalate privileges via a discretionary access control list overwrite. It affects LSC version 03.12.003, which is no longer supported by Lenovo. ***The NTIC Cyber Center recommends keeping all software, including operating systems, patched and up-to-date, and decommissioning any unsupported or end-of-life (EOL) systems and software. Lenovo recommends that affected customers replace LSC with Lenovo Vantage or Lenovo Diagnostics software as soon as possible.***

Data Breaches and Leaks

HOSTINGER

Web hosting provider Hostinger announced a breach of information belonging to 14 million customers. According to the company, an unauthorized third party accessed a server containing client data and obtained information including usernames, hashed passwords, emails, first names, and IP addresses. Hostinger implemented a mandatory password reset for all affected customers and urges customers to choose new passwords that are strong and unique to that website. ***The NTIC Cyber Center recommends Hostinger customers remain vigilant for an increase in phishing attempts perpetrated through email, social media, or other avenues as a result of this data exposure.***

imperva

Application security firm Imperva disclosed a breach that affected their Cloud Web Application Firewall (WAF) product, previously known as Incapsula. The breach affected Incapsula customers who had accounts through September 15, 2017 and resulted in the compromise of email addresses, hashed and salted passwords, API keys, and customer-provided SSL certificates. As the incident is still under investigation, it is currently unknown how the breach occurred or what threat actors were involved. As a result, Imperva implemented forced password resets for customer accounts, consulted forensics experts, and activated internal security response teams. ***The NTIC Cyber Center***

encourages affected Imperva WAF users to change their passwords, enable multifactor authentication, reset API keys, and generate new SSL certificates.

Upcoming Webinars

Data Breach Today
Prevention. Response. Notification.

See and Protect Users and Endpoints Everywhere

Users have adopted the cloud, changing the way we work - has your security kept up?

Security gaps are widening more than ever as more users work remotely, more unmanaged devices connect to the network, and more threats evolve to take advantage of these vulnerabilities.

To keep your users safe, you need deep visibility into endpoints, apps, files, and locations. With this visibility, you can stop malicious behavior before an attack compromises your entire network.

To register for this free webinar on Tuesday, September 17 at 2:00 PM EDT, click here.

Data Breach Today
Prevention. Response. Notification.

Hacking Your Organization: 7 Steps Bad Guys Use to Take Total Control of Your Network

The scary fact is that human error is a contributing factor in more than 90% of breaches. With so many technical controls in place hackers are still getting through to your end users, making them your last line of defense. How are they so easily manipulated into giving the bad guys what they want? Well, hackers are crafty. And the best way to beat them is to understand the way they work.

In this webinar Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, will take you through the "Cyber Kill Chain" in detail to show you how a single email slip up can lead to the total takeover of your network.

Roger will show you:

- How detailed data is harvested using public databases and surprising techniques
- Tricks used to craft a compelling social engineering attack that your users WILL click
- Cunning ways hackers deliver malicious code to take control of an endpoint
- Taking over your domain controller and subsequently your entire network

But not all hope is lost. Roger will also share actionable strategies you can put in place now to greatly reduce your risk. Find out how to protect your organization before it's too late.

To register for this free webinar on Tuesday, September 10 at 11:30 AM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

A **romance scam**, also known as a sweetheart scam or confidence fraud, is a social engineering scheme where a perpetrator masquerades as a potential love interest, concealing his or her true intentions to elicit money or material possessions from unsuspecting victims looking for love online. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Texas Attacks Must Inform Other States as Ransomware 'Only Getting Worse,' Says Krebs
Analytic Comment: The US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released a new Strategic Intent document that outlines key principles, overall goals, and operational priorities for the agency. In this document, CISA Director Chris Krebs stresses the overall mission to "defend today, secure tomorrow" to strengthen the nation's resiliency against cyber threats. While unveiling the document, Director Krebs also commented on the recent ransomware attacks that targeted twenty-two Texas municipalities, discouraging affected organizations from paying the ransom and cautioning that more coordinated attacks and bigger payouts may only make the problem of ransomware worse. CISA's Strategic Intent should assist partner organizations in defining priorities and developing long-term strategic plans to defend against cyber attacks.

CISOs Believe Capabilities of Attackers are Outpacing Their Ability to Defend Their Organizations

Analytic Comment: Results of a recent survey conducted by cybersecurity firm Fortinet indicate that 84 percent of CISOs believe that cyber-attack risks will increase. A quarter of the respondents also believe threat actors' capabilities are surpassing available defenses. Respondents attribute these deficiencies to budget and talent limitations as well as the ever-expanding threat attack surface. This survey demonstrates the need for organizations to obtain solutions that are more cost-effective or increase budgets to accommodate the inevitable evolution of the cyber threat landscape

---

Patches and Updates

Apple Releases Multiple Security Updates

Google Releases Security Updates for Chrome

ICS-CERT Advisories

Datalogic AV7000 Linear Barcode Scanner

Delta Controls enteliBUS Controllers

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

September 5, 2019

National Capital Region Cyber Threat Spotlight

Revenge and Orcus Remote Access Trojans Target Government and Financial Organizations

Researchers at Cisco's Talos Security Intelligence and Research Group discovered threat actors using Revenge and Orcus Remote Access Trojans (RATs) in global malware distribution campaigns targeting sectors such as government, finance, and information technology. Orcus and Revenge combined can allow threat actors to commit a range of malicious activity including, but not limited to: opening remote shells, logging keystrokes, accessing webcams, extracting victims' passwords, and loading custom plugins. Payloads are delivered through spoofed emails containing malicious attachments or links. Threat actors obfuscate their command and control (C2) infrastructure using the Dynamic Domain Name System (DDNS). ***The NTIC Cyber Center recommends users remain vigilant for Orcus and Revenge RAT campaigns, avoid opening and unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. We also recommend that network administrators block the associated Revenge and Orcus indicators of compromise (IoCs) included in the Cisco Talos report titled RAT Ratatouille: Backdooring PCs with Leaked RATs.***

Federal Partner Announcements

September is National Preparedness Month: Be Prepared, Not Scared

National Preparedness Month (NPM) promotes family and community disaster and emergency planning. This year's theme is "Prepared, Not Scared."

Although most people understand that being prepared is essential to getting through an emergency such as a natural disaster, there is less awareness about the necessity of cybersecurity preparedness. Cybersecurity preparedness is often a deciding factor on how much of an impact a cyber-related event—such as a ransomware infection, identify theft, or data breach—has on an individual or an organization.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages individuals and organizations to develop their own cyber emergency response plans that include guidance on protections and controls such as keeping software and operating systems updated, regularly backing up files, keeping encrypted copies of important documents offline, and routinely running anti-virus scans.

Learn more about National Preparedness Month at Ready.gov/September and see Ready.gov/Cybersecurity and the following CISA Tips for resources on preparing for, and responding to, unexpected cyber-related events:

- Protecting Against Ransomware
- Preventing and Responding to Identity Theft
- Handling Destructive Malware
- Protecting Against Malicious Code

Cyber Safety for Students

As summer break ends, many students will return to school with mobile devices such as smart phones, tablets, and laptops. Although these devices can help students complete schoolwork and stay in touch with family and friends, there are risks associated with using them. However, there are simple steps that can help students stay safe while using their internet-connected devices.

The Cybersecurity and Infrastructure Security Agency (CISA) recommends reviewing the following resources for more information on cyber safety for students:

- Stop.Think.Connect. Toolkit
- Stay Safe Online
- Before You Connect a New Computer to the Internet
- Keeping Children Safe Online
- Rethink Cyber Safety Rules and the "Tech Talk" with Your Teens
- Concerned Parent's Internet Safety Toolbox

Current and Emerging Cyber Threats

Trickbot Targets US Mobile Carrier Customers

Researchers at Secureworks Counter Threat Unit (CTU) discovered a new Trickbot variant targeting US mobile carrier users' data from Verizon, T-Mobile, and Sprint. When users reach out to legitimate websites from a Trickbot-compromised system, Trickbot will intercept the traffic and proxy it via its C2 server. The C2 server embeds malicious HTML and JavaScripts on a compromised webpage that requests a PIN code in addition to the user ID and password. CTU believes that this variant is orchestrated by threat actors known as the Gold Blackburn and that requesting a PIN code is likely used to conduct SIM-swapping attacks. ***The NTIC Cyber Center recommends network administrators review the Secureworks report and block the associated IoCs. We also recommend mobile carrier customers refrain from inputting account PIN codes into online forms or sharing them via text messages or email. Account PIN codes should only be shared with official mobile carrier representatives who need to verify the identity of an account holder and only when the call to the mobile carrier is initiated by the customer.***

Magecart Attacks Impact More Than 80 Ecommerce Stores

Security researchers at Arxan discovered a Magecart payment-skimming campaign stealing customer personal and financial information from over 80 breached ecommerce stores. These stores, comprised of motorsports, luxury apparel, and other websites, were found to be operating outdated versions of the Magento ecommerce platform known to be vulnerable to numerous published exploits. These vulnerabilities allowed Magecart groups to perform attacks such as arbitrary file upload, remote code execution, and cross-site request forgery to compromise websites and steal customer data such as names, billing addresses, email addresses, phone numbers, credit card details, usernames, and passwords. The researchers also indicate that the breached sites lacked security features such as tamper detection and code obfuscation which, if implemented, may have alerted administrators of malicious activity or deterred attackers from compromising the websites. Magecart attacks have resulted in the theft of payment card details and personal information of millions of victims to date and they continue to pose significant risks to websites that are not configured with

effective security controls.

The NTIC Cyber Center recommends website visitors remain vigilant for indications that a webpage may be compromised. These may include being asked twice to enter payment or login information or being prompted for payment card details before being forwarded to a secure payment service provider. Customers making purchases on ecommerce platforms should routinely monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity. In addition, the NTIC Cyber Center recommends ecommerce website administrators regularly test web applications for vulnerabilities, implement file integrity monitoring or change-detection software, perform periodic penetration testing to identify weaknesses, and keep anti-malware solutions and security patches up to date. Administrators of ecommerce platforms built on Magento Community Edition should ensure that all websites are running the latest version of the software, version 2.1.7.

To read more about the threat of Magecart attacks and for additional mitigation strategies, please see our recent Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Heatstroke Uses Multi-Stage Phishing Attack and Steganography to Steal Information from Victims

A new phishing campaign known as Heatstroke uses a multi-stage attack to target victims. Threat actors utilizing Heatstroke target the victim's private email address by compromising legitimate websites and using them to generate dynamic phishing pages in which content displayed may vary based on visitor properties. The use of legitimate domains and constantly changing landing pages helps the phishing emails to bypass email security filters and reach end users. Stolen credentials are then sent to the threat actors using steganography, a technique used to hide information within images. ***The NTIC Cyber Center recommends users remain vigilant for Heatstroke campaigns, avoid opening and unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. We also recommend blocking the associated Heatstroke IoCs included in Trend Micro's report titled "Heatstroke" Campaign Uses Multistage Phishing Attack to Steal PayPal and Credit Card Information.***

Multiple Malicious Android Applications Discovered in Google Play Store

Security researchers have discovered multiple malicious Android apps available in the Google Play Store that perform click fraud, deliver additional malware, and extort money from victims by subscribing them to premium paid SMS services. In a report released by cybersecurity firm Symantec, two malicious apps that have been downloaded over 1.5 million times masquerade as both a fitness app (Beauty Fitness: daily workout, best HIIT coach) and a notepad app (Idea Note:

OCR Text Scanner, GTD, Color Notes). When installed, these apps secretly click ads that run in the background, generating fraudulent revenue for the threat actors behind the campaign. In a separate report by CSIS Security Group, 24 malicious Android apps were discovered harboring a Trojan dubbed "the Joker." These apps, which have been downloaded over 472,000 times from the Google Play Store, masquerade as photo viewers and editors, facial scanners, device wallpaper, and virtual private networks. After installation, however, the embedded Trojan delivers a second-stage malware that performs as click fraud and steals victims' contact lists and SMS messages. It also sends SMS messages from the infected device to premium phone numbers, racking up expensive charges on the victim's phone bill. Although Google has been working to remove the offending apps from its Play Store, malicious mobile apps remain a threat to Android users as profit-motivated criminals continue to circumvent the Google Play Store's app review process to deliver malware to victims. ***The NTIC Cyber Center recommends Android users install and use Google Play Protect, an official Android tool that scans apps for malware prior to download. After installing any new app, monitor the device for unusual behavior such as excessive power consumption, excessive data usage, unexpected pop-ups, and uninstall problematic apps immediately, performing a factory reset of the device if necessary. If the device permissions required by an app do not match the advertised functionality, refrain from installing it. Lastly, we recommend all Android users update their devices to the latest OS - Android 10 - as soon as possible.***

Data Breaches and Leaks

Software provider Foxit, developer of PhantomPDF editor and Foxit Reader PDF products, announced a breach of user account data. According to the company's security notification, third parties gained access to information including customer names, email addresses, passwords, phone numbers, company names, and IP addresses, though payment information is not believed to have been accessed. Foxit has disabled account passwords for affected users and will require users to reset passwords upon login to restore account access. ***The NTIC Cyber Center recommends that users of Foxit software products enable multifactor authentication on any account that offers it, monitor their accounts for suspicious activity, and remain vigilant for an increase in phishing***

attempts perpetrated through email, social media, telephone, text message, or other avenues as a result of this data exposure.

Upcoming Webinars

Data Breach Today
Prevention. Response. Notification.

Building Effective Zero Trust Kill Chains Using Data-Centric Analytics

Taking a Zero Trust approach that emphasizes users and data offers a significant opportunity to modernize security and traditional kill chain models. While many of today's models leverage data detected on endpoints, they lack the critical context of how users are interacting with data and sensitive applications in the cloud and from devices lurking in blind spots from traditional controls.

To establish more inclusive Zero Trust kill chains that pinpoint troublesome data handling - in direct relation to business objectives - today's security practitioners require the ability to inject context from data protection tools, including cloud access security brokers and data loss prevention solutions, deeper into the process. Integrated analytics that combine and analyze these data sources hold the key to increased effectiveness.

Register for this webinar to learn how to:

- Provide more robust data protection, married with targeted threat prevention
- Pinpoint users and systems that pose the greatest risks, related to exfiltration
- Highlight key differentiators between internal and external threats
- Tie business-driven data protection priorities directly to incident response

To register for this free webinar on Thursday, September 19 at 11:30 AM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Disaster scams are a type of social engineering scheme in which perpetrators target and defraud victims of natural disasters, severe weather events, or other catastrophic occurrences. These scams attempt to further victimize those struggling to recover from incidents such as floods, hurricanes, wildfires, and tornadoes, although scammers are known to exploit victims in the wake of nearly any emergency situation. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Innovation on the Dark Web: How Bad Actors Are Keeping Pace

Analytic Comment: In the wake of global law enforcement operations to dismantle major dark web marketplaces, cyber criminals are shifting their operations to adapt to the current state of the dark web. In place of selling through marketplaces, criminals are selling directly to trusted buyers, cultivating a client base through new dark web forums such as Dread. Those who still use marketplaces have configured new platforms with additional security features to prevent scams and ensure greater anonymity for sellers and buyers. Criminals have also employed new tools and techniques such as specialized account-checkers to launch targeted credential stuffing attacks, multi-factor authentication bypassing methods to reset passwords, and SIM-swapping attacks to steal messages and data from mobile users. Because these tactics are also offered as "dark web weapons-as-a-service," inexperienced criminals have few barriers to entry into the emerging avenues of dark web cybercrime.

Multifactor Authentication Blocks 99.9 Percent of Automated Cyber Attacks

Analytic Comment: A recent Microsoft report concludes that multifactor authentication (MFA) methods block 99.9 percent of nearly all automated cyber attacks on online services and websites. However, attacks against systems not secured with MFA are frequently successful, with the reuse of login credentials across personal and work accounts contributing to the high success rate of unauthorized third-party access to these systems. These findings underscore the need to shift from reliance on password rules for securing account access toward implementing tools such as MFA to enable stronger authentication on all online services and websites.

Patches and Updates

Cisco Releases Security Updates for Multiple Products

Mozilla Releases Security Updates for Firefox and Firefox ESR

Samba Releases Security Updates

Supermicro Releases Security Updates

ICS-CERT Advisories

Change Healthcare McKesson and Horizon Cardiology

EZAutomation EZ PLC Editor

EZAutomation EZ Touch Editor

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

September 12, 2019

National Capital Region Cyber Threat Spotlight

BlueKeep Exploit Weaponized in Metasploit Penetration Testing Tool

Cybersecurity firm, Rapid7, published a BlueKeep exploit module for their Metasploit penetration testing platform. Bluekeep (CVE-2019-0708) is a vulnerability discovered in Microsoft Windows Remote Desktop Protocol that, if exploited, allows for the unauthorized execution of arbitrary code on a remote system. The Rapid7 exploit module can perform code execution unlike other proof-of-concept Bluekeep exploits posted online. While there are 700,000 reported systems currently vulnerable to BlueKeep, this module only affects the 64-bit version of Windows 2008 R2 and Windows 7. Additionally, the Rapid7 exploit module cannot be automated as it only works in "manual" mode and requires direct user input for proper execution. Microsoft released patches to address the BlueKeep vulnerability on May 14, 2019. ***The NTIC Cyber Center recommends network administrators who have not yet patched systems to protect them against the BlueKeep vulnerability do so as soon as possible. A free tool has been created to help administrators scan for systems vulnerable to BlueKeep and is available via links provided a Bleeping Computer article here. Lastly, we recommend network administrators proactively block TCP port 3389 at the perimeter firewall to protect unpatched systems within a secured network and disable unneeded Remote Desktop Services in their environment.***

Federal Partner Announcements

Ransomware Protection Strategies

The Cybersecurity and Infrastructure Security Agency (CISA) has observed an increase in ransomware attacks across the Nation. Helping organizations protect themselves from ransomware is a chief priority for CISA. Organizations are encouraged to review the following resources to help prevent, mitigate, and recover against ransomware:

- CISA Insights: Ransomware Outbreak
- CISA resource page on ransomware
- FireEye blog and report on ransomware protection and containment strategies

Victims of ransomware should report it immediately to CISA, a local FBI Field Office, or a Secret Service Field Office.

FBI Releases Article on Think Before You Post Campaign

The Federal Bureau of Investigation (FBI) has released an article on their Think Before You Post campaign, designed to educate students on the use of social media and how to avoid making poor choices when posting, texting, or emailing thoughts or grievances that could lead to disruptive behavior, including threats. The FBI article stresses that this type of online behavior could result in serious consequences to the individual as well as the community.

CISA encourages users to review the FBI article for information about the Think Before You Post campaign. CISA also recommends users review the CISA Tip on Identifying Hoaxes and Urban Legends for information on the potential dangers of viral emails. CISA encourages users to report suspicious activity to their local FBI field office and to FBI CyWatch at cywatch@fbi.gov.

North Korean Malicious Cyber Activity

CISA and the FBI have identified two malware variants—referred to as ELECTRICFISH and BADCALL—used by the North Korean government. The US government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA.

CISA encourages users and administrators to review the HIDDEN COBRA - North Korean Malicious Cyber Activity page, which contains links to Malware Analysis Reports MAR-10135536-

21 and MAR-10135536-10, for more information.

Current and Emerging Cyber Threats

Fraudulent Paypal Site Distributes Nemty Ransomware

An independent security researcher recently discovered a fraudulent site masquerading as the popular online payment platform, PayPal, that distributes Nemty ransomware. This malicious website promises unsuspecting victims a three to five percent return on purchases if they download and install an application. If victims click the "Download Now" button on the site, they will be prompted to install a malicious file which will infect the victims' systems with ransomware. To fool victims, the threat actors behind the campaign employ homograph domain name spoofing, a technique that replaces legitimate Unicode domain characters with characters from different alphabets, to make the URLs appear legitimate. Major antivirus providers and web browsers have already flagged the offending website as malicious; however, more will likely emerge as the Nemty ransomware campaigns continue. ***The NTIC Cyber Center recommends never using a link provided in an email, text message, messaging application, or through a social medial platform to visit or sign into any online account. We also recommend never downloading or installing applications from suspicious or untrusted sources and to keep antivirus software running and up-to-date with the latest virus definitions.***

Lilocked Ransomware Targets Servers and Websites

Lilocked, also known as Lilu, is a relatively new ransomware variant that is actively targeting web servers, encrypting data contained within and delivering a ransom note named #README.lilocked that demands payment in Bitcoin. Files encrypted by Lilocked display the .lilocked extension at the end of their names. Although the current distribution method is unknown, it is likely that web servers running software containing known vulnerabilities and that have remote access ports open and enabled are at an increased risk of this threat and other malicious activity. There is currently no publicly available decryption tool available to unlock files encrypted by Lilocked ransomware. ***The NTIC Cyber Center recommends web server administrators regularly back up website files, disable unnecessary remote desktop services and close unneeded ports, and keep all hardware, software, plugins, and operating systems patched and updated to reduce the risk of web server compromise. In addition, administrators are encouraged to use complex and unique login credentials and enable multifactor authentication for all administrator accounts and control panels, if possible.***

Vulnerabilities

Exim Mail Transfer Agent

Independent researchers identified a vulnerability within the Exim mail transfer agent (MTA) known as CVE-2019-15846 that, if abused, could allow unauthorized local and remote users without root access to execute programs on servers that accept TLS connections. CVE-2019-15846 is exploitable when threat actors send custom ServerName Indication (SNI) data during the initial TLS handshake. All Exim servers versions 4.80 and newer that accept TLS connections are vulnerable. Currently, the exploit is only a proof of concept and Exim's development team developed a patch. ***The NTIC Cyber Center recommends Exim server administrators update to Exim version 4.92.2 as soon as possible.***

Multiple GPS Tracker Devices

Researchers at Avast discovered vulnerabilities in 29 GPS tracker models from manufacturer Shenzhen i365, which have been redistributed under various brand names. Some of these devices are advertised as child and pet trackers and 600,000 of them are available for purchase via the Amazon.com marketplace and other online merchants. The vulnerabilities impacting these trackers can allow unauthorized parties to spoof user location, access the microphone, view personal user information, send SMS messages, and install new firmware. Additionally, the user accounts associated with the trackers use default passwords and the data transferred between the devices and their online accounts is routed through the insecure hypertext transfer protocol (HTTP). There is currently no patch or workaround available for these vulnerabilities. Avast disclosed the vulnerabilities to the manufacturer and, to date, have not received a response. ***The NTIC Cyber Center recommends users of affected Shenzhen i365 GPS tracking devices implement the appropriate vendor patches if and when they become available. If possible, consider decommissioning affected devices and replacing them with devices from reputable vendors.***

Data Breaches and Leaks

Security researchers identified a breach of personal data belonging to an unknown number of users of the job search platform Monster. Data exposed includes the names, addresses, email addresses, phone numbers, and employment history of job-seekers who posted résumés, CVs, and other documents to Monster between 2014 and 2017. The company believes the data was left exposed on

the web server of a third-party recruitment customer. ***The NTIC Cyber Center recommends that customers of Monster remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text message, or other avenues as a result of this data exposure.***

A security researcher discovered an exposed database containing over 419 million records of Facebook account holders. The database, which was left unsecured without a password, included information such as phone numbers, Facebook IDs, names, and genders of users in the United States, Vietnam, and the UK. Facebook believes the information was originally compiled by an unknown third party that scraped the platform for user data. ***The NTIC Cyber Center recommends that Facebook users remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text message, or other avenues as a result of this data exposure.***

Researchers believe that hackers breached the popular webcomic site XKCD and stole the personal data of 562,000 forum users. The stolen data, which has been since leaked on the Internet, includes usernames, email addresses, MD5 encrypted passwords, and IP addresses of the forum users. XKCD has issued a statement urging users to immediately change the passwords to any accounts on which they may have reused their XKCD login credentials. ***The NTIC Cyber Center recommends that XKCD forum users remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text message, or other avenues as a result of this data exposure. In addition, we encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication on any account that offers it to avoid falling victim to credential compromise.***

Upcoming Webinars

Data Breach Today
Prevention. Response. Notification.

Can't Stop, Won't Stop: How to Actually Prevent Employee Data Breaches

People cause data breaches every day. That simple statement hides layers of complexity, compliance issues, and stress for CISOs and their security teams. While we may be able to "logically" explain malicious breaches by linking them to motivations such as financial gain, it is often more difficult to understand and anticipate incidents caused by well-intentioned employees: the staff member who, for example, has too many things to do and sends an email to the wrong person or the person who feels they need to share information just to get their job done, choosing not to apply security or using unapproved channels.

This webinar will look at the psychology behind these breaches, and what technology can do to prevent incidents caused by employees sharing sensitive data via email. In particular, the session will examine developments in machine learning and advanced data loss prevention (DLP) technologies that can determine the risk of a data breach in real time to prevent unauthorized disclosure and enforce security for assured compliance.

Register for this webinar and learn about:

- Why well-meaning employees cause data breaches
- The most common email data breach incidents
- How machine learning and advanced DLP technology can prevent breaches and improve protection for shared data

To register for this free webinar on Tuesday, September 24 at 11:30 AM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Business Email Compromise (BEC) – also known as a CEO scam or whaling – is a type of phishing scheme in which the perpetrator conducts online reconnaissance against a target

organization and then uses various social engineering techniques to try and convince employees within that organization to divulge sensitive personal or financial information. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

A Ransomware Tale: Mayor Describes City's Decisions

Analytic Comment: Although the city of New Bedford, MA initially agreed to pay $400,000 to cyber criminals after a Ryuk ransomware attack impacted 158 city computer systems, the criminals' refusal to reduce the $5.3 million ransom demand resulted in the city's IT staff deciding to restore affected data from backups rather than allowing the criminals to profit from their misdeeds. Fortunately, several factors contributed to the quick containment and remediation of the infection, including the compartmentalized nature of the city's network infrastructure and the absence of many employees over the July 4th holiday weekend when the infection took place. Since the attack, the city has rebuilt its server network, restored most software applications, and replaced all affected computer workstations. According to one cybersecurity firm, New Bedford's response exemplifies best practices for quickly detecting, responding to, and recovering from the effects of a ransomware attack.

Interfaith's Zero Trust Network Protects Against Cyberattacks, Saves $2 Million

Analytic Comment: Interfaith Hospital in Brooklyn, NY, conducted a ransomware outbreak exercise to identify gaps in security controls, staff response protocols, and the organization's incident response plan. Participation in this simulation proved particularly beneficial in demonstrating the value of network segmentation for mitigating the spread of the ransomware outbreak. The hospital has since implemented a zero-trust network approach to ensure that lateral movement of any future malware outbreak will not endanger software or hardware systems, disrupt hospital operations, or compromise patient data. In addition, virtualization of the organization's servers has also saved the hospital more than two million dollars over the past seven years. These findings highlight the importance of taking proactive steps to bolster preparedness for cyber attacks and demonstrate the numerous benefits that exercises such as these can provide to high-risk or commonly targeted organizations.

Patches and Updates

Adobe Releases Security Updates

Exim Releases Security Patches

Google Releases Security Updates for Chrome

Intel Releases Security Updates

Microsoft Releases September 2019 Security Updates

WordPress Releases Security Update

ICS-CERT Advisories

BD Pyxis

Delta Electronics TPEditor

OSIsoft PI SQL Client

Red Lion Controls Crimson

Siemens IE-WSN-PA Link WirelessHART Gateway

Siemens Industrial Products

Siemens SIMATIC PCS7, WinCC, TIA Portal (Update C)

Siemens SIMATIC TDC CP51M1

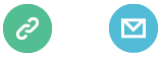
Siemens SIMATIC WinCC and PCS7 (Update B)

Siemens SINETPLAN

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

September 19, 2019

National Capital Region Cyber Threat Spotlight

Ryuk-Associated Malware Targets and Steals Military, Government, and Financial Files

Security researchers recently discovered a new malware variant that contains references to Ryuk ransomware in its code but, prior to encrypting files, this unnamed malware searches for and uploads sensitive files via file transfer protocol (FTP) to a site operated by the threat actor behind the campaign. It scans infected systems for folder and file names containing words such as *secret*, *private*, *confident*, *important*, *undercover*, *federal*, *government*, *military*, *finance*, and *security*, among others to upload to its FTP server. It also compares file names and extensions against a blacklist to prevent exfiltrating and encrypting critical system files. The malware distribution method is currently unknown. ***The NTIC Cyber Center encourages network administrators review our Ransomware Mitigation Guide and implement the recommendations provided to reduce the risk of a ransomware infection. Additionally, we recommend implementing a reputable data loss***

prevention solution to reduce the risk of sensitive data exfiltration and proactively block the indicators of compromise (IoCs) provided in this BleepingComputer article.

Federal Partner Announcements

2019 CWE Top 25 Most Dangerous Software Errors

MITRE has released the 2019 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Errors list. The Top 25 is a compilation of the most frequent and critical errors that can lead to serious vulnerabilities in software. An attacker can often exploit these vulnerabilities to take control of an affected system, obtain sensitive information, or cause a denial-of-service condition.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review the Top 25 list and evaluate recommended mitigations to determine those most suitable to adopt.

Current and Emerging Cyber Threats

Phishing Campaign Bypasses Email Security Using CAPTCHA

Researchers at Cofense discovered a new phishing campaign that abuses the online challenge-response verification test known as CAPTCHA to bypass automated security filters. From a compromised email account, threat actors send a phishing email to recipients that masquerades as a missed voicemail notification with an embedded link. Once clicked, users are prompted to solve the CAPTCHA test, which then forwards users to a phishing page designed to harvest login credentials. Links delivered through CAPTCHA bypass the secure email gateway (SEG) validation process since the SEG scans the URL for the clean CAPTCHA code landing page and not the URL where the victim is redirected. Additionally, in this campaign, the CAPTCHA and phishing sites are hosted on compromised websites using legitimate Microsoft top level domains, thus avoiding domain blacklisting. ***The NTIC Cyber Center recommends users remain vigilant for CAPTCHA phishing campaigns, avoid opening unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. We also recommend network administrators reference and block the associated IoCs contained in Cofense's report.***

New Malicious Email Campaigns Delivering Emotet

On August 23, 2019, the NTIC Cyber Center released a Cyber Alert to inform our members that the previously dormant command and control (C2) servers associated with Emotet, a modular banking trojan designed to steal network and account login credentials, was reactivated. Over the past week, independent security researchers observed a malicious email campaign attempting to deliver Emotet to governments, corporations, and individuals across the globe, confirming that the infrastructure is now actively in use. The malware payload in this campaign is delivered either via malicious links or attachments and, some emails also deliver the Trickbot Trojan. ***The NTIC Cyber Center recommends users remain vigilant for Emotet phishing campaigns, avoid opening and unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. If you believe you have been infected with Emotet, notify your organization's IT security team immediately so they may contain and remediate the infection.***

Vulnerabilities

SIM Card Vulnerability May Enable Remote Compromise of Mobile Devices

Researchers at AdaptiveMobile Security disclosed a SIM card vulnerability that allows threat actors to compromise mobile phones via SMS messages, possibly affecting over one billion users. This vulnerability, known as "Simjacker," allows threat actors to obtain personal information from a targeted device such as location, IMEI data, and system status information. Additionally, threat actors can also send messages and place phone calls originating from the victim's number, open URLs from the mobile browser, and disable the SIM card. This vulnerability exists within an application known as the SIMalliance Toolbox Browser, or S@T Browser, that is preinstalled on numerous SIM cards and can be exploited via a malicious SMS message. Threat actors only need a GSM modem to send the malicious SMS. Researchers have disclosed the vulnerability to the both the GSM Association and SIM alliance that represents SIM card manufacturers. ***The NTIC Cyber Center recommends GSM mobile device users monitor their devices for unusual and suspicious activity and update mobile systems if and when a patch becomes available.***

Comba and D-Link Routers

A Trustwave SpiderLabs security researcher discovered insecure storage vulnerabilities in Comba and D-Link brand routers. D-Link routers models DSL-2875AL and DSL-2877AL expose default administrator credentials in the source code. Additionally, DSL-2875AL exposes passwords in clear text when threat actors access a *romfile* configuration file via IP-based control panel. In Comba AC2400 Wi-Fi Access Controller, credentials are stored in a *DBconfig* configuration file in the

easily reversable M5 hash format. In the Comba AP2600-I Wi-Fi Access Point, plaintext credentials are exposed in a database file and are also included in a reversable MD5 hashed version in the source code of the IP-based control panel. There is currently no patch or workaround available for the vulnerable Comba routers. ***The NTIC Cyber Center recommends users monitor systems for unusual and suspicious activity and update D-Link routers with the latest firmware update. We also recommend updating the Comba AP2600-I Wi-Fi Access Point if and when a patch becomes available.***

Data Breaches and Leaks

Security researchers discovered customer contracts of over two million Verizon Wireless customers on a publicly accessible website. According to the researcher, a Verizon subdomain originally intended to be accessible only by employees contained PDF documents of contracts belonging to customers who paid for mobile devices using monthly installment plans. Information in the exposed contracts includes customers' full names, addresses, phone numbers, models and serial numbers of acquired devices, and customers' signatures. ***Though Verizon does not believe third parties other than the researcher accessed these records, the NTIC Cyber Center recommends that Verizon Wireless customers remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text message, or other avenues as a result of this data exposure.***

Russell Stover Candies released a customer notice disclosing data breaches that occurred at numerous Russell Stover retail stores throughout the United States. The company believes that malware installed on the stores' point-of-sale systems allowed cyber criminals to steal the payment card numbers, expiration dates, card verification codes, and cardholder names of over 74,000 customers at select Russell Stover locations from February 9, 2019 to August 7, 2019. Security researchers indicate that hackers have posted these records for sale on dark web marketplaces, with more records expected to be added in the coming weeks or months. So far, researchers believe 25 of the company's 28 retail locations were affected. ***Though Russell Stover does not have any retail locations within the National Capital Region, the NTIC Cyber Center recommends that customers who may have made purchases at any other Russell Stover retail locations during the affected time frame monitor their account statements and immediately notify their financial***

institutions of any unauthorized or suspicious activity.

A Security Discovery researcher discovered a misconfigured and unprotected Elasticsearch database exposing over 198 million user records from the vehicle listing website, Dealer Leads. The 413GB database includes user names, email addresses, physical addresses, phone numbers, finance data, loan data, vehicle information, and IP addresses. The database was exposed for an undetermined length of time and was publicly accessible without credentials. Dealer Leads has since restricted access to the database. ***The NTIC Cyber Center recommends any prospective car buyer who has submitted personal information into a car dealer's website remain vigilant for phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues. Administrators of Elasticsearch databases are encouraged to reference these instructions for configuring Elasticsearch cluster security to reduce the risk of unauthorized access and data compromise.***

Account data belonging to users of the third-party Google Drive application LuminPDF, a PDF viewing and editing tool, was stolen and leaked onto a hacking forum. Data exposed in the breach includes the full names, email addresses, gender, language settings, hashed password strings, and Google access tokens of over 24.3 million users of the software. Since stolen Google access tokens could allow malicious actors to access users' Google accounts, the NTIC Cyber Center advises users of LuminPDF to revoke the application's access to their Google drive accounts immediately. For instructions on how to manage app permissions and access, please reference the "Remove Google Drive Apps" section of Google's support page. ***In addition, the NTIC Cyber Center recommends that users of the LuminPDF tool, either as a standalone product or through the third-party Google Drive application, enable multifactor authentication on any account that offers it, monitor accounts for suspicious activity, and remain vigilant for an increase in phishing attempts as a result of this data exposure.***

A Grofers security researcher discovered over 8,000 publicly accessible Google Calendars belonging to various organizations. These calendars include sensitive details such as email addresses, event names, event details, locations, meeting links, internal presentation links, corporate data, and more. Researchers caution that publicly exposed calendars may allow third parties to access saved information, add malicious links to new events, or target users with credential-stealing phishing emails. ***The NTIC Cyber Center recommends Google Calendar users manage calendar access permissions under the "Settings" tab of Google Calendar to protect against the inadvertent exposure of sensitive information. Instructions on how to set Google Calendar visibility and sharing options is available on the G Suite Admin Help page here.***

Upcoming Webinars

Data Breach TODAY®
Prevention. Response. Notification.

Account Origination Fraud: Mitigating Human Farms

Online account origination (OAO) fraud has grown 30 percent since 2017, with $1.3 billion in losses in 2018. The increase in losses has a lot to do with fraud rings switching from automated attacks to human workers who submit applications manually - this is because nothing solves a CAPTCHA like a human.

Join this webinar to learn the patterns, tactics, and behavior that expose human farms and other bad actors who use stolen or fake identities, and mitigate them before it's too late.

Key takeaways will include:

- How OAO can directly impact your revenue
- The anatomy of a human farm attack
- How passive biometrics can mitigate human farms

To register for this free webinar on Wednesday, September 25 at 2:00 PM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

A ***dark pattern*** is a type of social engineering technique whereby businesses or other organizations use crafty user interface/user experience (UI/UX) designs to manipulate users into making unintended choices. Dark patterns are often used to charge unwitting customers money, maintain a user's attention, harvest personal data, gain or retain subscribers, and display advertisements. While most of these tactics are not necessarily illegal, they can cost customers time, money, and privacy. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Fraudsters No Longer Operate in Silos, They Are Attacking across Industries and Organizations
Analytic Comment: A recent LexisNexis report highlights emerging tactics that cyber criminals employ when attacking organizations across industries. The firm observed cyber criminals increasingly using bot attacks to create new accounts and build online identities for financial gain. In the first six months of 2019, the firm recorded a 305 percent increase in the number of bot attacks perpetrated against online marketplaces, virtual gift card companies, and ridesharing sites. In addition, mobile app attacks have increased by 148 percent, with these attacks targeting media companies, social media organizations, and gaming organizations for personal information and bank account access. This report provides insight into the current shifts in threat actor tactics and underscores the importance of implementing multi-layered fraud defense platforms for combating these threats.

Cybercrime Black Markets: RDP Access Remains Cheap and Easy
Analytic Comment: Cybercrime-as-a-service and other illicit offerings on the dark web remain cheap and easily accessible, according to research from cloud security vendor Armor. For example, prices for stolen payment cards have fallen due to an excess in supply of stolen payment cards obtained from online skimming attacks. Additionally, cybercriminals sell stolen credentials, such as those used to access targeted Remote Desktop Protocol (RDP) servers, for around $25 per server. Illicit access to RDP servers is one of the initial attack vectors on which cybercriminals often rely when deploying ransomware or other malicious payloads onto targeted systems. Other offerings for

sale on Dark Web marketplaces include stolen medical records, tax information, identity packets, bank account credentials, and spamming services. This report demonstrates that the ease of access to readily-available and inexpensive cybercrime tools has lowered the barrier of entry for criminals and, in turn, has facilitated the prevalence of cybercrimes such as identity theft, ransomware attacks, and fraud.

Most Cyber Attacks Focus on Just Three TCP Ports

Analytic Comment: Cyber threat intelligence firm Alert Logic released a report stating that the TCP ports that are most frequently used to conduct cyber attacks are 22 (SSH), 80 (HTTP), and 443 (HTTPS). Additionally, the firm notes that Microsoft's Remote Desktop Protocol (RDP) that communicates over TCP port 3389 is also commonly used in remote attacks against systems and networks. In addition to vulnerable ports, the firm found that 75 percent of organizations surveyed ran outdated and unsupported software and 66 percent employed weak encryption algorithms to protect data. This report highlights the importance of keeping software updated and closing or restricting access to remote access ports to reduce the risk of a successful cyber attack.

Patches and Updates

VMware Releases Security Updates for Multiple Products

ICS-CERT Advisories

3S-Smart Software Solutions GmbH CODESYS V3 Web Server

3S-Smart Software Solutions GmbH CODESYS V3 Library Manager

3S-Smart Software Solutions GmbH CODESYS Control V3 Online User Management

3S-Smart Software Solutions GmbH CODESYS Control V3 OPC UA Server

3S-Smart Software Solutions GmbH CODESYS V3 Products Containing a CODESYS Communication Server

Advantech WebAccess

Honeywell Performance IP Cameras and Performance NVRs

Philips IntelliVue WLAN

Siemens SINEMA Remote Connect Server

We welcome your feedback.

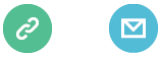
Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on ***Subscribe*** *to Receive Our Products* at the top of the page, and enter your information.



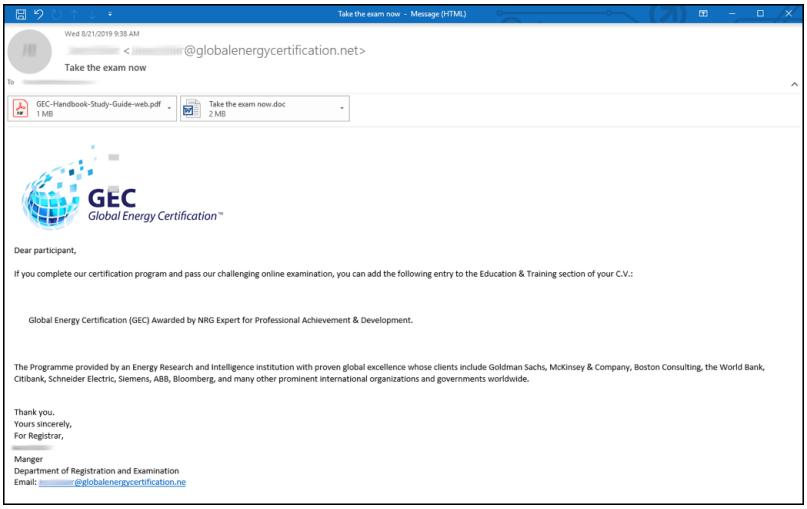
NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

September 26, 2019

National Capital Region Cyber Threat Spotlight



LookBack Malware Distributed in Spear Phishing Emails Targeting Utility Sector Organizations

Cybersecurity company Proofpoint released analysis of a spear phishing campaign targeting US utility sector companies with malware known as “LookBack,” a remote access Trojan (RAT) primarily used to access and exfiltrate data from infected systems. This campaign sends emails that appear to originate from Global Energy Certification, a legitimate licensing organization, and contain malicious macro-enabled Microsoft Word documents that deliver and install the LookBack RAT when opened. LookBack can perform the following functions:

- Enumeration of services
- Viewing of process, system, and file data
- Finding, reading, writing, and deleting files

- Executing commands
- Taking screenshots
- Moving and clicking the cursor
- Rebooting the machine and deleting itself from an infected host

According to Proofpoint's report, the LookBack campaign targeted at least 17 US utility sector entities between April 5, 2019 and August 29, 2019. Proofpoint observed threat actors scanning targeted organizations for open Server Message Block (SMB) protocols over port 445 up to two weeks before the arrival of the LookBack-laden phishing emails. This preoperational reconnaissance tactic may have helped the threat actors identify vulnerable systems and map targeted networks to ensure the successful lateral movement of the infection. Some security researchers suggest that the Chinese state-sponsored hacking group APT10 is responsible, though no formal attribution has been made.

Since exploiting Microsoft Office macro functionality to deliver malicious payloads is a common attack vector, the NTIC Cyber Center recommends that users disable Microsoft Office macros by default and avoid opening documents from unknown and untrusted sources. We also advise network administrators, particularly those in the critical infrastructure sector, to proactively block SMB port 445 at the perimeter firewall to prevent the malicious scanning of networks and systems. Furthermore, we recommend implementing a reputable data loss prevention solution to reduce the risk of sensitive data exfiltration. Finally, we encourage administrators to scan for and proactively block the latest Indicators of Compromise (IoCs) associated with LookBack malware provided in ProofPoint's article here.

Fake Employment Site Targets Veterans with Malware

Cisco's Talos Security Intelligence and Research Group discovered a malware campaign targeting US veterans seeking employment. This campaign attempts to lure veterans to hiremilitaryheroes[.]com, a fraudulent website that is designed to deliver malware to Windows

systems. The website advertises a free “desktop app” that, if downloaded, installs malware that exfiltrates system information and allows threat actors to remotely control the infected system. Security researchers have attributed this campaign to Tortoiseshell, an Iranian nation-state hacking group. ***The NTIC Cyber Center recommends only downloading applications from trusted and vetted sources and running reputable and up-to-date antivirus software. We also recommend network administrators reference and block the associated IoCs contained in Talos's report.***

Federal Partner Announcements

CISA Releases Four New Insights Products

The Cybersecurity and Infrastructure Security Agency (CISA) has released four new CISA Insights products informed by US intelligence and real-world events. Each of the following products provides a description of the threat, lessons learned, recommendations, and additional relevant resources:

- Mitigate DNS Infrastructure Tampering
- Remediate Vulnerabilities for Internet-Accessible Systems
- Secure High Value Assets
- Enhance Email and Web Security

CISA urges organizations to review the updated CISA Insights page and implement the recommendations.

National Cybersecurity Awareness Month 2019

October 1 marks the beginning of National Cybersecurity Awareness Month (NCSAM) 2019. NCSAM is a collaborative effort between government and industry to raise awareness about the importance of cybersecurity and ensure that all Americans have the resources they need to be safer and more secure online.

With NCSAM just around the corner, head to the NCSAM 2019 Website to download all the materials needed to "Own IT. Secure IT. Protect IT." this October. The website will continuously release products leading into NCSAM, so be sure to bookmark this page and return often to see the

latest and greatest NCSAM materials. Products include tip sheets, presentations, graphics, and more.

Join the conversation throughout the month by following and engaging with CISA social media outlets such as @cyber, @CISAgov, @CISAKrebs, and @CISAManfra. Promote NCSAM on social media by using the hashtags #BeCyberSmart, #CyberAware, and #NCSAM2019. And help spread the word by including NCSAM-branded graphics in business outreach efforts.
Lastly, NCSAM engagement opportunities can be found at several upcoming events. Visit the NCSAM booth, attend a NCSAM workshop, or listen to a NCSAM speaker at one of the events listed below.

- October 2: Public Sector Innovation Summit, Arlington, Virginia
- October 8: Smart Cities Connect Fall Conference and Expo, National Harbor, Maryland
- October 10: Federal Ignite Conference, Washington, D.C.

More NCSAM event programming can be found at StaySafeOnline.org.

Current and Emerging Cyber Threats

Emotet Distributed in Spam Campaign Advertising Snowden Book

Malwarebytes researchers discovered a new malicious email campaign that claims to deliver a free scanned copy of Edward Snowden's new book ""Permanent Record" via an attachment while attempting to infect users with Emotet, a modular banking Trojan designed to steal network and account login credentials. Once the attachment is opened, a message is displayed that prompts recipients to click an "enable editing" or "enable content" button to continue. The "enable" button loads a macro that delivers the Emotet payload onto the target system. ***The NTIC Cyber Center recommends users remain vigilant for Emotet email campaigns, avoid opening and unexpected emails, and refrain from clicking on links or opening attachments from unknown or untrusted sources. If you believe you have been infected with Emotet, notify your organization's IT security team immediately so they may contain and remediate the infection.***

IRS Phishing Campaign Spreads Amadey Botnet

Researchers at Cofense discovered a new phishing campaign masquerading as notices from the Internal Revenue Service (IRS) that attempts to infect users with the Amadey botnet. Threat actors send spoofed IRS correspondence via email informing users of a tax refund along with a single use credential. In the email body, recipients are urged to click the "Login Right Here" button which forwards them to a fraudulent IRS login page where they are prompted to enter the single use

credential. Once logged in, users are prompted with instructions on how to obtain a tax refund that includes downloading a document containing a Visual Basic script (VBScript) dropper. The VBScript will then deploy the Amadey payload onto the target system. Amadey will immediately reach out to its command and control (C2) server siphoning system information and standby for further commands from the threat actor. Amadey will maintain persistence on the target system via the registry editor. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns disguised as IRS refund notices, avoid opening unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. We also recommend network administrators reference and block the associated indicators of compromise (IoCs) contained in Cofense's report.***

Spoofed Version of Stockfolio Trading App Distributes Malware

Researchers at Trend Micro discovered two malware variants distributed through a compromised version of Stockfolio, a stock trading app available for Mac systems. Threat actors laced Stockfolio version 1.4.13 with one of two variants known as *Trojan.MacOS.GMERA.A* and *Trojan.MacOS.GMERA.B*, both of which pilfers the target's system information and are signed with the malware developer's digital certificate. *Trojan.MacOS.GMERA.A* features bundled shell scripts in the Resources directory which siphons information into a hidden file uploading to a URL. *Trojan.MacOS.GMERA.B* features malware execution logs and the ability to maintain persistence allowing threat actors to run shell commands. In July, Apple revoked the malware developer's digital certificate for the fraudulent app after Trend Micro disclosed it to them. ***The NTIC Cyber Center recommends only downloading applications from trusted and vetted sources and running reputable and up-to-date antivirus software. We also recommend network administrators reference and block the associated IoCs contained in Trend Micro's report.***

Malicious Android Apps Discovered in Google Play Store

Security researchers at Wandera discovered two malicious Android apps available in the Google Play Store that perform click fraud and record audio without user consent. The two malicious apps have been downloaded over 1.5 million times and masquerade as photography apps dubbed Sun Pro Beauty Camera and Funny Sweet Beauty Selfie Camera. When installed, these apps secretly record user audio and click ads that run in the background, generating fraudulent revenue for the threat actors behind the campaign. To avoid removal and maintain persistence, these apps create a shortcut and hide themselves from the app drawer. Google has removed the two malicious apps from the Google Play Store. ***The NTIC Cyber Center recommends Android users install and use Google Play Protect, an official Android tool that scans apps for malware prior to download. After installing any new app, monitor the device for unusual behavior such as excessive power consumption, excessive data usage, unexpected pop-ups, and uninstall problematic apps***

immediately, performing a factory reset of the device if necessary. If the device permissions required by an app do not match the advertised functionality, refrain from installing it. Lastly, we recommend all Android users update their devices to the latest OS, Android 10, as soon as possible.

Vulnerabilities

D-Link DNS-320 ShareCenter Network Storage Devices

A researcher at CyStack Security discovered a vulnerability in the D-Link DNS-320 ShareCenter network storage device. If exploited, this vulnerability could allow a remote attacker to execute remote commands with root permission. This vulnerability exists in all versions of the device's firmware in versions 2.05b10 and older, though D-Link has issued a patch that fixes the issue in the latest release, v2.06b01. ***The NTIC Cyber Center encourages administrators of D-Link DNS-320 to install the latest update, available here, to mitigate the risks posed by this vulnerability. In addition, we remind administrators to keep network storage devices disconnected from the open Internet, maintain regular system backups to recover any data lost in a disaster, and ensure any computers that access information on network storage devices are enabled with anti-virus protection and malware protection.***

vBulletin Forum Software

An anonymous security researcher published details of a zero-day vulnerability affecting vBulletin, a popular Internet forum software package. If exploited, this vulnerability could allow remote attackers to execute commands on servers running vBulletin versions 5.0.0 to 5.5.4 (the latest version), possibly facilitating the takeover of forum installations and the theft of forum users' information. Since the disclosure of the vulnerability, a user on GitHub has also posted a script tool that automates searches for vulnerable vBulletin sites. Security experts believe that, as there are estimated to be tens of thousands of vBulletin forums installed across the Internet, this vulnerability could impact billions of registered forum users. ***The NTIC Cyber Center advises administrators of websites hosting vBulletin forum installations to download the latest patch, available at vBulletin's site here.***

Upcoming Webinars

Account Origination Fraud: Mitigating Human Farms

It used to be that we would only have to worry about losing all of our data if we suffered a massive system crash. Now, the fear of having your information held hostage by threat actors demanding payment is just as common. Since paying the ransom is no guarantee that all of the data will be recovered and remediation costs can be thousands of dollars, one would almost prefer a system failure.

Whether it's individuals, organizations or even entire cities—it seems like no one is safe from the epidemic of ransomware that has spread worldwide. Now that everyone has a target on their backs, what can be done?

Join cybersecurity experts Bob Erdman, Security Product Manager at Helpsystems, and Holger Schulze, CEO and Founder of Cybersecurity Insiders, as they discuss motivations and perpetrators of attacks, who is at the highest risk, and the most effective solutions to this pervasive problem to help you better understand ransomware and reduce the large threat it poses. Learn more about:

- Entrance points for ransomware
- Frequency of attacks
- Detection of ransomware
- Response to ransomware and remediation

To register for this free webinar on Tuesday, October 8 at 12:00 PM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Whether tax season elicits delight or dread, one thing is for sure: it's prime time for scammers to perpetrate ***Internal Revenue Service (IRS) tax scams***. These scams may come in a variety of forms, all designed to separate you from your money. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Top 10 Tactical Recommendations for SMB Cybersecurity
Analytic Comment: There are basic steps that all small and medium-sized businesses can take to reduce their risk of successful cyber attacks and data breaches. For example, keeping operating systems updated, downloading and installing patches and updates regularly, using strong passwords and a password management tool, and implementing two-factor authentication on employee user accounts can go a long way in preventing businesses from becoming victimized in an opportunistic attack. Having a robust and regularly tested data backup plan in place that includes encrypting data at rest and storing data off the network can protect against unauthorized data exfiltration and ransomware infections. These recommendations, however commonplace they may seem, are invaluable, and could spell the difference between data and system recovery and the irreparable and catastrophic loss of critical data needed to run and maintain business operations.

Businesses Need to Treat Cybersecurity as Something That Crosses Organizational Boundaries
Analytic Comment: A recent CompTIA survey of 500 businesses illuminates the differing perspectives of the state of cybersecurity within companies' business units. According to the survey, 91 percent of executives and business staff believe there is a strong understanding of cybersecurity at their company, whereas only 78 percent of IT staff hold the same belief. Similarly, over 50 percent of executives and business staff rated their organization's cybersecurity efforts as satisfactory, with only 35 percent of IT staff responding the same way. These disparities demonstrate the differences in opinions held by business staff and technology professionals toward the state of an organization's cyber readiness. Furthermore, they highlight the need for businesses to treat cybersecurity as a cross-organizational concern, and not simply as one confined to a company's IT department.

Patches and Updates

Jira Service Desk

Tridium Niagara

ICS-CERT Advisories

Adobe Releases Security Updates for ColdFusion

Apple Releases Security Updates

Canadian Centre for Cyber Security Releases Advisory on New Ransomware Campaign

Google Releases Security Updates for Chrome

Microsoft Releases Out-of-Band Security Updates

VMware Releases Security Updates

VMware Releases Security Updates for Multiple Products

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

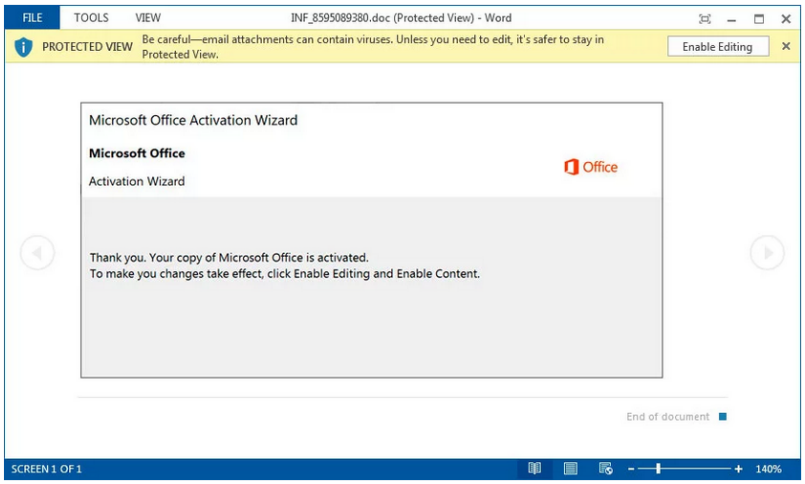
TLP:WHITE

Product No. 2019-10-002

HSEC-1 | NTIC SIN No. 2.5, 5.4

October 3, 2019

National Capital Region Cyber Threat Spotlight



Renewed Emotet Campaigns Target Users with Fraudulent MS Office Activation Wizard Messages

The NTIC Cyber Center has observed an increase in reported malware campaigns attempting to deliver Emotet, a modular banking Trojan designed to steal network and account login credentials from unsuspecting users. On August 23, 2019, we reported that, after a two month hiatus, the command and control (C2) infrastructure associated with Emotet became active again, according to researchers at Cofense Labs. Shortly after the infrastructure was reactivated, cybersecurity firms began observing new Emotet campaigns employing various methods to infect victims, the latest using malicious email attachments that masquerade as the Microsoft Office Activation Wizard. As is common in many malicious email campaigns, this Emotet campaign attempts to trick recipients into

enabling macros on the malicious document that will then download and install the pervasive banking Trojan. ***As Emotet campaigns continue to evolve and employ new methods to infect victims, the NTIC Cyber Center would like to remind our readers to never open attachments, enable macros in documents, or click on links contained within unexpected or unsolicited emails. Additionally, always run updated reputable antivirus software on all computer systems and mobile devices. If you believe you have been infected with Emotet, notify your organization's IT security team immediately so they may contain and remediate the infection.***

Federal Partner Announcements

National Cybersecurity Awareness Month

October is National Cybersecurity Awareness Month (NCSAM), which is a collaborative effort between the Cybersecurity and Infrastructure Security Agency (CISA) and its public and private partners—including the National Cyber Security Alliance (NCSA)—to ensure every American has the resources they need to stay safe and secure online while increasing the resilience of the Nation against cyber threats. This year's theme, "Own IT. Secure IT. Protect IT.," focuses on promoting personal accountability and positive behavior when it comes to cybersecurity.

CISA encourages organizations to see the NCSAM 2019 webpage and the NCSAM 2019 Toolkit for ways to participate in and promote NCSAM.

US Food and Drug Administration Warns of Vulnerabilities Affecting Connected Medical Devices and Health Care Networks

The US Food and Drug Administration (FDA) is informing patients, health care providers and facility staff, and manufacturers about cybersecurity vulnerabilities that may introduce risks for certain medical devices and hospital networks. The FDA is not aware of any confirmed adverse events related to these vulnerabilities. However, software to exploit these vulnerabilities is already publicly available.

Security researchers have identified 11 vulnerabilities, named "URGENT/11." These vulnerabilities may allow anyone to remotely take control of the medical device and change its function, cause denial of service, or cause information leaks or logical flaws, which may prevent device function.

These vulnerabilities exist in IPnet, a third-party software component that supports network communications between computers. Though the IPnet software may no longer be supported by the original software vendor, some manufacturers have a license that allows them to continue to use it without support. Therefore, the software may be incorporated into other software applications, equipment, and systems which may be used in a variety of medical and industrial devices that are still in use today.

Security researchers, medical device manufacturers, and the FDA are aware that some versions of the following operating systems are affected. Please note that the vulnerable IPnet software component may not be included in all versions of these operating systems:

- VxWorks (by Wind River)
- Operating System Embedded (OSE) (by ENEA)
- INTEGRITY (by Green Hills)
- ThreadX (by Microsoft)
- ITRON (by TRON Forum)
- ZebOS (by IP Infusion)

Some medical device manufacturers are already actively assessing which devices that use these operating systems are affected by URGENT/11 and identifying risk and remediation actions. Several manufacturers have also notified their customers consumers with devices determined to be affected so far, which include an imaging system, an infusion pump, and an anesthesia machine. The FDA expects that additional medical devices will be identified that contain one or more of the vulnerabilities associated with the original IPnet software.

Mitigation recommendations for manufacturers, health care providers, health care facility and IT staff, patients, and caregivers are available in the October 1, 2019 FDA News Release.

Current and Emerging Cyber Threats

PcShare Backdoor Modified for Additional Malicious Functions

Researchers at Cylance discovered threat actors utilizing a modified version of an open-source backdoor, PcShare, for reconnaissance. PcShare features command-and-control (C2) encryption and

proxy bypass functionality and allows threat actors to exfiltrate data, move laterally within a network, execute arbitrary code, modify data, and upload and download files remotely. Threat actors infect users by dynamic-link library (DLL) side-loading a legitimate NVIDIA application, NVIDIA Smart Maximise Helper Host, facilitating the payload onto the target system. Cylance researchers suggest that this modified version of PcShare was developed by a Chinese advance persistent threat group. ***The NTIC Cyber Center recommends only downloading applications from trusted and vetted sources and running reputable and up-to-date antivirus software. We also recommend network administrators reference and block the associated IoCs contained in Cylance's report.***

WhiteShadow Malware Downloader Distributed in Phishing Emails Disguised as Invoices

Researchers at Proofpoint discovered a malicious email campaign that uses a Visual Basic macro, dubbed WhiteShadow, to infect users with various malware. Threat actors send recipients emails masquerading as invoices that prompt users to open an attachment or click a URL. Once the attachment is opened or the URL is clicked, WhiteShadow executes a SQL query against a threat actor-controlled Microsoft SQL server database that delivers malware such as remote access Trojans (RATs), keyloggers, and downloaders to the victim's computer. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns disguised as invoice notices, avoid opening unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. We also recommend network administrators reference and block the associated indicators of compromise (IoCs) contained in Proofpoint's report and to thoroughly vet network traffic traveling over TCP port 1433.***

Nodersok Malware Uses Legitimate Computer Applications for Malicious Activity

Security researchers at Microsoft discovered a fileless malware campaign dubbed Nodersok that abuses legitimate tools and services, a technique known as living-off-the-land binaries (LOLBins). Nodersok allows threat actors to use infected systems as a proxy to access other connected systems such as compromised machines, C2 servers, and websites. Additionally, Nodersok attempts to disable Windows Defender Antivirus and Windows updates and also elevates account privileges. Users are infected when they download and execute an HTML application (HTA) file, usually disguised as a browser-based ad. Once executed, a multi-stage infection process occurs utilizing JavaScript code and Powershell to compromise machines. Because Nodersok uses LOLBins, leveraging legitimate system infrastructure, common signature-based antivirus tools are less likely to detect the infection. ***The NTIC Cyber Center recommends users remain vigilant for Nodersok malware campaigns and refrain from clicking on links or downloading applications from unknown or untrusted sources. If you believe you have been infected with Nodersok, notify your***

organization's IT security team immediately so they may contain and remediate the infection.

Phishing Campaigns Abuse Open Redirect Vulnerabilities in Adobe and Google Domains

Security researchers warn that attackers are using open redirect vulnerabilities found in Google and Adobe domains to wage phishing campaigns and direct users to malicious sites. Open redirect vulnerabilities allow attackers to construct web addresses that appear legitimate but instead divert visitors to malicious destinations. Examples of these maliciously crafted web addresses have been observed in recent spam campaigns crafted to steal recipients' Microsoft Office 365 credentials, with attackers hiding malicious links in web addresses that appear to point to legitimate Google or Adobe domains. Such abuse of open redirect vulnerabilities adds legitimacy to spam emails and increases the likelihood that unsuspecting users will visit associated fraudulent login pages or other harmful websites. ***The NTIC Cyber Center advises email recipients to remain vigilant for malicious links that redirect from other domains, avoid opening unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources.***

For more information about open redirect vulnerabilities, including tips for web administrators on how to mitigate these risks, please see our recent Cyber Advisory entitled Open Redirect Vulnerabilities Facilitate Malicious Cyber Activity.

Cyber Threat Group Silent Starling Perpetrating "Vendor Email Compromise" Scams

Researchers at email security firm Agari have observed a new cyber threat group, called Silent Starling, conducting a novel attack dubbed "vendor email compromise" (VEC). Instead of using typical business email compromise (BEC) tactics to impersonate an employee's communications with his or her finance department, Silent Starling has shifted to impersonating vendors' communications with customers. In these scams, threat actors hijack the email accounts of employees within vendors' finance departments and monitor correspondence between vendors and customers over time. Once threat actors have obtained enough data and context on the parties' transactions, they send invoices convincing customers to send payments for products or services to threat-actor owned accounts. Agari indicates that Silent Starling has used phishing emails disguised as suspicious activity alerts, Microsoft OneDrive notifications, DocuSign requests, and voicemail and fax notifications to obtain user credentials and gain access the email communications of over 700 employees from 500 companies in 14 countries to date. ***The NTIC Cyber Center recommends all organizations review vendor update procedures to ensure that vendors and suppliers are properly verified before any changes are made to payment methods or account information. Furthermore, we recommend users remain vigilant for phishing attempts disguised as security***

notifications or other benign correspondence, avoid opening unexpected emails, and refrain from clicking on links from unknown or untrusted sources.

Data Breaches

Food delivery company DoorDash announced a data breach affecting 4.9 million users of the DoorDash platform. Information compromised includes the names, email addresses, delivery addresses, order histories, phone numbers, and hashed passwords of consumers, drivers, and merchants who joined the DoorDash platform on or before April 5, 2018. In addition, the driver's license numbers of approximately 100,000 DoorDash delivery drivers were also compromised in this breach. Though DoorDash does not believe the information accessed could allow attackers to make fraudulent credit card charges or bank account withdrawals, the company has nevertheless urged users to change their account passwords to prevent unauthorized access. ***The NTIC Cyber Center recommends that DoorDash users who registered on the platform before the affected time frame remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text message, or other avenues as a result of this data exposure. In addition, we encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication on any account that offers it to avoid falling victim to credential compromise.***

Gaming company Zynga has announced a breach of data belonging to 218 million users of its popular mobile gaming app "Words With Friends." Information stolen in the breach includes the names, email addresses, login IDs, hashed passwords, password reset tokens (if ever requested), phone numbers (if provided), Facebook ID (if connected), and Zynga account ID of all players who installed and registered for the "Words With Friends" gaming app before September 2, 2019. The infamous hacker Gnosticplayers, known for stealing collectively over one billion user credentials in various data breaches to date, has claimed responsibility for the attack. In addition to breaching "Words With Friends," the hacker also claims to have accessed user data from other Zynga apps including "Draw Something" and "OMGPOP." ***The NTIC Cyber Center urges users of Zynga-***

developed mobile gaming apps to immediately change their login passwords and passwords to any accounts on which they may have reused their Zynga login credentials. In addition, we encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication on any account that offers it to avoid falling victim to credential compromise. Lastly, we recommend users remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text message, or other avenues as a result of this data exposure.

Cybersecurity company Comodo announced a breach of data belonging to 245,000 registered users of its discussion board and forum service known as ITarian. Information accessed in this breach includes users' full names, email addresses, login usernames, hashed passwords, last IP addressed used to access the forums, and, for some users, social media usernames. Comodo believes that attackers exploited a recent zero-day vulnerability affecting vBulletin, the server application powering the company's forums, to compromise the site and steal user information. ***The NTIC Cyber Center advises users of Comodo's ITarian discussion boards and forums to immediately change their account passwords. In addition, we remind administrators of websites hosting vBulletin forum installations to immediately download and install the latest vBulletin patch to prevent similar incidents.***

Customer service software provider Zendesk disclosed a data breach affecting approximately 10,000 users using Zendesk Support and Chat products from accounts created before November 1, 2016. Information compromised in the breach includes end-user and agent names, phones numbers and email addresses, credentials (salted and hashed), transport layer security (TLS) encryption keys, and configuration settings of apps installed from the Zendesk app marketplace or private apps. Zendesk will notify affected users and is remediating the situation by informing law enforcement, activating internal response teams, and consulting with third-party forensic providers. ***The NTIC Cyber Center***

recommends that customers who registered for Zendesk Support and Chat accounts prior to November 1, 2016, monitor their accounts for any unauthorized or suspicious activity, change their credentials, and enable multifactor authentication on any account that offers it.

Upcoming Webinars

Data Breach Today
Prevention. Response. Notification.

Security Leaders Share Secret Sauce for Success with Digital Transformation

Digital transformation continues to reshape the modern enterprise. Savvy organizations that understand and drive forward digital innovation ultimately win the within an organization. However, securing the technologies that enable digital transformation becomes its own challenge.

This panel brings together three industry practitioners, including a TD Ameritrade CISO, a former CISO at AT&T and a security veteran from CyberArk to discuss issues surrounding security and digital transformation. We have asked these security leaders to share the most pressing challenges organizations face today and to lend some insights into their secret sauce for success with digital transformation.

As a security professional in today's digital enterprise, this is a slice of collective wisdom to help you overcome the security, technology and organizational challenges you are facing today.

The panelists will offer practical tips and best practices for security leaders to help manage risk, prioritize security solutions, handle security product implementations and align with digital transformation requirements from their business organizations.

You will learn:

- The changing role of security and how it affects you
- How to overcome roadblocks to security in the digital enterprise
- How to best align security and business needs
- The most vulnerable areas of the digital enterprise and how to secure them
- Why privileged access security should be considered in the digital transformation projects

To register for this free webinar on Tuesday, October 8 at 11:30 AM EDT, click here.

How Organizations are Responding to the Continuing Challenge of Ransomware

It used to be that we would only have to worry about losing all of our data if we suffered a massive system crash. Now, the fear of having your information held hostage by threat actors demanding payment is just as common. Since paying the ransom is no guarantee that all of the data will be recovered and remediation costs can be thousands of dollars, one would almost prefer a system failure.

Whether it's individuals, organizations or even entire cities—it seems like no one is safe from the epidemic of ransomware that has spread worldwide. Now that everyone has a target on their backs, what can be done?

Join cybersecurity experts Bob Erdman, Security Product Manager at Helpsystems, and Holger Schulze, CEO and Founder of Cybersecurity Insiders, as they discuss motivations and perpetrators of attacks, who is at the highest risk, and the most effective solutions to this pervasive problem to help you better understand ransomware and reduce the large threat it poses. Learn more about:

- Entrance points for ransomware
- Frequency of attacks
- Detection of ransomware
- Response to ransomware and remediation

To register for this free webinar on Tuesday, October 8 at 12:00 PM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Celebrity scams – also known as imposter scams, impersonation scams, and fan scams – are a type of social engineering scheme in which the perpetrator masquerades as a celebrity or popular social media personality, concealing his or her true intentions to elicit money or personal information or to trick the victim into clicking on malicious links. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Legit-Looking iPhone Lightning Cables That Hack You Will Be Mass Produced and Sold

Analytic Comment: A security researcher who sold a limited number of malicious Apple lightning cables at this year's DEFCON conference announced that the cable will soon be ready for mass-production. The cable, known as the "O.MG Cable," looks like a legitimate Apple charging cable but has been modified to include components that can allow an attacker to wirelessly take control of any computer into which the cable is connected, from up to 300 feet away. The O.MG cable will be sold and distributed on the hacking and cybersecurity tools website Hak5, though the cable's price has yet to be announced. The impending sale of these devices highlights the increasing availability and accessibility of hacking tools that place malicious activity into the hands of any buyer willing to pay for them. In addition, it serves as a reminder to beware of third-party accessories that may be malicious and to avoid connecting any unapproved, untrusted, or unauthenticated cables or devices into USB ports.

There Have Been 800-Plus Political Cyberattacks in the Past Year Alone

Analytic Comment: Microsoft reports that in the past year, political campaigns, parties, and pro-democracy groups have been targeted with over 800 cyber attacks, with the number expected to continue to increase as the 2020 elections near. Phishing campaigns, distributed denial-of-service (DDoS) attacks, and domain name spoofing are just a few of the malicious activities threat actors have directed at the US election system and its participants. To combat these threats, Microsoft offers a free tool called AccountGuard, designed to provide notifications about cyber threats and incidents, to all current candidates for federal, state, and local office and their staff. As experts believe malicious cyber activity surrounding elections will increase, maintaining awareness of the cyber threat landscape, as well as consistent usage of cyber hygiene practices, will be likely be requirements for any parties concerned with ensuring the security of the US election system approaching 2020.

Patches and Updates

Apple Releases Security Updates

Cisco Releases Security Advisories

Exim Releases Security Update

MS-ISAC Releases Advisory on PHP Vulnerability

ICS-CERT Advisories

Interpeak IPnet TCP/IP Stack

Interpeak IPnet TCP/IP Stack

Moxa EDR 810 Series

Yokogawa Products

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2019-10-012

HSEC-1 | NTIC SIN No. 2.5, 5.4

October 10, 2019

National Capital Region Cyber Threat Spotlight

Microsoft Issues Warning on Iranian Threat Group Phosphorus

The Microsoft Threat Intelligence Center (MSTIC) issued a warning after discovering that an Iranian cyber threat group, dubbed Phosphorus, actively targeted email accounts associated with a US presidential campaign, current and former US government officials, and political journalists. According to MSTIC researchers, in a 30-day period between August and September of this year, Phosphorus attempted more than 2,700 times to identify specific Microsoft consumer email accounts, attacked 241 of those accounts, and successfully compromised four accounts, none of which were associated with any US government official or presidential campaign. The MSTIC observed Phosphorus using information likely gathered through online reconnaissance techniques, attempting to gain access to secondary email accounts linked to the targeted Microsoft accounts and using their targets' phone numbers when initiating password reset requests. These observations lead MSTIC to believe that the threat actors behind the campaign are highly motivated and are likely to continue their operations. ***To combat this and other advanced persistent threats, the NTIC Cyber Center recommends using lengthy, unique, and complex passwords for every account, enabling multifactor authentication when available, and regularly monitoring account login histories for***

suspicious and unauthorized activity. For more information about this threat and for instructions on how to secure Microsoft accounts, please review the Microsoft report titled "Recent Cyberattacks Require Us All to Be Vigilant."

Federal Partner Announcements

National Cybersecurity Awareness Month

October is National Cybersecurity Awareness Month (NCSAM), which is a collaborative effort between the Cybersecurity and Infrastructure Security Agency (CISA) and its public and private partners—including the National Cyber Security Alliance (NCSA)—to ensure every American has the resources they need to stay safe and secure online while increasing the resilience of the Nation against cyber threats. This year's theme, "Own IT. Secure IT. Protect IT.," focuses on promoting personal accountability and positive behavior when it comes to cybersecurity.

CISA encourages organizations to see the NCSAM 2019 webpage and the NCSAM 2019 Toolkit for ways to participate in and promote NCSAM.

FBI IC3 Issues Alert on High-Impact Ransomware Attacks

On October 2, 2019, the Federal Bureau of Investigation (FBI) released Public Service Announcement (PSA) I-100219-PSA to warn US businesses and organizations about the threat of high-impact ransomware attacks. This PSA is an update and companion to Ransomware PSA I-091516-PSA posted on www.ic3.gov and contains updated information about the ransomware threat. ***The NTIC Cyber Center recommends reviewing both FBI PSAs and implementing the recommended mitigation strategies.***

NSA Releases Advisory on Mitigating Recent VPN Vulnerabilities

The National Security Agency (NSA) has released an advisory on advanced persistent threat (APT) actors exploiting multiple vulnerabilities in Virtual Private Network (VPN) applications. A remote attacker could exploit these vulnerabilities to take control of an affected system. ***The NTIC Cyber Center recommends reviewing the*** *NSA Cybersecurity Advisory* ***and implementing the recommended mitigation strategies.***

The US Department of Energy Hosts CyberForce Competition

The U.S. Department of Energy (DOE) continues to work towards closing the gap of cybersecurity professionals needed in the energy sector and the federal government. Building on the success of the collegiate CyberForce Competition™, a corresponding CyberForce Competition Professional Pilot Program will also be held on November 15-16, 2019, at two DOE national laboratories: Argonne National Laboratory and Pacific Northwest National Laboratory. Applicants are required to register as teams of professionals (3-5 persons). Applicants should be seeking employment, be US citizens, and be able to travel to one of the two laboratory sites. CyberForce Competition scores will be considered when hiring for current and future DOE positions.

Applications are due by Friday, October 18, 2019. Selection of the teams to participate in the Cybersecurity Professional Pilot Program will be announced by Friday, October 25, 2019.

For more information about DOE's Office of Cybersecurity, Energy Security, and Emergency Response, please visit https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response.

Current and Emerging Cyber Threats

Spam Campaign Spoofs Windows Security Alerts to Deliver Ransomware

A new malicious spam campaign sends emails that masquerade as Microsoft Windows security alerts and attempts to deliver ransomware to victims via a fraudulent Windows Security Scanner executable file. The ransomware, dubbed Lost Files, targets certain file extensions under the C:\Users folder, appends .Lost_Files_Encrypt to file names, and corrupts the files instead of encrypting them, permanently destroying the affected data. Victims infected with Lost Files will not be able to recover their data, even if they pay the $500 ransom demand. ***The NTIC Cyber Center recommends users remain vigilant for Lost Files ransomware campaigns, avoid opening unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. We also recommend administrators reference and block the associated Indicators of Compromise (IoCs) contained in Bleeping Computer's report. If you believe you have been infected with Lost Files, notify your organization's IT security team immediately so they may contain and remediate the infection. For additional ransomware mitigation strategies, please review the NTIC Cyber Center Ransomware Mitigation Guide.***

CheckM8 iOS Exploit Tool Released

An independent security researcher revealed an iOS exploit dubbed checkm8 that can be used to compromise and install unauthorized arbitrary code on affected Apple devices. Checkm8 works by leveraging a flaw in the bootrom code within an unpatchable read-only memory chip in iPhones, Apple Watches, iPads, and Apple TVs that contain an A5 to A11 processor. Apple devices containing the A12 processor or newer are not impacted by this vulnerability. It is important to note that, in order to exploit this vulnerability, threat actors would need to have physical access to the targeted device. Additionally, rebooting the device will easily clear it of any infection resulting from the exploitation of this flaw. There currently is no patch or workaround available. ***The NTIC Cyber Center recommends affected iPhone users who may be concerned that this flaw will be used to target them and their data upgrade to a newer iPhone model that contains a CPU of A12 or***

higher. If you believe your Apple device has been compromised using the checkm8 exploit, restart your device or perform a factory reset if necessary.

Vulnerabilities

Apple Remote Desktop on MacOs

Threat actors have found a way to abuse macOS systems to conduct distributed denial-of-service (DDoS) amplification attacks, a DDoS variant in which threat actors use other servers as a conduit to redirect traffic to the victim's machine. In this case, threat actors leverage the Apple Remote Management Service (ARMS) within the Apple Remote Desktop (ARD) and target internet-connected systems outside a local network without firewall protection. According to cybersecurity firm Binary Edge, approximately 40,000 macOS systems are potentially vulnerable, most of which reside on university or enterprise networks. ***The NTIC Cyber Center recommend network administrators monitor network traffic to port 3283, disable unneeded instances of ARD, or restrict remote access to macOS systems using Virtual Private Networks (VPNs) or IP address whitelisting.***

Data Breaches

Food service parent company Focus Brands has reported data breaches at numerous locations of company-owned chains including McAlister's Deli, Moe's Southwest Grill, Schlotsky's, and Hy-Vee. The company believes that malware installed on the stores' point-of-sale systems allowed cyber criminals to steal the payment card numbers, expiration dates, card verification codes, and in some cases the cardholder names of an undisclosed number of customers. Payments made from April 29 to July 22 at select McAlister's and Moe's locations and from April 11 to July 22 at select Schlotzsky's locations are believed to be at risk. At select locations of Hy-Vee stores, the compromise is believed to have affected fuel pumps between December 14, 2018 and July 29, 2019, and restaurants and drive-thru coffee shops between January 15, 2019 to July 29, 2019. ***The NTIC***

Cyber Center recommends that customers who may have made purchases at these stores during the affected time frame monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity. To determine which store locations were affected, please reference the lookup tools included in the customer notices from McAlister's, Moe's, Schlotsky's, and Hy-Vee.

TransUnion Canada announced that an unauthorized third party used a credential stuffing attack to gain access to a company web portal containing consumer credit files. Likely leveraging credentials stolen in another breach, the attacker was able to log into the portal using a business customer account and view consumer credit information including full names, dates of birth, current and past addresses, information related to credit and loan obligations, and possibly Social Insurance Numbers. ***As the threat of compromise due to credential stuffing attacks could place the data of US account holders at risk as well, the NTIC Cyber Center reminds users to use lengthy, complex, and unique passwords for each account and enable multifactor authentication on any account that offers it to avoid falling victim to credential compromise.***

For more information on credential stuffing attacks, please reference the NTIC Cyber Center's product entitled Credential Stuffing Attacks – A Growing Yet Easily Mitigated Threat.

American Express disclosed a breach that compromised an unspecified amount of customer information. Breached data included credit card numbers, full names, addresses, birthdates, and Social Security numbers. This breach is not a result of an external threat actor gaining unauthorized access to the data, but rather an insider threat – an American Express employee who accessed customer data with alleged unlawful motives. American Express launched an investigation and is partnering with law enforcement. ***The NTIC Cyber Center recommends affected American Express customers monitor their financial account statements closely, report any unauthorized or suspicious activity to their financial institutions, and remain vigilant for phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure. We also recommend affected customers consider placing a fraud alert or***

security freeze on their credit file with Equifax, Experian, or TransUnion. American Express will be offering free credit monitoring and identity protection services to affected customers. For questions or concerns, call the American Express service line at 1-855-693-2213.

Upcoming Webinars

Re-examining Your Security Posture

To cope with a constantly changing threat landscape, many organizations have unsuccessfully tried to solve their overarching cybersecurity problem by adopting a myriad of point solutions, often from a variety of vendors. This has introduced duplicative features and harmed visibility, creating an advantage for attackers who are easily able to exploit the resulting security and capability gaps.

Join us for this short webinar where we will discuss and share considerations from our subject matter experts on how to outperform, outmaneuver and outfight your adversaries.

Attendees in this webinar will learn best practices for streamlining cyber operations, such as:

- Ensuring continuous real time visibility of managed and unmanaged assets
- Building threat driven operations
- Shaping the adversary experience to build your advantage
- Building proactive, protective, predictive, reflective and reactive defense capabilities

Learn more on how your organization can Gain the Decisive Advantage in the Cyber Battle.

To register for this free webinar on Tuesday, October 15 at 11:00 AM EDT, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Grandparent scams are a type of social engineering scheme that targets senior citizens. Malicious actors pose as

grandchildren in trouble and seek to exploit grandparents' emotional responses to steal money from unsuspecting elderly victims. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Baltimore Ransomware Carngage Compounded by Local Storage

Analytic Comment: Recovery efforts in the wake of Baltimore's May 7 ransomware attack have been hampered by a lack of available backups with which to restore encrypted data. Since the city had no IT policy in place at the time of the attack to mandate the centralized backup of data, files stored locally on employees' hard drives remain inaccessible. These data recovery challenges underscore the importance of maintaining regular backups that are stored securely off the network, routinely testing and certifying the integrity of backups, ensuring all applications and systems are kept up-to-date with the latest software patches, and keeping endpoint antivirus software updated with the latest virus definitions.

Magecart Strikes More Than 2 Million Websites as More Groups Get Involved

Analytic Comment: To date, researchers at RiskIQ have identified over two million websites infected with Magecart payment skimmers, malicious code that enables the theft of customer payment card information from ecommerce stores and other websites. The number of Magecart attacks are increasing and new research suggests that cyber criminals not traditionally associated with these attacks are now using Magecart tactics as well. Malwarebytes Labs believes that the threat group Cobalt, a financial crimes network known for targeting European banking institutions, may be among such groups that have expanded their criminal footprint to include engaging in these campaigns. Research by RiskIQ and Malwarebytes Labs highlights the exponential proliferation of Magecart attacks and demonstrates that a growing number of threat actors are implementing Magecart tactics despite the increasing attention placed on exposing their methodologies and infrastructure. For more information about Magecart attacks including mitigation strategies, please see the NTIC Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Patches and Updates

Apple Releases Security Updates

Cisco Releases Security Updates

Intel Releases Security Updates

iTerm2 Update

Microsoft Releases October 2019 Security Updates

Microsoft Re-Releases Security Updates

ICS-CERT Advisories

GE Mark VIe Controller

Siemens Industrial Products (Update A)

Siemens SIMATIC IT UADM

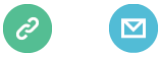
Siemens SIMATIC WinAC RTX (F) 2010

SMA Solar Technology AG Sunny WebBox

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2019-10-024

HSEC-1 | NTIC SIN No. 2.5, 5.4

October 17, 2019

National Capital Region Cyber Threat Spotlight

Domain Typosquatters Target 2020 Presidential Election Related Domains

Researchers at Digital Shadows uncovered several domain typosquatting campaigns designed to take advantage of US voters' interest in the upcoming 2020 presidential election. Domain typosquatters target visitors of popular websites by registering URLs, or website addresses, that are similar to legitimate sites but that deliberately contain typographical errors or common misspellings. If a visitor happens to enter the incorrect version of the URL, they may be delivered to a malicious website crafted to deliver malware, steal sensitive data, conduct ad fraud, or promote disinformation. Digital Shadows discovered more than 550 typosquatted election-related website domains noting that, while most sites were benign or contained content designed to tarnish a candidate's reputation, eight percent of the domains were considered misconfigured or illegitimate; some of these illegitimate sites could lead users toward scams, fraudulent browser extensions, and fraudulent program updates containing malware. ***The NTIC Cyber Center recommends users remain vigilant for malicious typosquatted domains. Network administrators should implement comprehensive and consistent IT security policies, redundancies, and cyber incident response plans that can help government agencies tackle these challenges and more effectively secure the***

US election security posture. Election community stakeholders are encouraged to correspond with CISA's #Protect2020 election security outreach campaign.

Federal Partner Announcements

CISA Releases the Updated National Emergency Communications Plan

CISA has released an update to the National Emergency Communications Plan (NECP) – the Nation's roadmap to ensuring emergency communications interoperability at all levels of government. CISA leveraged the feedback from more than 3,500 public safety representatives from federal, state, local, tribal, and territorial public safety agencies, non-governmental organizations, and other groups in revising the NECP to ensure it reflects the whole community's expertise, experience, and needs. The breadth of public safety's participation makes the NECP a key component of our Nation's preparedness.

The updated NECP:

- Builds upon the key concepts and principles of the 2008 and 2014 versions of the NECP.
- Revises the Vision statement to address secure information exchange and adds the public to acknowledge their increasing role in emergency communications.
- Emphasizes the importance of strategic and lifecycle planning and sustainable funding.
- Promotes the importance of evaluating and documenting lessons learned from training and exercises.
- Underscores the need for coordination of communications assets and capabilities at incidents and planned events.
- Emphasizes technology and infrastructure lifecycle management and focuses on effective and interoperable information sharing.
- Adds a new goal focused on cybersecurity risk management, the mitigation of cybersecurity vulnerabilities, cyber hygiene minimums, and funding.

To review the updated NECP, visit https://www.cisa.gov/necp. For questions about the NECP, contact necp@cisa.dhs.gov.

Current and Emerging Cyber Threats

Ryuk Ransomware Attacks Continue

Ecommerce and shipping company, Pitney Bowes, was the most recent target of a Ryuk ransomware campaign that disrupted their business operations. Ryuk is a ransomware variant that has been used in targeted attacks against various businesses and organizations across the globe. This variant can identify and encrypt files on shared network drives and delete Volume Shadow Copies to prevent file restoration by the victim. There is no publicly available decryption tool for this variant and, although researchers do not know how Ryuk is distributed, it is likely spread via phishing emails or Remote Desktop Protocol (RDP) compromise. Pitney Bowes is currently working with a third-party consultant to remediate the situation and does not believe that any customer accounts or data have been affected. ***The NTIC Cyber Center encourages network administrators review our Ransomware Mitigation Guide and implement the recommendations provided to reduce the risk of a ransomware infection. Additionally, we recommend network administrators proactively block the indicators of compromise (IoCs) provided in IBM's threat intelligence platform.***

Iranian Threat Group Silent Librarian Targets US and European Universities

Researchers at cybersecurity company Proofpoint reported that Silent Librarian, an Iranian Advanced Persistent Threat (APT) group also known as TA407, Cobalt Dickes, and Mabna Institute, is actively targeting universities' intellectual property via email phishing campaigns that masquerade as university library notifications. Silent Librarian sends phishing emails from compromised university accounts notifying recipients that the status of their accounts is pending due to inactivity or expiration. Recipients are then prompted to log into their accounts using a URL embedded in the body of the email that delivers them to a phishing page designed to steal their account credentials. To add legitimacy to the scheme, Silent Librarian uses university branding images in their emails and creates phishing pages that look identical to the universities' authentication portals. ***The NTIC Cyber Center recommends that all university faculty, staff, and students remain vigilant for phishing emails disguised as official library correspondence, avoid opening unexpected emails, and refrain from clicking on links or opening attachments from unknown or untrusted sources. If you receive an email that you suspect may be malicious, notify your IT security team immediately. We also recommend enabling multifactor authentication on any account that offers it to avoid falling victim to credential compromise.***

Android Apps Serving Adware Hide to Avoid Detection

Sophos researcers recently discovered 15 malicious Android apps in the Google Play Store that serve ads to users while hiding their icons to avoid detection and deletion. These apps, disguised as QR code readers, image editors, backup utilities, phone finders, and data scrubbing tools, collectively have been downloaded on over 1.3 million devices. The apps further obfuscate themselves by appearing under "phone settings" by names such as "Google Play Store," "Update," "Back Up," and "Time Zone Service." Malicious apps identified include:

Auto Cut Out
Auto Cut Out 2019
Auto Cut Out Pro
Background Cut Out New 1.8 APK
Background Cut Out Pro
Find Your Phone
Flash On Calls & Messages
Generate Elves
Image Magic
ImageProcessing
Photo Blur Background Maker 2019
QR Artifact
Read QR Code
Savexpense
Scavenger---speed guard

Google has been working to remove the offending apps from its Play Store, but malicious mobile apps remain a threat to Android users as profit-motivated criminals continue to circumvent the Google Play Store's app review process to deliver malware to victims. ***The NTIC Cyber Center recommends Android users install and use Google Play Protect, an official Android tool that scans apps for malware prior to download. After installing any new app, monitor the device for unusual behavior such as excessive power consumption, excessive data usage, unexpected pop-ups, and uninstall problematic apps immediately, performing a factory reset of the device if necessary. If the device permissions required by an app do not match the advertised functionality, refrain from installing it. We also recommend all Android users update their devices to the latest OS - Android 10 - as soon as possible. Lastly, we recommend that any Android user who has installed any of the apps listed above perform a factory reset of their device to ensure the adware and malicious content is completely removed.***

Vulnerabilities

Zero-day Vulnerability in Apple Software Update Used to Deliver BitPaymer/IEncrypt Ransomware

Security researchers at Mophisec Labs discovered that the threat actors behind the BitPaymer/IEncrypt ransomware campaign are abusing a zero-day vulnerability in Apple Software Update, a utility bundled with the Windows version of Apple iTunes, to infect and extort money

from unsuspecting victims. Apple Software Update is a mechanism that iTunes uses to deliver software updates to users. Since this utility is installed in conjunction with iTunes but maintains a separate installation file, it often remains on a system and continues to run in the background even after iTunes is uninstalled. Since the parent process in Apple Software Update is used to deliver the malicious payload, the ransomware is able to evade many behavior-based endpoint detection and response solutions. According to Mophisec, many computers spanning multiple enterprises have uninstalled iTunes years ago but they still have the outdated Apple Software Update component present. Apple has released a patch to remediate the vulnerability. ***The NTIC Cyber Center recommends system administrators remove all unneeded instances of Apple Software Update from Windows systems and immediately apply the patch for necessary instances. If you believe you have been infected with BitPaymer/IEncrypt ransomware, notify your organization's IT security team immediately so they can contain and remediate the infection. For additional ransomware mitigation strategies, please review the NTIC Cyber Center Ransomware Mitigation Guide.***

Cyberoam Firewall Vulnerability Allows Threat Actors to Compromise Targets without Passwords

A security researcher discovered a vulnerability in Sophos's Cyberoam firewall appliances that would allow threat actors to gain root access to vulnerable devices, access the target's network, and execute arbitrary commands all without a password. The vulnerability known as CVE-2019-17059 is initiated when threat actors use malicious remote commands to attack a vulnerable device's IP address, gaining access. While there is no clear number of affected devices, Sophos claimed that 99 percent of all affected devices have been patched and the remaining unpatched devices have their auto-update disabled or are not internet-facing. The vulnerability affects Sophos Cyberoam Firewall appliances running CyberoamOS (CROS) version 10.6.6 MR-5 and earlier. ***The NTIC Cyber Center recommends users monitor systems for unusual and suspicious activity. We also recommend updating the affected Cyberoam firewall appliances manually via customer support.***

Critical Vulnerability to Remain Unpatched in Several Older Models of D-Link Routers

Security researchers at Fortinet discovered a critical vulnerability in several models of older D-Link routers that will not be patched because they are no longer supported by the company. Affected devices include models DIR-652, DIR-655, DIR-866L, and DHP-1565. If exploited, the vulnerability could allow an attacker to send arbitrary input to the device interface, steal administrator passwords, install backdoors, and conduct other malicious activity. These products have reached End-of-Life (EOL) support and D-Link does not plan to release a security patch to address the vulnerability. ***As the affected routers will remain indefinitely vulnerable to malicious***

activity, the NTIC Cyber Center recommends immediately decommissioning the devices if in use and upgrading to a new device from a reputable vendor as soon as possible. We also encourage regularly auditing network environments for unsupported systems and decommissioning all EOL software and hardware as soon as possible.

Data Breaches

Online stores built with Volusion, an ecommerce business platform, were compromised resulting in stolen customer payment card data. More than 6,500 online stores are affected, the most prominent of which was the Sesame Street Live online store. Threat actors used Magecart payment skimmers, malicious code that enables the theft of customer payment card information from ecommerce stores and other websites. ***The NTIC Cyber Center recommends website visitors remain vigilant for indications that a web page may be compromised. These may include being asked twice to enter payment or login information or being prompted for payment card details before being forwarded to a secure payment service provider. In addition, customers making purchases on ecommerce platforms should routinely monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity. For more information about Magecart attacks including mitigation strategies, please see the NTIC Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.***

Online mailing and printing services company Click2Mail.com disclosed a breach of customers' personal and mailing data. Information exposed includes the names, organization names, account mailing addresses, email addresses, and phone numbers of approximately 200,000 Click2Mail customers. According to some affected customers, threat actors have already used the stolen information to target customers with spam and phishing emails. Click2Mail has begun sending notifications to affected customers and invites those with inquiries to contact 1-866-665-2787. ***The NTIC Cyber Center recommends Click2Mail customers remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text message, or other***

avenues as a result of this data exposure.

A security researcher identified a breach of data belonging to 221,130 users of the US job search platform Authentic Jobs. Information exposed includes the names, addresses, email addresses, phone numbers, and employment history of job-seekers who posted résumés, CVs, or other documents to the platform. The data had been publicly exposed in an improperly secured AWS cloud storage bucket and was available for anyone to see and download, though the company has since restricted access permissions to "private." The same researcher also discovered an unsecured cloud storage bucket belonging to the UK-based job search platform Sonic Jobs that contained the CVs of 29,202 users. ***The NTIC Cyber Center recommends that customers of Authentic Jobs or Sonic Jobs remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text message, or other avenues as a result of this data exposure.***

Upcoming Webinars

Modernize with Monitoring: Keys to Third-Party Risk Management Success

In today's shifting security and regulatory environment, ongoing third-party monitoring is crucial to compliance success. But how do you keep up with a constantly changing and growing list of vendors?

This session will outline the keys to third-party risk management success through a modern approach to monitoring vendors.

Join this session to learn how to:

- Proactively protect against third-party threats such as data breaches
- Leverage automation to keep vendor information up to date
- Reassess on an ongoing basis to meet modern compliance regulations

To register for this free webinar on Tuesday, October 22 at 2:00 PM ET, click here.

Threat Intelligence: Explained, Examined, & Exposed

Relevant threat intelligence leveraged throughout a cybersecurity strategy can help an organization reduce risk by improving detection, response, and prevention of secure critical infrastructure. Please join Sergio Caltagirone, Dragos VP, Threat Intelligence for a succinct 30 minute webinar during which he'll share his insights and real world experience hunting some of the most sophisticated threats. The webinar will be moderated by Dave Bittner, Producer and Host of The CyberWire Podcast.

We'll cover these topics and be prepared to answer your tough questions, such as:

- What is threat intelligence and why you need it
- How threat intelligence can reduce your organization's risk profile
- Vulnerable industrial assets that need protection
- Highlights from major cyber risks impacting Oil and Gas and Utilities

To register for this free webinar on Tuesday, October 22 at 11:30 AM ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Utility scams are fraudulent acts conducted by profit-motivated criminals who impersonate utility company employees to steal money or valuables from victims. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

How Texas Used Its Disaster Playbook after a Huge Ransomware Attack

Analytic Comment: Texas officials indicate that the decision to issue a disaster declaration after an August ransomware attack affected 23 municipalities played a critical role in enabling the state to coordinate a response to the cyber attacks. The declaration allowed the activation of the State Operations Center and facilitated the coordination between the Department of Information Resources, the Texas Department of Emergency Management, the National Guard, Texas A&M University, and other organizations. Furthermore, officials also credit the state's cyber attack response plan for providing guidance and instruction and ensuring a controlled response to the attacks. The Texas ransomware incidents highlight the need to maintain basic cyber hygiene, such as installing security patches and maintaining strong password policies, and underscore the utility of preparing a response plan in advance that can be quickly referenced in the event of a major cyber incident.

11 Steps Organizations Should Take to Improve Their Incident Response Strategy

Analytic Comment: There are several basic steps that all organizations can take to improve their incident response strategy and become more resilient against a cyber attack. In advance of an incident, it is important to assign organizational roles, retain external legal, public relations, and technical support, study reporting requirements, and perform tabletop exercises to identify process gaps. In the event of a cyber incident, it is important to clearly communicate the impact of the event to all interested or affected stakeholders. After an incident, it is essential to address the reasons why the incident occurred, critique and learn from your organization's response, and share key findings and takeaways with others. These steps are simple but effective; using them to develop a proactive incident response strategy puts organizations in a better position to effectively respond to and mitigate the effects of cyber attacks.

Patches and Updates

Adobe Releases Security Updates for Multiple Products

Google Releases Security Updates for Chrome

Juniper Networks Releases Security Updates

Multiple Vulnerabilities in Pulse Secure VPN

Oracle Releases October 2019 Security Bulletin

VMware Releases Security Update for Harbor Container Registry for PCF

WordPress Releases Security Update

ICS-CERT Advisories

Interpeak IPnet TCP/IP Stack (Update A)

Interpeak IPnet TCP/IP Stack (Update B)

Philips Brilliance Computed Tomography (CT) System (Update A)

Siemens Industrial Products Local Privilege Escalation Vulnerability (Update I)

Siemens Industrial Real-Time (IRT) Devices

Siemens PROFINET Devices

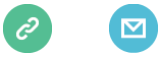
Siemens SIMATIC PCS7, WinCC, TIA Portal (Update D)

Siemens SIMATIC WinCC and PCS7 (Update C)

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2019-10-027

HSEC-1 | NTIC SIN No. 2.5, 5.4

October 24, 2019

National Capital Region Cyber Threat Spotlight

Organizations Accidentally Upload Sensitive Files to VirusTotal

Security researchers at Otorio reported that organizations are unintentionally uploading sensitive and confidential files in VirusTotal, a free online file and URL scanning platform owned by Google's parent company Alphabet. Otorio's research reveals organizations are uploading unprotected files such as blueprints and intellectual property from a range of industries such as automotive, industrial, food and pharmaceutical. In the wrong hands this data can reveal vulnerabilities. VirutTotal's terms of service states the following:

> IF YOU DO NOT WANT TO PUBLICLY SHARE A SAMPLE IN THE MANNER SET OUT IN THESE TERMS OR IN THE PRIVACY POLICY, DO NOT SEND IT/CONTRIBUTE IT TO THE SERVICE AS THE SERVICE IS DESIGNED TO WORK THROUGH THE COLLECTIVE AGGREGATION AND SHARING OF THREAT-INTELLIGENCE WITH AND THROUGH THE COMMUNITY.

Virus total allows their data to be analyzed by academic researchers and cyber security firms after thorough vetting and meeting select criteria. Otorio has does not have any evidence indicating that uploaded files have been used for malicious purposes. ***The NTIC Cyber Center recommends users to avoid uploading sensitive and confidential files in VirusTotal and to only vet files with approved software provided by your IT security team. We also recommend reviewing and comprehending the terms of service before using any service.***

Federal Partner Announcements

Microsoft Ending Support for Windows 7 and Windows Server 2008 R2

On January 14, 2020, Microsoft will end extended support for their Windows 7 and Windows Server 2008 R2 operating systems. After this date, these products will no longer receive free technical support, or software and security updates. Organizations that have regulatory obligations may find that they are unable to satisfy compliance requirements while running Windows 7 and Windows Server 2008 R2.

Technical Details:

All software products have a lifecycle. “End of support” refers to the date when the software vendor will no longer provide automatic fixes, updates, or online technical assistance. For more information on end of support for Microsoft products see the Microsoft End of Support FAQ.

Systems running Windows 7 and Windows Server 2008 R2 will continue to work at their current capacity even after support ends on January 14, 2020. However, using unsupported software may increase the likelihood of malware and other security threats. Mission and business functions supported by systems running Windows 7 and Windows Server 2008 R2 could experience negative consequences resulting from unpatched vulnerabilities and software bugs. These negative consequences could include the loss of confidentiality, integrity, and availability of data, system resources, and business assets.

Mitigations

The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and organizations to:

- Upgrade to a newer operating system.
- Identify affected devices to determine breadth of the problem and assess risk of not upgrading.
- Establish and execute a plan to systematically migrate to currently supported operating systems or employ a cloud-based service.
- Contact the operating system vendor to explore opportunities for fee-for-service maintenance, if unable to upgrade.

Current and Emerging Cyber Threats

Phishing Scheme Masquerades as Performance Appraisal Notifications

Security researchers recently uncovered a phishing campaign that masquerades as employee performance appraisals to steal user credentials. Threat actors send recipients spoofed human resource email correspondence requesting that recipients complete a performance appraisal. In the email body, recipients are urged to click a URL containing the supposed performance appraisal form, which forwards them to a fraudulent login page where they are prompted to enter their corporate account login credentials. ***The NTIC Cyber Center recommends users remain vigilant for performance appraisal phishing campaigns, avoid opening unexpected emails, and refrain from clicking on links or opening attachments from unknown or untrusted sources. If you receive an email that you suspect may be malicious, notify your IT security team immediately.***

Malvertising Campaign Targets Visitors of Legitimate Websites

Researchers at SlashNext discovered a malicious advertising – or malvertising – campaign attempting to infect visitors of legitimate websites, such as the New York Times, with malware. Threat actors inject digital advertisements laced with malware into legitimate distributed ad networks that display ads on numerous legitimate websites. These seemingly innocuous yet malicious ads prompt users to download utility applications. These applications are reported to spy on user behavior and run malicious third-party content within the browser. Malvertising campaigns that leverage legitimate websites to deliver malicious content are often undetected by standard automated security filters. ***The NTIC Cyber Center recommends using a reputable ad blocker when browsing the web to protect against malvertising campaigns. We also recommend refraining from downloading or installing any unexpected software, updates, or browser extensions as these can be used in conjunction with malvertising campaigns to deliver malware, such as ransomware, to victims.***

Phishing Campaign Targets Microsoft Account Credentials

Researchers at Heimdal Security identified a Microsoft email phishing campaign targeting Office365 and other Microsoft accounts. Threat actors send spoofed correspondence via email urging users to view work related documents and providing recipients with an attachment. These attachments lead recipients to fraudulent Microsoft Office365 web pages that request account login credentials. To add legitimacy to the scheme, threat actors send phishing emails from compromised accounts in the victim's contact list. ***The NTIC Cyber Center recommends users remain vigilant for phishing emails disguised as official correspondence, avoid opening unexpected emails, and refrain from clicking on links or opening attachments from unknown or untrusted sources. If you receive an email that you suspect may be malicious, notify your IT security team immediately. We also recommend administrators reference and block the associated Indicators of Compromise (IoCs) contained in Heimdal Security's post.***

Vulnerabilities

Smart Personal Assistants

Researchers at Security Research Labs (SRLabs) discovered that smart assistant platforms Amazon Alexa and Google Home have eavesdropping and phishing capabilities. Threat actors could edit characters within the backend of Alexa or Google Home applications enabling the application to remain silent while recording conversations or request user credentials for an "update requirement." While Amazon and Google vet applications during the application submission process, they neglected to vet successive app update components, allowing both smart assistant platforms to be exploitable. The existence of these capabilities was revealed last year and, since then, both Amazon and Google have employed patches. Still, researchers are constantly uncovering new workarounds. In the wake of the latest workaround, Amazon and Google implemented new patches and restated that their smart assistant platforms will never ask users for passwords. ***The NTIC Cyber Center recommends only downloading applications from trusted and vetted sources and to never share usernames or passwords with Amazon Alexa or Google Home if verbally prompted to do so.***

Fujitsu Wireless Keyboards

Researchers discovered two vulnerabilities in the Fujitsu wireless keyboard LX390 which may allow threat actors to remotely harvest keystrokes and hijack a victim's system. The first vulnerability, CVE-2019-18201, allows threat actors to intercept and decipher data sent between the keyboard and desktop from 150 feet away. While the keyboard employs data obfuscation, known as "data whitening," it is unencrypted and decipherable using specialized software. The second vulnerability, CVE-2019-18200, allows threat actors to send arbitrary commands to the desktop via relayed packet from the keyboard, potentially leading to a hijacked system. The Fujitsu wireless keyboard LX390 has reached its end-of-life (EOL) since May 2019 and a patch or workaround is not available or expected. ***The NTIC Cyber Center recommends decommissioning any unsupported or end-of-life (EOL) hardware and software. We urge affected Fujitsu wireless customers to update to a different model that is unaffected by these vulnerabilities.***

Data Breaches

Researchers from Comparitech discovered an unsecured MongoDB database belonging to the telecommunications provider, CenturyLink, containing approximately 2.8 million records of customer information. Data compromised in this breach include names, physical addresses, email addresses, phone numbers, account numbers, notification logs and conversation logs of CenturyLink customers. The database was exposed for approximately 10 months before being closed on September 17th. The exposure is attributed to a third-party communication platform used by CenturyLink. CenturyLink states that no financial information was compromised. ***The NTIC Cyber Center recommends CentryLink customers remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

Antivirus provider Avast disclosed a breach in which an unknown threat actor attempted to infect its system cleaner software, CCleaner, with malware. Avast detected the intrusion to its internal network on September 23, 2019 and believes the perpetrator has been attempting to gain access since May this year. The threat actor compromised an employee's Virtual Private Network (VPN) credentials that were not secured with multifactor authentication. Avast reset all employee credentials and changed the digital certificate to sign CCleaner updates preventing threat actors from leveraging older certificates. Avast states that CCleaner has not been infected and has released an automatic update for its CCleaner software. ***The NTIC Cyber Center recommends CCleaner users update their software to the latest version. We also recommend administrators to implement multifactor authentication on any account that offers it to avoid falling victim to credential compromise.***

Upcoming Webinars

Three Scary Questions Haunting Cybersecurity Teams This Halloween

Security teams need to constantly ask themselves three basic questions that illustrate how effective their strategies are: What do I know about my enemy? What does my enemy know about me? What do I know about myself?

During this webinar, we will explore these three questions using examples of:

- How cybercriminals exploit lackluster security teams
- How attack surfaces extend well beyond company assets
- Details security teams often overlook
- Recent leaked databases and admin credentials for sale

To register for this free webinar on Wednesday, October 30 at 8:00 PM ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Chinese phone scams are automated telephone calls that spoof official Chinese embassy or consular communications to extort money from Chinese speakers. Criminals direct these calls to phone customers with Chinese last names and to random people in locations with large populations of Mandarin speakers. Although these scammers are frequently located in China, their calls target people all over the world. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

District of Columbia Residents Most Likely to Incur Identity Theft and Fraud
Analytic Comment: Personal finance website, Wallet Hub, conducted an analysis of 10,818 data breaches between January 1, 2005 and August 31, 2019 revealing that District residents are more likely to become victims of identity theft and fraud because they are more frequently targeted than residents of other states. The analysis underscores the importance of email security because emails serve as a gateway for compromising connected accounts. These findings highlight the importance of bolstering District resident's cybersecurity posture and the need to invest in cybersecurity awareness, education, and

defensive techniques such as multifactor authentication and password managers.

Fileless Malware on the Rise

Analytic Comment: A TrendMicro report indicates that fileless attacks increased 265 percent in the first half of 2019 compared to the same time frame last year. While more conventional cyber threats require external files to be downloaded and installed, fileless attacks are stealthier because they masquerade malicious activity as routine system processes. Common security filters are far less likely to detect fileless attacks because of this. This underscores the importance for the cyber security industry to keep pace with the ever-evolving threat actors' tactics, techniques and procedures.

Patches and Updates

Google Releases Security Updates for Chrome

ISC Releases Security Advisories for BIND

Juniper Networks Releases Junos OS Security Advisory

Mozilla Releases Security Updates for Firefox and Firefox ESR

ICS-CERT Advisories

AVEVA Vijeo Citect and Citect SCADA

Horner Automation Cscape

Schneider Electric ProClima

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2019-10-056

HSEC-1 | NTIC SIN No. 2.5, 5.4

October 31, 2019

Happy Halloween from the NTIC Cyber Center!

This year, don't fall for any tricks when answering your phone, opening your email, reading your text messages, or scrolling through your social media feeds! There are monsters lurking in every corner of the Internet just waiting to sink their teeth into your personal information. There's no need to fear them, however, as a little awareness can go a long way in protecting you and your loved ones from identity theft, financial fraud, and account takeovers. To help shine a light on their wicked ways, we work hard to help our readers recognize and avoid being victimized by the most dangerous cyber scams and schemes. To learn more, please visit our Securing Our Communities blog series, available on our website. We here at the NTIC Cyber Center wish you all a happy, safe, and cybersecure Halloween!

National Capital Region Cyber Threat Spotlight

Government and Military Personnel Details Leaked in Unsecured Server Data Breach

Security researchers recently discovered a publicly accessible Elasticsearch database containing 179 gigabytes worth of sensitive data about US government and military personnel. The database, which is believed to belong to travel services company Autoclerk, contained travel arrangement details such as full names, dates of birth, home addresses, email addresses, phone numbers, dates and costs of travel, and partial credit card information. In some cases, records of hotel room numbers and check-in times as well as login credentials for other external accounts were also in the database. Autoclerk is a reservations management system owned by Best Western Hotels and Resorts Group that connects to hotel and travel platforms used by individuals worldwide. ***In light of this data exposure and until more is known about the impacts of this data breach, the NTIC Cyber Center recommends US government and military personnel remain vigilant to phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues. Furthermore, the NTIC Cyber Center recommends administrators of Elasticsearch databases reference instructions for configuring Elasticsearch cluster security to reduce the risk of unauthorized access.***

Current and Emerging Cyber Threats

DDoS Attacks and Ransom Payment Demands Impacting Financial Services Organizations

Security researchers warn that threat actors posing as the Russian cyber threat group "Fancy Bear" are targeting organizations in the financial sector with Distributed Denial of Service (DDoS) attacks and ransom payment demands. Perpetrators of the campaign send a ransom note threatening attacks if victims do not remit payment of 2 Bitcoin (~$15,000 USD). Unlike DDoS attacks that target companies' public facing websites, these attacks have been directed at companies' backend servers that are typically not protected by DDoS mitigation solutions. In addition to attacking organizations in the finance sector, the threat actors also have attempted to extort entertainment and retail companies using the same methods. ***The NTIC Cyber Center recommends end users notify their IT security teams immediately if they receive this or any other extortion email. We also encourage***

recipients to report instances of ransom demands or DDoS attacks to their local police department and the FBI's Internet Crime Complaint Center.

Android Malware Remains Despite Factory Reset

Cybersecurity company Symantec observed a new android malware variant that maintains persistence on an infected mobile device by reinstalling itself after it is uninstalled and even after a factory reset has been performed. This malware, dubbed xHelper, displays unwanted advertisements, attains and maintains hidden persistence, and serves as a dropper that delivers additional malware to an infected system. Symantec estimated that xHelper has compromised over 45,000 Android devices. While the initial infection vector is uncertain, some researchers suggest that xHelper may be bundled with other miscellaneous apps downloaded from a third-party application store. Once installed, xHelper will launch itself as a self-contained service without a visible app icon seen on the launcher. ***The NTIC Cyber Center recommends that users only download applications from trusted and vetted sources, keep device operating systems up to date, and backup data on mobile devices regularly. In addition, before installing any app, exercise caution and research both the app itself and the developer. Once an app is installed, monitor the app's requests for permission authorizations and data activity.***

Raccoon Infostealer Malware Popular in Underground Markets

Cybereason researchers recently discovered a new malware variant, dubbed Raccoon Infostealer, Mohazo, and Racealer, that pilfers credit card data, login credentials, emails, cryptocurrency wallets, screenshots, browser data, and system information. Raccoon Infostealer is distributed via phishing campaigns, bundled malware, and exploit kits and can delete itself from the infected system after it exfiltrates data. The malware has gained popularity in underground markets and is offered as a "as a service" to anyone willing to pay a monthly $200 subscription fee lowering the barrier to entry for threat actors who do not have technical skills. ***The NTIC Cyber Center recommends users remain vigilant for the Raccoon Infostealer, avoid opening unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. We also recommend network administrators reference and block the associated Indicators of Compromise (IoCs) contained in Cybereason's report. If you believe you have been infected with Raccoon Infostealer, notify your organization's IT security team immediately so they may contain and remediate the infection.***

Phishing Campaign Targets Humanitarian Organizations

Researchers at cybersecurity firm Lookout discovered a phishing campaign targeting non-government humanitarian organizations such as the United Nations and UNICEF. The infrastructure used in this phishing campaign has been active since March 2019 and is capable of detecting when

victims are using a mobile device to visit the phishing pages to tailor the content. The phishing pages are also capable of capturing any data entered into its fields, regardless of whether or not the victim presses the associated login button. During select timeframes, the phishing pages used legitimate SSL certificates to appear secure. ***The NTIC Cyber Center recommends users remain vigilant for humanitarian phishing campaigns, avoid opening unexpected emails, and refrain from clicking on links or opening attachments from unknown or untrusted sources. We also recommend administrators reference and block the associated Indicators of Compromise (IoCs) contained on Lookout's website.***

Cash App Scam Promises Money

Researchers at Tenable discovered a Cash App scam in which scammers targeting users on Instagram, Twitter and YouTube are leveraging legitimate Cash App promotional campaigns with "money flipping" scams that promise a large return on investments. Scammers use the same hashtags as those that are used in legitimate Cash App campaigns to lure unsuspecting victims to profiles that request cash transfers with the promise of a larger sum of money in return. Once the scammers receive the money, however, they default on their promise of payment and often ask victims for additional funds. In the YouTube variation, scammers advertise "secret" methods to earn "free money" from Cash App. However, this is merely a ruse designed to trick victims into downloading malicious applications. ***The NTIC Cyber Center recommends Cash App users remain vigilant for money flipping scams and refrain from sending money to unknown accounts, clicking on unsolicited links, or downloading applications from unknown or untrusted sources.***

Malicious Apps Discovered on Apple's App Store

Security researchers at Wandera recently discovered 17 malicious apps in the Apple App Store that are infected with clicker Trojan malware. These apps, comprising productivity tools, platform utilities, and travel apps, perform fraud-related tasks without user interaction to generate ad revenue for an attacker or to inflate website traffic. Malicious apps identified include:

RTO Vehicle Information
EMI Calculator & Loan Planner
File Manager – Documents
Smart GPS Speedometer
CrickOne – Live Cricket Scores
Daily Fitness – Yoga Poses
FM Radio – Internet Radio
My Train Info – IRCTC & PNR (not listed under developer profile)
Around Me Place Finder
Easy Contacts Backup Manager
Ramadan Times 2019
Restaurant Finder – Find Food
BMI Calculator – BMR Calc
Dual Accounts
Video Editor – Mute Video
Islamic World – Qibla
Smart Video Compressor

Apple is working to remove the offending apps from its App Store, but malicious mobile apps remain a threat to mobile device users as profit-motivated criminals continue to circumvent marketplace review processes to deliver malware to victims. ***The NTIC Cyber Center recommends Android users install and use Google Play Protect, an official Android tool that scans apps for malware prior to download. After installing any new app, monitor the device for unusual behavior such as excessive power consumption, excessive data usage, unexpected pop-ups, and uninstall problematic apps immediately, performing a factory reset of the device if necessary. If the device permissions required by an app do not match the advertised functionality, refrain from installing it. We also recommend all Apple users update their devices to the latest operating system – iOS 13—as soon as possible. Lastly, we recommend that any Apple user who has installed any of the apps listed above perform a factory reset of their device to ensure the adware and malicious content is completely removed.***

Vulnerabilities

Smart Pet Feeders

A security researcher discovered vulnerabilities in Xiaomi FurryTail smart pet feeders that can allow threat actors to change a pet's feeding schedule without a password and create an Internet of Things Distributed Denial of Service (IoT DDoS) botnet. The application programming interface (API) allows threat actors to view all Xiaomi FurryTail pet feeders and modify feeding schedules. Vulnerabilities within the embedded ESP8266 WiFi chipset allows threat actors to install new firmware which could be leveraged for an IoT DDoS botnet. Xiaomi has acknowledged the findings and stated they will release a patch. ***The NTIC Cyber Center recommends Xiaomi FurryTail smart pet feeder users monitor systems for unusual and suspicious activity. We also recommend updating the Xiaomi FurryTail smart pet feeders if and when a patch becomes available.***

Data Breaches

A security researcher discovered an exposed database containing over seven million records of Adobe Creative Cloud account holders. The database, which was left unsecured without a password, included information such as email addresses, account creation date, Adobe products used, subscription status, Adobe employment status, member IDs, country, and time since last login. ***Although the exposed data did not contain payment information or passwords, the NTIC Cyber Center nevertheless recommends that, as a result of this data exposure, Adobe Creative Cloud users remain vigilant for an increase in phishing attempts perpetrated through email, social media, or other avenues.***

A security researcher indicates that threat actors successfully targeted the ecommerce site of the American Cancer Society using Magecart payment skimming attacks. By infecting the site with malicious code, attackers were able to steal customer payment card information from any visitor who entered data on the cancer.org online store on or around October 24, 2019. The researcher has reported the issue to the American Cancer Society, but the skimmer may still be active. ***The NTIC Cyber Center recommends that customers who may have recently entered information on the American Cancer Society's page monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity. For more information about Magecart attacks including mitigation strategies, please see the NTIC Cyber Advisory titled*** *Magecart: A Rapidly Growing Threat to Ecommerce Websites*.

Retail chain Bed Bath and Beyond has announced a breach of data affecting less than one percent of all online customer accounts. According to a report, a third-party used email and password information to access customer accounts. At this time, the company has not disclosed what information was accessed, though they do not believe that customer payment card information was compromised during this incident. Bed Bath and Beyond says it has "implemented remedial measures" and has notified affected customers of this breach. ***The NTIC Cyber Center recommends affected Bed Bath and Beyond online customers remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues.***

A researcher at Sanguine Security discovered that Procter & Gamble's online beauty store, First Aid Beauty, was compromised, resulting in stolen US customer payment card data. While it is unclear how many online customers were affected, First Aid Beauty has been compromised since May 5, 2019 and the site has had approximately 100,000 monthly visitors since that time. Threat actors used Magecart payment skimmers, malicious code that enables the theft of customer payment card information from e-commerce stores and other websites. ***The NTIC Cyber Center recommends website visitors remain vigilant for indications that a web page may be compromised. These may include being asked twice to enter payment or login information or being prompted for payment card details before being forwarded to a secure payment service provider. In addition, customers making purchases on e-commerce platforms should routinely monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity. For more information about Magecart attacks including mitigation strategies, please see the NTIC Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.***

Security news website KrebsOnSecurity reports that domain name registrar Web.com was the victim of a data breach that also affected subsidiary companies NetworkSolutions.com and Register.com. According to the notice posted on their website, Web.com discovered on October 16, 2019 that a third-party gained unauthorized access to the company's computer systems in late August 2019. Web.com hired an independent cybersecurity firm to investigate and determined that the data of current and former customers may have been accessed including names, addresses, phone numbers, email addresses, and service information. They maintain that no credit card information was compromised and have forced password resets to affected accounts. ***The NTIC Cyber Center recommends affected Web.com, Register.com, and NetworkSolutions.com customers change their account passwords immediately, enable multifactor authentication if available, and remain vigilant for an increase in phishing attempts perpetrated through email, telephone, text messages, or other avenues.***

Upcoming Webinars

BANK INFO SECURITY®

A New Strategy for Effective Cyber Security Awareness Campaigns

The best way to change user behavior and create a culture of enhanced security awareness is through a comprehensive security program that leverages a wide variety of tools and techniques. During this webinar, we'll explore how organizations can develop a fit-for-purpose cyber awareness strategy that engages employees, reduces risk, and ultimately helps create a culture of cyber security awareness.

Join this webinar to learn more about developing a new security ethos in your organization, including:

- How to identify the key aspects of an effective cyber security awareness campaign
- How to build momentum for an awareness campaign
- The importance of security frameworks and data protection
- What methods can be employed to engage senior executives and obtain support for awareness campaigns

To register for this free webinar on Wednesday, November 6 at 8:00 AM ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Social Security number (SSN) suspension scams are a type of government imposter scam in which perpetrators identify themselves as representatives of the Social Security Administration and attempt to convince victims that their SSNs have been suspended due to suspicious or criminal activity. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

DHS Is Mulling an Order That Would Force Agencies to Set Up Vulnerability Disclosure Programs
Analytic Comment: The Department of Homeland Security (DHS) is considering issuing a Binding Operational Directive (BOD) that, if implemented, would mandate vulnerability disclosure programs for federal civilian agencies. These programs would require agencies to allow outside security researchers to search for and report vulnerabilities in government websites and software programs. DHS's draft of the BOD outlines principles that agency disclosure programs should follow, including protections for security researchers, expectations for agencies to mitigate vulnerabilities found, and the scope of assets that disclosure programs should cover. Mandatory vulnerability disclosure programs are intended to help increase the security of agencies' cyber infrastructure and may help government entities identify security issues faster than malicious hackers can exploit them.

TikTok Raises National Security Concerns in Congress as Schumer, Cotton ask for Federal Review
Analytic Comment: Two members of Congress have asked the US Intelligence Community to review the Chinese-owned social networking app TikTok for potential counterintelligence and national security risks. TikTok, which has been downloaded 110 million times in the United States alone, is a widely popular platform that allows users to share short videos. Congress members have questioned the app's data-collection practices and ties to the Chinese government, raising concerns about the location information collected on users, where that information is stored, the app's ability to suppress sensitive political content, and the parent company's possible support of and cooperation with Chinese government intelligence work. US lawmakers also fear that TikTok could be used in foreign influence campaigns similar to those waged through social media platforms during the 2016 election. The inquiry sheds light on counterintelligence and foreign influence concerns that are likely to arise as the 2020 elections approach and should serve as a reminder for social media users to exercise caution when sharing any information via social networking platforms.

Patches and Updates

Apple Releases Security Updates

Mozilla Releases Security Update for Thunderbird

MS-ISAC Releases Advisory on PHP Vulnerabilities

MS-ISAC Releases EOS Software Report List

Samba Releases Security Updates

Samsung Releases Galaxy S10 Update

ICS-CERT Advisories

AVEVA Vijeo Citect and Citect SCADA

Honeywell IP-AK2

Horner Automation Cscape

Moxa IKS, EDS (Update A)

Philips IntelliSpace Perinatal

PHOENIX CONTACT Automation Worx Software Suite

Rittal Chiller SK 3232-Series

Schneider Electric ProClima

Siemens Industrial Real-Time (IRT) Devices

Siemens PROFINET Devices

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2019-11-007

HSEC-1 | NTIC SIN No. 2.5, 5.4

November 7, 2019

National Capital Region Cyber Threat Spotlight

First BlueKeep Exploitation Observed in Cryptocurrency Miner Campaign

Security researchers observed the first mass malware distribution campaign that leverages BlueKeep, a vulnerability that affects the Windows Remote Desktop Protocol (RDP) service and allows a remote attacker to execute arbitrary commands on an exploited machine. Until now, BlueKeep had not been used extensively for attacks in the wild and was previously only demonstrated as a proof of concept. However, researchers recently discovered BlueKeep attacks compromising vulnerable honeypot servers. Fortunately, these attacks only resulted in the installation of a cryptocurrency miner onto the servers; they have not yet been observed spreading from one computer to the next. Researchers do fear, though, that this vulnerability could eventually be used in a global, wormable outbreak similar to the NotPetya or WannaCry incidents of 2017.

In May, 2019, Microsoft released patches to address the BlueKeep vulnerability. ***As BlueKeep continues to pose a threat to hundreds of thousands of Windows computers that remain***

unpatched, the NTIC Cyber Center reminds users and administrators of affected Windows operating systems to apply the available patch as soon as possible. Additionally, we recommend network administrators proactively block TCP port 3389 at the perimeter firewall to protect unpatched systems within a secured network and disable unneeded RDP services in their environment.

Chinese Cyber-Espionage Group APT41 Employs MESSAGETAP Tool to Collect SMS Messages and Call Logs

According to a recent FireEye report, Chinese advanced persistent threat group APT41 is actively targeting Linux servers with MESSAGETAP, a cyber-espionage tool used to collect SMS messages and call records of persons of interest to the Chinese intelligence community. FireEye discovered this tool within a number of Linux servers during a recent investigation at an unnamed telecommunications network provider. MESSAGETAP works by monitoring incoming and outgoing connections from the compromised server, analyzing the traffic, extracting SMS messages and then scanning them for predefined keywords. Collected SMS messages are then encrypted using the XOR cipher and stored on the compromised server as a CSV file for later retrieval. Additionally, researchers observed APT41 collecting sensitive information such as travel services and healthcare providers used by targeted individuals. FireEye recommends highly targeted individuals such as journalists, dissidents, and political officials take additional precautions to mitigate this attack by only using communication programs that employ end-to-end encryption and refrain from sending sensitive information via SMS messages as this activity is likely to continue. ***The NTIC Cyber Center recommends anyone who believes they may be a target of interest of APT41 review FireEye's report and modify their communication behavior to reduce their risk of compromise.***

Federal Partner Announcements

National Critical Infrastructure Security and Resilience Month

November is National Critical Infrastructure Security and Resilience Month. The Nation's critical infrastructure (CI) relies on a highly interdependent environment, in which physical and cyber systems converge. CI plays a vital role in keeping our Nation and communities safe and secure. Everyone is involved in the mission to protect CI and can help by using cybersecurity best practices, reporting cybersecurity incidents and phishing attempts, and submitting malware for review.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages critical infrastructure owners and operators to download the Critical Infrastructure Security and Resilience Month Toolkit and to visit CISA's Critical Infrastructure Security and Resilience Month resource page throughout November for information and updates.

CSET Version 9.2 Now Available

The Cybersecurity and Infrastructure Security Agency (CISA) has released version 9.2 of its Cyber Security Evaluation Tool (CSET). CSET is a desktop software tool that guides asset owners and operators through a consistent process for evaluating control system networks as part of a comprehensive cybersecurity assessment that uses recognized government and industry standards and recommendations.

CSET 9.2 includes the following feature enhancements and upgrades:

- Web-based diagram editor
- Enhanced reporting
- New capability maturity model for financial sector customers
- National Credit Union Administration (NCUA) Automated Cybersecurity Examination Tool (ACET) Standard
- Financial sector risk assessment wizard
- New analysis for network diagram questions
- Transportation Security Administration (TSA) 2018 Pipeline security standard
- International Society of Automation (ISA)/International Electrotechnical Commission (IEC) 62443 standards

CISA encourages users to update to CSET version 9.2, available at github[.]com/cisagov/cset/wiki.

Current and Emerging Cyber Threats

Two New Phishing Campaigns Target Microsoft Office 365 Account Credentials

Two new phishing campaigns are currently targeting Microsoft Office 365 account credentials. In the first campaign, fraudulent emails appear to originate from Microsoft and claim that a voicemail is waiting to be retrieved from the server. When recipients open the file attached to the email, a recording begins to play and the file redirects recipients to a phishing page that prompts them to enter their Microsoft Office 365 usernames and passwords in order to listen to the rest of the voicemail message.

In the second campaign, attackers use the promise of a salary increase to lure recipients into clicking a phishing link embedded in the malicious email. If clicked, recipients are redirected to a phishing landing page designed to collect Microsoft Office 365 account credentials. These malicious emails are crafted to look as though they originate from the human resources department of the organizations where the recipients work and contain a link that appears to open an Excel spreadsheet containing recipients' salary details.

As Microsoft Office 365 account credentials continue to be an attractive target for cyber threat actors, the NTIC Cyber Center would like to remind our readers to never open attachments or click links contained within unexpected or unsolicited emails. Additionally, never enter login credentials for any account into a website that originated from a link in an email, text message, or social media message. Lastly, we recommend enabling multifactor authentication on every account that offers it to avoid falling victim to credential compromise.

New QSnatch Malware Targets QNAP NAS Devices

A new malware campaign is actively targeting QNAP Network Attached Storage (NAS) devices with a malware variant dubbed QSnatch. Once QSnatch locates vulnerable and exposed QNAP NAS devices, it steals device credentials, retrieves malicious code from the attacker's command-and-control (C2) servers, and injects it into the devices' firmware. The modified firmware can then be used to prevent additional firmware updates, modify operating system timed jobs and scripts, and load additional malware and features. The exact vulnerability that QSnatch exploits to infect these devices is currently unknown; however, infections can be removed by performing a full factory reset, which will also erase all data stored on the compromised NAS device. ***The NTIC Cyber Center recommends all owners and administrators of QNAP NAS devices immediately apply QNAP's latest patch, place NAS devices behind a firewall, disable unneeded SSH and Telnet connections, use lengthy, complex, and unique administrator credentials, and regularly monitor***

devices for unauthorized user accounts and access. For more information, please review QNAP's Security Advisory.

NFC on Android Devices Exploited to Deliver Malware

A security researcher discovered an Android vulnerability that allows threat actors to place malware on Android devices via NFC (Near-Field Communication) on Android versions 8.0 and above. The vulnerability, known as CVE-2019-2114, is initiated when threat actors leverage NFC beaming, normally used for file sharing, to send malicious apps to a target device that bypasses typical security prompts, enabling users to download malware with one press. While, in most cases, Google provides security prompts when non-Google Play Store apps or apps from "unknown sources" are about to be downloaded, certain application sources have been whitelisted such as Google Chrome or Android Dropbox, which can be used to deliver malicious payloads to the target device. Google has released a patch. ***The*** NTIC Cyber Center recommends Android users update all Android devices to the latest operating system version and disable the NFC feature when not in use.

New Gafgyt Malware Targets Zyxel and Huawei Routers to Conduct DDoS Attacks

Security researchers at cybersecurity firm Palo Alto recently discovered a new Gafgyt botnet malware variant targeting Zyxel routers, Huawei routers, and exposed devices that contain the Realtek RTL81xx chipset. Although Gafgyt malware has been active and used to conduct distributed denial-of-service (DDoS) attacks since 2014, this new variant has been updated to exploit the following vulnerabilities: CVE-2017-18368, CVE-2017-17215, and CVE-2014-8361. The malware is used to conduct various simultaneous DDoS attacks to target any system that runs the Valve Source video game engine, and the cyber threat actors behind the campaign are currently advertising DDoS services on popular social media platforms at a low cost. ***The NTIC Cyber Center recommends administrators of affected devices have the latest patches installed, use lengthy, complex, and unique administrator credentials, and monitor devices and network traffic for anomalies and other unauthorized activity. We also recommend proactively blocking the associated indicators of compromise (IoCs) provided in Palo Alto's report.***

WordPress and Blogger Websites Targeted in Latest Sextortion Scam

Security researchers report that scammers are hacking WordPress and Blogger websites to post sextortion messages disguised as security alerts. In these messages, scammers threaten website visitors with the release of compromising video content if they do not remit payment of $776 in Bitcoin. As is the case in most sextortion scams, however, there is no such content recorded; scammers are simply seeking to scare potential victims into paying the extortion fee. It is not

currently known how the sites are being hacked, though researchers believe scammers may be using credential stuffing attacks to gain access to blog sites and post sextortion messages. ***The NTIC Cyber Center would like to remind our members to ignore sextortion scam attempts. We also encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication on any account that offers it to limit the impact of credential compromise. For more information on sextortion scams, please review our product titled Securing Our Communities: Sextortion Scams.***

Vulnerabilities

Horde Webmail

A security researcher has identified several vulnerabilities in the open source webmail software Horde that enable attackers to access users' inboxes. By tricking victims into opening a malicious link, an attacker can scrape a victim's inbox and exfiltrate its entire contents to an attacker-owned server. While an update to the latest version of Horde webmail fixed several related security issues, the critical vulnerabilities that allow for the theft of user emails (outlined in CVE-2019-12095) remain unpatched and continue to affect all versions of the software. ***The NTIC Cyber Center recommends administrators of Horde webmail systems suspend the use of the email client within their network environments until a patch becomes available.***

Some Smart Devices Vulnerable to Laser "Light Commands"

Researchers at the University of Michigan and University of Electro-Communications in Tokyo discovered a technique dubbed "light commands" that can allow threat actors to utilize laser pointers to hijack voice-activated smart devices, such as smart home assistants and smart phones. Threat actors can use this exploit to command these voice-activated devices to visit websites, unlock doors, and start vehicles. Focused lasers can trigger voice-activated devices that use micro-electro-mechanical systems (MEMS) within microphones in the same manner as sound. While it is currently unclear how and why lasers affect MEMS in same manner, researchers were able to conduct a malicious attack from 360 feet away. ***The NTIC Cyber Center recommends that users enable authentication on any device that offers it and to be mindful of the location of their microphone-enabled smart devices if they believe they may be at risk of this threat.***

Data Breaches

Marriott disclosed a data breach that resulted in the exposure of personal information of an unknown number of associates. According to Marriott's notification, an unauthorized third party accessed information stored on the network of a third-party vendor that processed official documents such as subpoenas and court orders for the company. Information exposed in the data breach includes associates' names, addresses, and Social Security numbers. ***The NTIC Cyber Center encourages those affected to place a fraud alert or security freeze on their credit file with Equifax, Experian, or TransUnion. In addition, we advise activating the free credit monitoring and identity protection services offered to affected associates. For questions or concerns, please call Marriott's dedicated service line at 1-833-281-4825.***

Upcoming Webinars

Office 365 Forensics and Business Email Compromises

This webinar will discuss the types of evidence that should be collected in a response to a business email compromise/Office 365 email investigation. Topics will include methods of email compromise (phishing, malware, brute force attacks, external compromise/credential stuffing), types of data at risk, and commonly seen schemes, along with:

- A review of the Office 365/Azure Admin Centers
- Collecting evidence from Office 365 (logs, rule/forwarding/ Sharepoint/Onedrive data)
- Extracting mailboxes with the Office 365 eDiscovery tool
- Analyzing and interpreting the types of log data available in Office 365
- Steps to secure the Office 365 environment during an incident

To register for this free webinar on Wednesday, November 13 at 1:00 PM ET, click here.

Making Security Part of the Business Team

With record breaches, regulatory action, and GDPR fines in the news almost weekly now, security needs to be at the forefront of all digital business projects. However, a recent International Data Group (IDG) study found that only 42 percent of CISOs are involved in those projects from the very beginning.

Register for this live webinar and learn about:

- Why CISOs should build collaborative bridges beyond tech and IT
- How security management can boost business outcomes
- Creating a holistic approach to security throughout the business

To register for this free webinar on Tuesday, November 12 at 2:00 PM ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Two-factor authentication (2FA) scams are a type of man-in-the-middle phishing scheme in which criminals masquerade as customer service representatives to trick victims into revealing verification codes designed to authenticate account holders and prevent unauthorized access to online accounts. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Brooklyn Hospital Center Malware Attack Results in Loss of Patients' Health Records

Analytic Comment: A July 2019 ransomware attack affecting servers at Brooklyn Hospital Center in New York resulted in the permanent loss of certain patient information. Following two months of exhaustive recovery efforts, a third-party forensics firm was ultimately unable to restore data, including some patients' dental and cardiac images, from an encrypted state. Brooklyn Hospital's data recovery challenges underscore the importance of maintaining regular backups stored securely off the network, routinely testing and certifying the integrity of backups, ensuring all applications and systems are kept up-to-date with the latest software patches, and keeping endpoint antivirus software updated with the latest virus definitions.

Cybersecurity: Under Half of Organizations Are Fully Prepared to Deal with Cyber Attacks

Analytic Comment: A recent Fireye report states that 51 percent of organizations are not confident in their ability to handle a cyber-related attack. Additionally, 29 percent of organizations have outdated plans or untested cyber threat response plans even though most organizations believe that cyber threat incidents will increase in 2020. These findings underscore the importance of dynamic and updated cyber incident response plans and training that can adapt with the ever-evolving cyber threat landscape.

GandCrab RaaS Was a Training Ground for Malware Distributors

Analytic Comment: Many ransomware infections are more than just random, opportunistic attacks used by individual hackers to make a few dollars. For organized and experienced cybercriminals, ransomware can be a lucrative business model, especially when they encourage others to propagate their malware through turn-key affiliate programs that require little to no technical knowledge to implement. By creating the ransomware variant and selling access to ready-made kits or taking a percentage of the ransom paid by victims, malware developers can reduce their risk of being arrested while still making a tidy profit. Unfortunately, the Ransomware-as-a Service (RaaS) business model makes it far too easy for low-skilled hackers to conduct these types of attacks and guarantees that this threat is here to stay.

Patches and Updates

CSET Version 9.2 Now Available

Google Releases Security Updates for Chrome

ICS-CERT Advisories

Advantech WISE-PaaS/RMM

Honeywell equIP and Performance Series IP Cameras

Honeywell equIP and Performance Series IP Cameras and Recorders

Honeywell equIP Series IP Cameras

Interpeak IPnet TCP/IP Stack (Update C)

Omron CX-Supervisor

Omron Network Configurator for DeviceNet (Update A)

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2019-11-018

HSEC-1 | NTIC SIN No. 2.5, 5.4

November 14, 2019

National Capital Region Cyber Threat Spotlight

Foreign Intelligence Services Abuse LinkedIn to Obtain Confidential Information from Legitimate Users

Law enforcement officials warn that foreign intelligence services are abusing the LinkedIn social media platform to obtain confidential information such as government secrets and intellectual property from unsuspecting, legitimate LinkedIn users. These threat actors use fraudulent profiles and build phony networks of accounts to target real LinkedIn users, often sending thousands of connection requests at a time. LinkedIn accounts displaying information such as security clearances and positions of power or influence within large organizations are particularly at risk of being targeted. LinkedIn is aware of the abuse and, between January and June in 2019, the social media platform claims to have taken action against 21.6 million fraudulent accounts, preventing many of them from becoming fully registered accounts. Although LinkedIn uses artificial intelligence and machine learning to help it distinguish between legitimate and fraudulent accounts, some accounts still slip under the radar and put real users at risk. ***The NTIC Cyber Center recommends LinkedIn users limit the amount of personal and professional information they share online through this and other social media platforms and refrain from listing information such as their clearance status or their ability to access sensitive and confidential information. We also recommend all***

social media users remain wary of unsolicited social media messages received from people they do not know and regularly check and tighten privacy settings on these platforms.

Federal Partner Announcements

Holiday Shopping, Phishing, and Malware Scams

As this holiday season approaches, the Cybersecurity and Infrastructure Security Agency (CISA) encourages users to be aware of potential holiday scams and malicious cyber campaigns, particularly when browsing or shopping online. Cyber actors may send emails and ecards containing malicious links or attachments infected with malware or may send spoofed emails requesting support for fraudulent charities or causes.
CISA encourages users to remain vigilant and take the following precautions:

- Avoid clicking on links in unsolicited emails and be wary of email attachments (see Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams).
- Use caution when shopping online (see Shopping Safely Online).
- Verify a charity's authenticity before making donations. Review the Federal Trade Commission's page on Charity Scams for more information.

Training Opportunity

Palo Alto Networks Offers Free Cybersecurity Training to Veterans

Cybersecurity company Palo Alto Networks has launched a free cybersecurity training and certification program for military veterans. This program, called Second Watch, aims to provide veterans with practical skills for transitioning into careers in cybersecurity. Second Watch is comprised of nine self-paced steps that guide students through digital learning courses to prepare for the free Palo Alto Networks Certified Network Security Administrator (PCNSA) exam. The Second Watch program also offers free employment resources for veteran job seekers. ***The NTIC Cyber***

Center encourages interested military veterans to review Palo Alto's Second Watch program for more information on this no-cost cybersecurity training and certification initiative.

Current and Emerging Cyber Threats

Webex Phishing Campaigns Abuse Cisco Open Redirect to Deliver RAT

Security researchers warn that attackers are using spoofed WebEx meeting invitations and open redirect vulnerabilities to infect recipients with Remote Access Trojan (RAT) malware. Open redirect vulnerabilities allow attackers to construct web addresses that appear legitimate but instead divert visitors to malicious destinations. In this campaign, fraudulent WebEx meeting invitation emails feature carefully crafted links that redirect from a legitimate Cisco domain to point recipients to a site spoofing the Cisco Webex website. When users follow prompts to start the meeting, a malicious executable file disguised as a Webex installer automatically downloads and installs the RAT malware, giving attackers full remote access to victims' computers. Abuse of open redirect vulnerabilities adds legitimacy to spam emails and increases the likelihood that unsuspecting users will visit associated fraudulent login pages or other harmful websites. ***The NTIC Cyber Center advises email recipients to remain vigilant for malicious links that redirect from other domains, avoid opening unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources.***

For more information about open redirect vulnerabilities, including tips for web administrators on how to mitigate these risks, please see our recent Cyber Advisory entitled Open Redirect Vulnerabilities Facilitate Malicious Cyber Activity.

Spearphishing Emails Disguised as Sexual Harassment Complaints Distribute TrickBot Trojan

Security researchers have observed threat actors using spearphishing emails disguised as sexual harassment complaints to distribute the TrickBot information-stealing Trojan. These emails spoof correspondence from the US Equal Employment Opportunity Commission and bait recipients into opening malicious Microsoft Word documents that distribute the malware. To add legitimacy to the campaign, threat actors also include recipients' full names, names of workplaces, job titles, and phone numbers in the emails. TrickBot is often delivered through macro-enabled attachments and remains an extremely destructive malware that allows attackers to steal banking information and exfiltrate various user credentials. ***The NTIC Cyber Center recommends users remain vigilant for malicious emails disguised as sexual harassment complaints, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from***

unknown or untrusted sources. If you receive an email that you suspect may be malicious, notify your IT security team immediately.

NanoCore RAT Delivered via Attached ZIP File

Researchers at Trustwave discovered a malicious email campaign that distributes the NanoCore Remote Access Trojan (RAT) via an attached ZIP file. While NanoCore is used for stealing user information and spying on victims, threat actors can add modules or plugins to modify its functionality. In this campaign, threat actors have altered the End of Central Directory (EOCD) record within the attached ZIP archive to bypass secure email gateways. ***The NTIC Cyber Center recommends users remain vigilant for malicious email campaigns, avoid opening and unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. We also recommend administrators reference and block the associated Indicators of Compromise (IoCs) contained in Trustwave's report.***

MegaCortex Ransomware Changes Account Password

Researchers discovered a new MegaCortex ransomware variant that changes victims' Windows account password and threatens to publicly publish victims' data. This variant is often initially delivered to systems through network compromise facilitated by Trojans such as Emotet. It then spreads to other machines on the same network using post-exploitation kits or active directory controllers. Once a system is infected, MegaCortex encrypts files, appends the *.m3g4c0rtx* extension to the file names, and then drops a ransom note named *!-!_README_!-!* on the desktop. It also uses the net user command to change the Windows account password and adds a notice at the login prompt. ***The NTIC Cyber Center encourages network administrators to review our Ransomware Mitigation Guide and implement the recommendations provided to reduce the risk of a ransomware infection. Additionally, we recommend network administrators proactively block the indicators of compromise (IoCs) provided in Bleeping Computer's post.***

Vulnerabilities

Magento

Magento's security team recently warned of a remote code execution vulnerability currently affecting Magento Commerce versions 2.3.1, 2.3.2, and all unsupported versions of Page Builder. This vulnerability, tracked as CVE-2019-8144, may allow an attacker to insert and remotely execute a malicious payload on a targeted merchant's site. ***As exploiting vulnerabilities in ecommerce platforms such as Magento has proven to be a popular tactic for Magecart attackers to***

compromise websites and steal customer data, the NTIC Cyber Center advises administrators of Magento platforms to consult Magento's guidance on installing security patches to mitigate this vulnerability as soon as possible.

LEADTOOLS

Researchers at Cisco's Talos Security Intelligence and Research Group discovered four vulnerabilities within software development kits (SDK) from provider, LEADTOOLS, that could allow threat actors to conduct denial-of-service conditions and remote code execution. CVE-2019-5084 features an exploitable heap out-of-bounds write vulnerability and CVE-2019-5100 features an exploitable heap overflow vulnerability. The remaining vulnerabilities, CVE-2019-5099 and CVE-2019-5125, feature an exploitable integer overflow vulnerability. A patch is available for vulnerable versions. ***The NTIC Cyber Center recommends LEADTOOLS users to immediately apply the patch for necessary versions and to monitor systems for unusual and suspicious activity.***

Data Breaches

Facebook announced a security incident that resulted in the exposure of private group member information. According to the company, approximately 100 developers of primarily video streaming and social media management apps were inadvertently granted access to private group information such as member names and profile pictures for a period of time longer than intended. Facebook has asked developers to delete the exposed data and the company intends on conducting audits to confirm compliance with this request in the future. ***As a result of this breach and the potential for continued exposure of private group information, the NTIC Cyber Center recommends Facebook users maintain vigilant for targeted communications or phishing attempts perpetrated through social media or other avenues.***

Trend Micro disclosed a security incident in which an employee stole information and sold it to a third-party to be used in tech support scams. The employee pilfered information such as names, email addresses, ticket numbers, and phone numbers from the company's customer support database. TrendMicro has terminated the employee and is collaborating with law enforcement. Additionally, Trend Micro stated that there is no indication that financial data was compromised and

plans to notify affected customers. ***The NTIC Cyber Center recommends Trend Micro customers remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

Upcoming Webinars

How to Build a Threat Hunting Capability in AWS

Threat hunting offers proactive ways to detect anomalous behavior in your environment. Do you know how to build an effective threat hunting program in your AWS environment? In this webinar, you will learn how threat hunting differs from alerts and SOC monitoring, and what threats to look for. You will also discover real-life examples that demonstrate how threat hunters can apply cloud infrastructure best practices to reduce the noise in often chaotic environments, making it easier to detect potential events. Leveraging detailed use cases, this webinar can help you develop an effective threat hunting program.

Attendees will learn to:

- Use the Threat Hunting Loop to identify what to look for, which tools you need to analyze available data, and ways to tease out patterns that indicate potential events
- Strike the right balance of how much data to capture, identify gaps in information, and determine how best to collect that information
- Analyze logs efficiently and effectively using Amazon CloudWatch, AWS CloudTrail, and Amazon GuardDuty
- Automate the process of evaluating and enriching complex data sets by utilizing SIEM and SOAR solutions to detect possible threats

To register for this free webinar on Wednesday, November 21 at 11:00 AM ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share

this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Mortgage wire fraud, also known as a mortgage closing scam, is a type of social engineering scheme in which perpetrators steal money or elicit personally identifiable information (PII) from victims through fraudulent real estate correspondence for financial gain or identity theft. Perpetrators take advantage of the numerous steps taken and parties involved in the real estate acquisition process. They target victims using email, voice messaging services, and websites. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Major ASP.NET Hosting Provider Infected by Ransomware

Analytic Comment: Attackers recently breached the network of web hosting provider SmarterASP.net and encrypted customer data with the Snatch ransomware variant. According to some of the company's 440,000 customers, the ransomware attack rendered accounts inaccessible and encrypted customer data including website files and backend databases. Customers using SmarterASP.net's servers as a backend for synchronizing data or maintaining backups are now facing challenges in migrating impacted sites to other web hosting platforms. This ransomware attack highlights the increasing threat of cyber attacks targeting third parties such as hosting providers and should serve as a reminder for customers to maintain and store their own backups of website data and files securely off the network.

Study of Over 11,000 Online Stores Finds 'Dark Patterns' on 1,254 Sites

Analytic Comment: Dark patterns, or misleading user interface designs, are becoming increasingly common on popular websites, particularly ecommerce stores. Dark patterns are carefully crafted website features designed to trick customers into purchasing additional items, subscribing to unwanted services, or surrendering personal information. Researchers have also identified dark patterns that add hidden costs to online transactions, trick users into believing products are in high demand, make it difficult to opt out of marketing communications, and perform other deceitful or manipulative functions. As more and more websites are believed to be employing these features, we encourage online shoppers to review the NTIC Cyber Center's product titled *Securing Our Communities: Dark Patterns* to help recognize these practices and avoid being influenced by misleading user interfaces, especially as the holiday shopping season approaches.

Patches and Updates

Adobe Releases Security Updates

Cisco Releases Security Updates

Intel Releases Security Updates

Microsoft Releases November 2019 Security Updates

VMware Releases Security Updates

ICS-CERT Advisories

Fuji Electric V-Server

Medtronic Valleylab FT10 and FX8

Medtronic Valleylab FT10 and LS10

Mitsubishi Electric MELSEC-Q Series and MELSEC-L Series CPU Modules

Philips Tasy EMR (Update A)

Siemens SINAMICS (Update A)

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2019-11-021

HSEC-1 | NTIC SIN No. 2.5, 5.4

November 21, 2019

National Capital Region Cyber Threat Spotlight

Law Enforcement Warns that Free Bluetooth Scanning Apps Facilitate Theft of Electronic Devices

Law enforcement officials warn that criminals are using Bluetooth scanners to locate and steal electronic devices left in vehicles. By using free tools available for download, such as mobile phone applications, burglars can scan for the signals that Bluetooth-enabled devices emit to easily and quickly and find and steal unattended gadgets. Locating nearby devices is simple as many electronic devices today, including phones, laptops, and watches, feature Bluetooth capabilities that beacon out pairing signals making them easily trackable—even when the devices are in "sleep" or idle mode. Scanning apps can alert thieves to the presence of new devices in the area, the types of device registered, and the relative locations of devices within a few meters of accuracy. ***The NTIC Cyber Center advises users to avoid keeping electronic devices in vehicles or other locations that may be subject to theft. If such placement of devices is unavoidable, we encourage device owners to completely power down any Bluetooth-enabled electronic devices before storing them to protect against theft of the devices themselves and any and all information that may be stored on them.***

Federal Partner Announcements

Reminder: Malware Can Exploit Improper Configurations

Protect yourself from unwanted—and potentially harmful—files or programs by adhering to vendor-recommended configurations for hardware and software. Doing so in addition to maintaining regular patch maintenance, will help give your systems and networks the best security possible.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review the following tips and guidance:

- What is Cybersecurity?
- Handling Destructive Malware
- Protecting Against Malicious Code
- Understanding Patches and Software Updates
- CISA's Cyber Essentials (for small businesses and small SLTT governments)

Current and Emerging Cyber Threats

Phishing Campaign Targets Office 365 Administrators

Researchers from PhishLabs detected a new email phishing campaign targeting Microsoft Office 365 administrators in order to compromise their domain and propagate another email phishing campaign. Threat actors send fraudulent emails that masquerade as official Microsoft correspondence notifying users of an actionable alert with an embedded link in the email body. Phishing emails are sent from a spoofed domain that helps the emails bypass email security filters and reach end users. Once clicked, users are forwarded to a fraudulent Microsoft login page that request and harvest user credentials. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns disguised as official Microsoft correspondence, avoid opening unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. We also recommend blocking the associated IoCs included in PhishLabs' report.***

Pipka Card Skimmer Covers Its Tracks

Researchers from the Visa Payment Fraud Disruption (PFD) team discovered a new JavaScript payment card skimmer, dubbed Pipka, that targets site visitors' payment data. Threat actors compromised these sites with malicious code that enables the theft in at least 17 unnamed, yet popular, ecommerce sites. After the financial data is pilfered, Pipka tries to cover its tracks by removing itself from the HTML code after execution. ***The NTIC Cyber Center recommends website visitors remain vigilant for indications that a web page may be compromised. These may include being asked twice to enter payment or login information or being prompted for payment card details before being forwarded to a secure payment service provider. In addition, customers making purchases on ecommerce platforms should routinely monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.***

Cyber Threat Actors Masquerade as US Postal Service

Researchers from cybersecurity firm Proofpoint observed threat actors masquerading as the US Postal Service (USPS) to deliver malware via malicious emails. Primarily targeting the healthcare, manufacturing, and IT services sectors, threat actors tailor region-specific campaigns and bait recipients with urgent tax notifications. Included in these emails were malicious Microsoft Word attachments featuring user-activated macros distributing the IcedID banking Trojan. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns disguised as official Microsoft correspondence, disable Microsoft Office macros by default, avoid opening unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. We also recommend blocking the associated IoCs included in Proofpoint's report.***

Scammers Using Bots to Test Stolen Credit Cards

Security researchers at PerimeterX warn that cybercriminals are using carding bots to test the validity of stolen payment card details in preparation for the upcoming holiday shopping events such as Black Friday and Cyber Monday. One attack method, known as a canary carding bot attack, uses bots to make small-value purchases on ecommerce retailers' websites. Another method, known as a shortcut carding bot attack, relies on API website access to bypass the ecommerce site altogether and send card details directly to external payment processing services to determine card validity. One recommendation that PerimeterX suggests for combating the threat of carding bot attacks is for ecommerce administrators to block website visitors' access to payment pages if their online shopping carts are empty. ***The NTIC Cyber Center encourages credit card and debit card holders to monitor their account statements for any unexpected small value transactions, as such charges could signal the imminent and fraudulent usage of compromised cards, and to report any unauthorized activity to the associated financial institution.***

Ransomware Roundup

Welcome to Ransomware Roundup, a new feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

AnteFrigus

AnteFrigus is a new ransomware variant that targets systems running Windows OS and infects victims who use the Internet Explorer (IE) web browser. AnteFrigus is delivered though malicious advertising – or malvertising – campaigns that redirect them to websites hosting the RIG exploit kit designed to exploit vulnerabilities in IE. Once installed, AnteFrigus searches for and attempts to encrypt files on USB drives and mapped network drives, but does not target any files on the system's C: drive. AnteFrigus appends a random character extension to encrypted files and drops a ransom note labeled *"[extension]-readme.txt*." If the victim does not submit payment within four days of the infection, the ransom demand increases from $1995 to $3990. There is currently no free decryption tool available for this variant. More information about AnteFrigus, including IoCs, is available on the Bleeping Computer website.

NextCry

NextCry is a new ransomware variant that targets Nextcloud file hosting services. Malware analysts have determined that this variant is comprised of a Python script compiled in a Linux ELF binary using pyInstaller. Once a system is infected, NextCry searches for the victim's Nextcloud file share and sync data directory and deletes folders that the victim could use to restore encrypted files. It then encrypts all files in the data directory, appends file names with the *.nextcry* extension, and drops a ransom note named "*READ_FOR_DECRYPT*." It is currently unknown how this ransomware is distributed, but researchers suggest that a vulnerability within the default Nextcloud NGINX configuration could be to blame. Nextcloud recommends administrators upgrade their PHP packages and NGINX configuration files per their security alert. There is currently no free decryption tool available for this variant. More information about NextCry, including IoCs, is available on the Bleeping Computer website.

PureLocker

PureLocker, named after PureBasic, the programming language used to build it, is a new ransomware variant currently employed in attacks against enterprise production servers. The researchers who discovered it noted that this variant originates from a Malware-as-a-Service (MaaS) provider used by such financially-motivated cybercrime groups as Cobalt Gang and FIN6. This variant is unique in that it is capable of infecting systems running Windows, Linux, and macOS. It uses AES and RSA algorithms to encrypt files, appends *.CR1* to file names, and drops a ransom note labeled "*YOUR_FILES*" that demands victims contact the attacker via email to negotiate the ransom amount. There is currently no free decryption tool available for this variant. More information about PureLocker , including indicators of compromise (IoCs), is available on the Intezer website.

Free Jigsaw Decryption Tool Released

Researchers at cybersecurity firm Emsisoft just released a free decryption tool for victims impacted by the Jigsaw ransomware variant. This tool can decrypt 85 versions of Jigsaw and will be updated as new versions emerge. More information and a link to download the tool is available on the Emsisoft website. Additional free tools designed to decrypt files impacted by other ransomware variants are available from No More Ransom, an international initiative created to help combat ransomware.

Vulnerabilities

Jetpack WordPress Plugin

A critical security update was released for Jetpack, a third-party security-based WordPress plugin with over five million active installations. The vulnerability details are currently undisclosed. One million WordPress sites have yet to apply the update. ***The NTIC Cyber Center recommends WordPress website administrators who installed the Jetpack plugin update it to the latest version (7.9.1) immediately. Enabling two-factor authentication on website administrator accounts and properly vetting all plugins prior to and after installation is also recommended.***

Data Leaks and Breaches

Department store Macy's is the latest retailer to announce a breach of data from their ecommerce site as a result of Magecart payment skimming attacks. By infecting Macy's website with malicious

code, attackers were able to steal customer names, addresses, email addresses, and payment card information from any visitor who entered the data on macys.com between October 7, 2019 and October 15, 2019. Upon discovery of the issue, Macy's removed the malicious code and began notifying affected customers of the incident. ***The NTIC Cyber Center recommends that customers who may have made purchases through Macy's ecommerce website during the affected time frame monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.***

To read more about the threat of Magecart attacks and for additional mitigation strategies, please see our recent Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Transcription service Rev is currently facing scrutiny over the firm's policies governing the handling of sensitive client information. According to reports, customer audio or video file submissions, which Rev claims are kept "private and protected from unauthorized access," can allegedly be accessed by any of Rev's 40,000 freelance workers that provide transcription support for the company. Sensitive content that workers have encountered include personal phone calls, open investigation casework, police body camera footage, medical files, and more. Security professionals have expressed concerns that transcriptionists have far more access to data files than necessary and that Rev offers too few safeguards to protect clients against data scraping or the exploitation of personally identifiable information. ***In light of these concerns, the NTIC Cyber Center advises customers of Rev or other transcription services to be aware of security concerns surrounding the submission of sensitive or personal data to cloud environments that lack adequate data protections.***

The largest US independent supplier of insulin pumps and continuous glucose monitors (CGMs), Solara Medical Supplies, disclosed a data breach affecting customer data. On June 28, 2019 Solara discovered that an unknown threat actor compromised employees' Office 365 accounts between April 2, 2019, and June 20, 2019. Data compromised in this breach include customer names, addresses, birth dates, Social Security numbers, employee identification numbers, medical details, health insurance information, financial and payment card details, driver's licenses, state IDs, passport information, login credentials, billing details, claims details, Medicare IDs, and Medicaid IDs. The breach is attributed to a series of phishing attacks. Solara is collaborating with law

enforcement, notifying potentially affected customers and resetting affected account credentials. Affected customers are offered free credit monitoring and identity protection services ***The NTIC Cyber Center recommends Solara Medical Supplies customers remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure and monitor financial accounts for suspicious activity and unauthorized transactions. Affected customers may refer to the Solara Medical Supplies notice for further information and to obtain credit monitoring and identity protection services at no charge.***

Researchers from Fidus Information Security discovered a misconfigured database belonging to the role-playing game publisher, Wizards of the Coast, containing approximately 452,000 records of customer information. Data compromised in this breach include names, user names, hashed and salted passwords, email addresses, phone numbers, and account creation dates and times. It is unknown how long the database has been exposed. The exposure is attributed to an unencrypted backup database filed within a public Amazon Web Services storage bucket. Wizards of the Coast has since closed the database and will contact affected customers. ***The NTIC Cyber Center recommends Wizards of the Coast customers remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

Upcoming Webinars

Six Steps to Effective ICS Threat Hunting

On November 22, Dragos Principal Threat Analysts Dan Gunter and Marc Seitz will be joined by Tim Conway, Technical Director - ICS and SCADA Programs at SANS, to introduce a 6-step ICS

threat hunting model. They'll demonstrate how to apply it to real-world threat hunting scenarios, pinpoint adversary behavior patterns, and stop ICS threats from going undiscovered.

What You'll Learn:

- Why proactive threat hunting is necessary for ICS cybersecurity defense
- How to complete effective threat hunting
- What adversary behavior patterns look like
- How to apply the model to real world threat hunting scenarios
- How to measure the effectiveness of threat hunts

To register for this free webinar on Friday, November 22 at 1:00 PM ET, click here.

Securing Our Communities

Last week, due to a technical glitch (or, more likely, human error), our bulletin's Securing Our Communities section incorrectly linked to our previous blog post on two-factor authentication (2FA) scams. We sincerely apologize and have decided to include our piece on Mortgage Wire Fraud again this week for anyone who was unable to read it.

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Mortgage wire fraud, also known as a mortgage closing scam, is a type of social engineering scheme in which perpetrators steal money or elicit personally identifiable information (PII) from victims through fraudulent real estate correspondence for financial gain or identity theft. Perpetrators take advantage of the numerous steps taken and parties involved in the real estate acquisition process. They target victims using email, voice messaging services, and websites. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Brave Urges Congress to Require Ad Blocking Browsers for Government Employees

Analytic Comment: Developers of the security conscious Internet browser "Brave" have urged Congress to require the use of ad blocking browsers on government networks to protect employees from malvertising. The company warns that malvertising, or the insertion of malicious code into advertisements on websites, is a known malware distribution vector and could allow foreign and domestic threat actors to access sensitive information or gain entry into government networks. Threat actors frequently disguise malware in fraudulent updates for Adobe, Flash, or other programs and have used malvertising to infect victims with ransomware, information-stealing Trojans, and Remote Access Trojans (RATs). Though Brave is not the first entity to raise concerns about the threat of malvertising, the company's stance highlights the merits of configuring browsers with ad blocking extensions to stop the launch of executable code in advertisements by default.

Disney+ 'Hack' Panic Stresses Why You Need to Use Unique Passwords

Analytic Comment: With the launch of the new Disney+ streaming service, reports have surfaced that over 4,000 Disney+ accounts were hacked, and their login credentials were placed up for sale on Dark Web forums. Disney immediately refuted these claims, countering instead that the "hack" was, in fact, the result of credential stuffing attacks on accounts that were inadequately secured with passwords leaked in previous data breaches. In these attacks, hackers likely used old username and password combinations along with automated hacking tools to gain access to the accounts. The ease and swiftness at which hackers manage to accomplish this feat should remind users of the importance of using a password manager to generate and store lengthy, unique passwords for all online accounts to reduce the risks associated with password reuse.

Patches and Updates

Google Releases Security Updates for Chrome

WhatsApp

ICS-CERT Advisories

ABB Power Generation Information Manager (PGIM) and Plant Connect

Flexera FlexNet Publisher

Omron CX-Supervisor

Philips IntelliBridge EC40/80

Siemens Desigo PX Devices

Siemens Industrial Products (Update B)

Siemens Mentor Nucleus Networking Module

Siemens PROFINET Devices (Update A)

Siemens S7-1200 CPU

Siemens SINAMICS (Update A)

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on *Subscribe to Receive Our Products* at the top of the page, and enter your information.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2019-11-039

HSEC-1 | NTIC SIN No. 2.5, 5.4

November 27, 2019

Happy Thanksgiving from the NTIC Cyber Center!

We here at the NTIC Cyber Center are thankful for you, our subscribers, who welcome our emails into your inbox each and every week. We sincerely hope you find our content valuable as we work to bring you the latest in open-source cyber threat information and actionable intelligence. The NTIC Cyber Center wishes all of our members a happy, fun, and safe Thanksgiving weekend!

Current and Emerging Cyber Threats

Trickbot Trojan Updated with Password Stealing Module

Palo Alto Networks Unit 42 research group discovered that the Trickbot banking trojan has recently been updated with a password stealing module that can pilfer OpenVPN passwords, OpenSSH private keys and configuration files on Windows systems. Threat actors typically infect machines

with malicious spam (malspam) campaigns that incapacitate Windows Defender antivirus. The newly modified Trickbot can use HTTP POST requests to send OpenSSH private keys and OpenVPN passwords and configuration files to its command and control (C2) servers. It can also pilfer data from various apps such as Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge, Microsoft Outlook, FileZilla, and WinSCP. ***The NTIC Cyber Center recommends users remain vigilant for malspam campaigns, avoid opening and unexpected emails, and refrain from clicking on links or downloading attachments from unknown or untrusted sources. If you believe you have been infected with the Trickbot Trojan, notify your organization's IT security team immediately. Additionally, we recommend network administrators keep all systems and software up-to-date with the latest security patches and to proactively block the indicators of compromise (IoCs) provided in Trend Micro's post.***

Ransomware Roundup

Welcome to Ransomware Roundup, a new feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

Clop

Discovered earlier this year, Clop ransomware, a version of the CryptoMix variant, has recently been observed attempting to disable Windows Defender and remove Microsoft Security Essentials and Malwarebytes' Anti-Ransomware software from infected systems. Clop performs these functions prior to encrypting files to prevent behavior-based malware detection systems from blocking the malware. If successful, Clop appends *.CLOP* or *.CIOP* to the names of encrypted files and drops a ransom note named *CIopReadMe.txt* on infected systems. There is currently no free decryption tool available for this variant. More information about CLOP ransomware is available on Bleeping Computer's website.

Shade

Previously observed targeting Russian victims, the threat actors behind Shade ransomware began to set their sights on US targets earlier this year. According to cybersecurity firm Group-IB, Shade accounted for over 50 percent of all malware seen in the wild, making it the most prevalent strain the firm saw in the first half of 2019. Shade ransomware, also known as Troldesh, has been active since 2014 and is traditionally distributed via malicious email campaigns and exploit kits. Its

creators have continuously updated the variant over the years and have recently included cryptocurrency-mining and ad fraud capabilities. Shade infects systems running Windows and the latest variant appends *.crypted000007* to the names of affected files. No More Ransom provides a free decryption tool for some versions of Shade here. Data Breach Today provides more information about Shade and other prevalent strains here.

Vulnerabilities

Virtual Network Computing Services

Security researchers have identified 37 vulnerabilities affecting the Virtual Network Computing (VNC) implementations including LibVNC, TightVNC 1.X, TurboVNC, and UltraVNC VNC. The vulnerabilities, all caused by memory corruption flaws, may allow attackers to launch denial of service attacks, access user information, or execute malicious code on a targeted device. Researchers believe over 600,000 VNC servers currently exposed on the open Internet may be vulnerable to these attacks. ***The NTIC Cyber Center recommends administrators of VNC servers block unrequired remote connections, ensure VNC applications are kept updated with the latest patches, protect VNC servers with strong passwords, and to avoid connecting to untrusted or untested VNC servers.***

Data Leaks and Breaches

Smartphone manufacturer OnePlus announced a breach of data resulting from unauthorized third-party access to customer order information. Data exposed in this breach includes customer names, contact numbers, emails, and shipping addresses of customers who placed orders on OnePlus's online store. Customer payment information and login credentials are not believed to have been affected in this breach. ***The NTIC Cyber Center recommends OnePlus online shopping customers remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

Cellular phone carrier, T-Mobile, disclosed a data breach affecting its prepaid customers in which unknown threat actors gained unauthorized access to an undisclosed number of customer accounts. Breached data included customer names, phone numbers, billing addresses, account numbers, rate plans, and calling features. T-Mobile states that no Social Security numbers, passwords, or financial information were compromised and the company will notify affected customers. ***The NTIC Cyber Center recommends affected T-Mobile customers immediately change their PINs, monitor their accounts, and immediately notify T-Mobile customer service of any unauthorized or suspicious activity.***

The threat actors behind Maze ransomware compromised security staffing firm, Allied Universal, and published some of its data to the public after a missed ransom payment with more published leaks to follow if demands are not met. While it is uncertain how Maze has infected Allied Universal in this case, recent reporting suggests it could have been distributed via an exploit kit. Allied Security is currently strengthening its internal security posture and is working with third-party consultants to verify corrective measures. The threat actors claim to still have access to Allied Universal's servers. ***The NTIC Cyber Center encourages network administrators to review our Ransomware Mitigation Guide and implement the recommendations provided to reduce the risk of a ransomware infection. Additionally, we recommend network administrators proactively block the indicators of compromise (IoCs) provided in Bleeping Computer's post.***

Upcoming Webinars

Data Breach Today
Prevention. Response. Notification.

Best Practices for Mitigating Third-Party Remote Access Risk

63% of data breaches are caused by third-party, yet most organizations treat their vendors like internal employees when it comes to remote access. Because of this, the average organization spends endless hours and resources investigating incidents and pulling together reports, which only compounds the problem. Data breaches are not only financially devastating and time consuming, but most organizations aren't equipped to prevent them.

In this webinar, Justin Strackany, Chief Customer Officer, and Tony Howlett, CISO at SecureLink will discuss how to align your organization with industry regulations such as HIPAA, PCI, CJIS

requirements and how to alleviate third-party vendor risk.

Register for this live, interactive workshop to learn:

- Current state of third-party access
- Lessons learned from recent third-party data breaches
- The challenges with vendor management
- How to best identify, control and audit your vendors

To register for this free webinar on Thursday, December 5 at 2:00 PM ET, click here.

How to Prevent 81% of Phishing Attacks from Sailing Right into Your Inbox with DMARC

Only ~20% of companies use DMARC, SPF, and DKIM, global anti-domain-spoofing standards, which could significantly cut down on phishing attacks. But even when they are enabled and your domain is more secure, 81% of phishing attacks still continue to sail right through to the end-user.

In this webinar, Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, will teach you how to enable DMARC, SPF, DKIM the right way! Then, learn the six reasons why phishing still might get through to your inbox and what you can do to maximize your defenses.

What you'll learn:

- How to enable DMARC, SPF, and DKIM
- Common configuration mistakes
- How to best configure DMARC and other defenses to fight phishing
- Techniques to empower your users to identify and avoid phishing attempts that make it through your surface-level defense

To register for this free webinar on Tuesday, December 10 at 11:30 AM ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

The ***Secret Sister Gift Exchange*** is a type of pyramid scheme primarily targeting female Facebook users, in which

perpetrators use the guise of an innocent holiday gift exchange to steal personal information from participants. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Twitter Just Confirmed a Better Way to Secure Your Account

Analytic Comment: Twitter has updated its two-factor authentication (2FA) settings to allow users to secure their accounts with methods other than a personal telephone number. This change will make Twitter users less vulnerable to SIM swapping attacks, scams in which hackers take over victims' phone numbers and intercept one-time passwords sent via phone or SMS-based 2FA methods. Twitter now offers the ability for customers to use mobile security apps instead, which offer enhanced account verification security features without the risks associated with phone or SMS-based 2FA. Twitter's move acknowledges the importance of keeping customers secure from new and evolving cyber threats and should serve as a reminder for endpoint users to enable 2FA on all accounts that offer it.

110 Nursing Homes Cut Off from Health Records in Ransomware Attack

Analytic Comment: Virtual Care Provider Inc. (VCPI), an IT services provider for nursing homes with locations in 45 states, was infected with the Ryuk ransomware variant. Many services are affected such as communications, patient records access, billing, and payroll operations. In some facilities, nurses are unable to get medication delivered on time. The unknown threat actors are demanding a $14 million ransom payment. VCPI's CEO states that her firm cannot afford the ransom but it is working to restore customer access. VCPI is just one of many healthcare organizations affected by recent ransomware attacks. Difficulties associated with restoration efforts highlight the importance of taking proactive steps, including patching systems and performing frequent backups, to prevent falling victim to a ransomware attack.

Patches and Updates

Microsoft Releases Outlook for Android Security Update

ICS-CERT Advisories

ABB Relion 650 and 670 Series

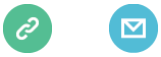
ABB Relion 670 Series

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

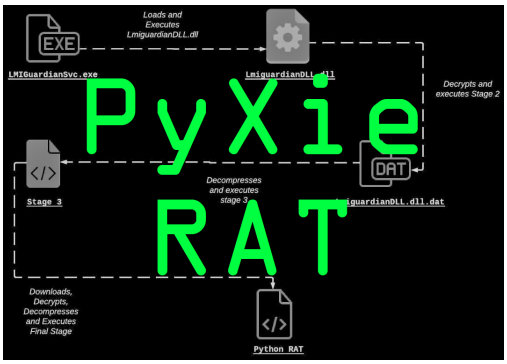
TLP:WHITE

Product No. 2019-12-004

HSEC-1 | NTIC SIN No. 2.5, 5.4

December 5, 2019

National Capital Region Cyber Threat Spotlight



Remote Access Trojan PyXie Targets Healthcare and Education Organizations

Researchers at Cylance discovered a new malware variant, dubbed PyXie, targeting organizations within the healthcare and education sectors. PyXie is a Remote Access Trojan (RAT) equipped with functions that include keylogging, credential harvesting, and video recording. It is also capable of stealing cookies, performing man-in-the-middle attacks, and deploying additional malware, including ransomware, onto infected systems. Threat actors have deployed PyXie onto targeted machines using sideloading—a technique that leverages dynamic link libraries (DLLs) in legitimate applications to load malware components onto targeted devices. In the case of PyXie, threat actors abused DLLs in LogMeIn and Google software components installed locally to force the installation of the malware. Though PyXie has only recently been discovered, researchers believe that its careful obfuscation may have allowed threat actors to use it stealthily in hacking campaigns since at least 2018.

To combat the threat of PyXie Trojan malware, the NTIC Cyber Center encourages network administrators, especially those in the healthcare and education sectors, to keep all systems and software up-to-date with the latest security patches and to proactively block the indicators of compromise (IoCs) provided in Cylance's report.

Current and Emerging Cyber Threats

New Android Trojan Ginp Steals Text Messages and Banking Details

Security researchers discovered a new strain of malware that infects Android devices with Ginp, a mobile banking Trojan. Ginp masquerades as Adobe Flash Player and, once installed, can set itself as a device's default text message application, read and send text messages, place phone calls, and access mobile banking applications on infected devices, among other functions. These capabilities allow the malware not only to steal payment card details from banking applications, but also to intercept two-factor authentication (2FA) codes that banks commonly send via text message to secure customer accounts against fraudulent login attempts. ***The NTIC Cyber Center advises Android device users to remain vigilant for banking Trojans disguised as Adobe Flash Player installations or other applications. If you suspect your device may be compromised, or if it exhibits unusual behavior such as excessive power consumption, excessive data usage, or unexpected pop-ups, we advise performing a factory reset of the device to ensure that malicious content is completely removed.***

RevengeHotels Malware Campaign Targets Hospitality Sector Organizations

A new malware campaign, dubbed RevengeHotels, is targeting computer systems at hotels, hostels, and hospitality and tourism companies worldwide. This campaign features maliciously crafted Microsoft Word, Excel, and PDF documents sent as attachments in spear phishing emails that masquerade as requests to book numerous rooms for a large group. When opened, the malicious attachments launch Remote Access Trojans (RATs) and other custom malware variants designed to collect data from the system clipboard, intercept documents sent to a printer, take screenshots, and capture guest credit card data stored in hotel systems or transmitted from online travel booking sites. In addition, the malware also infects hotel front desk computers with a credential-stealer capable of capturing login credentials from hotel administration software. Researchers have observed some threat actors selling remote access to compromised hotel systems, enabling other cybercriminals to access and further profit from stolen data. ***The NTIC Cyber Center advises businesses in the hospitality sector to avoid opening emails and attachments from unknown or untrusted sources***

and to scan for and proactively block the IoCs associated with this campaign.

New Mobile Spyware Disguised as Chat Applications

Security researchers identified a new family of mobile spyware masquerading as chat applications. The spyware, dubbed "CallerSpy," was found in both the Chatrious and Apex App—two chat applications available for download from phishing sites that use typosquatted domains to spoof legitimate Google websites. CallerSpy runs on Android devices and can collect and exfiltrate call logs, text messages, contact lists, and screenshots from infected devices. ***The NTIC Cyber Center advises users who may have downloaded Chatrious or Apex App to perform a factory reset of the device to ensure the complete removal of CallerSpy spyware. In addition, we advise administrators to scan for and proactively block the IoCs listed in TrendMicro's report.***

Fraudulent Prize Lures Steam Users

A researcher discovered a phishing campaign targeting Steam customers that attempts to elicit victims' account credentials. Fraudulent user comments posted on the gaming platform attempt to lure victims with the promise of a prize giveaway and urge them to click a link. The link directs them to a fraudulent page advertising a $30,000 giveaway that contains free in-game accessories for Counter-Strike: Global Offensive (CSGO). Users are then prompted to click another fraudulent link that masquerades as a Steam login page in order to redeem the prize. ***The NTIC Cyber Center recommends Steam users remain vigilant for phishing attempts disguised as free prize giveaways and refrain from clicking on links from unknown or untrusted sources. We also recommend Steam users login to Steam directly from the official application or the official steampowered.com domain.***

Ransomware Roundup

Welcome to Ransomware Roundup, a new feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

DeathRansom

DeathRansom is a new ransomware variant that targets systems running Windows OS. Initially, this variant did not encrypt data but merely appended *.wctc* to the names of affected files, allowing victims to easily recover their data by removing the extension. However, it has been recently updated to encrypt targeted files but not modify the file names. DeathRansom drops a ransom note named *read_me.txt* with payment instructions and a unique victim identification code on each infected system and attempts to remove shadow volume copies to prevent victims from restoring files without paying the ransom. The initial infection vector is still undetermined and there is currently no publicly available decryption tool. More information about DeathRansom, including IoCs, is available on the Bleeping Computer website.

Vulnerabilities

Android StandHogg

Security researchers at Promon discovered an active Android vulnerability, dubbed StrandHogg, that lets existing malware masquerade as legitimate apps and affects Android OS versions up to and including 10. These apps can steal account credentials via login prompts and may ask for permissions that can grant threat actors access to photos, text messages, location information, contact lists, phone logs and more. Once infected, a victim who clicks a legitimate icon is presented with a malicious overlay menu that requests credentials and permissions and is then redirected back to the legitimate app. Threat actors initially compromise a device with separate malicious dropper apps and leverage a legitimate Android control setting known as "taskAffinity" that can allow any app to take on any identity in the multitasking system. This can all be done without needing to root the device. Promon states that the top 500 apps are at risk and there is no patch or workaround currently available. ***The NTIC Cyber Center recommends that users only download applications from trusted and vetted sources, keep device operating systems up to date, and backup data on mobile devices regularly. In addition, before installing any app, exercise caution and research both the app itself and the developer. Once an app is installed, monitor the app's requests for permission authorizations and data activity. Users who suspect that their devices have been compromised should perform a factory reset and restore devices to manufacturer default settings. Additionally, users impacted by this or other malicious Android apps are strongly encouraged to change their account credentials and monitor accounts for suspicious or unauthorized activity.***

Data Leaks and Breaches

Ecommerce web platform Magento announced a breach of customer data from their Marketplace application store. According to the company's notification, an unauthorized third party exploited a vulnerability in the store and gained access to the data of an unknown number of Magento accountholders. Information exposed in this breach includes customer names, usernames, email addresses, billing and shipping addresses, and phone numbers. Magento has patched the vulnerability and has informed affected customers of the incident. ***The NTIC Cyber Center advises Magento customers to remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure.***

Music streaming platform MixCloud reports that a hacker accessed the customer account data of 21 million registered platform users and posted the information for sale on an underground marketplace. Data stolen in this breach includes customer email addresses, IP addresses and, for users who did not sign up through Facebook, hashed account passwords. Though no plaintext passwords were leaked in this breach, MixCloud still encourages all users to change their account password as well as the passwords to any other online accounts for which the same credentials may have been used. ***The NTIC Cyber Center recommends MixCloud users remain vigilant for an increase in phishing attempts perpetrated through email, social media, or other avenues as a result of this data exposure.***

The online store of gun manufacturer Smith & Wesson was compromised as a result of Magecart payment skimming attacks that pilfered sensitive customer data. It is unclear how many customers were affected and what data was stolen, but it was determined that the site was compromised prior to Black Friday. The group behind the campaign used a dynamic script that would load malicious or non-malicious content depending on the site visitor and site section visited. ***The NTIC Cyber Center recommends that customers who have recently made purchases through Smith &***

Wesson's website remain vigilant for an increase in phishing attempts perpetrated though email, social media, or other avenues as a result of this data exposure. We also recommend monitoring financial account statements and immediately notifying financial institutions of any unauthorized or suspicious activity.

To read more about the threat of Magecart attacks and for additional mitigation strategies, please see our recent Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Upcoming Webinars

2020 Outlook for Healthcare Security

As 2020 approaches, healthcare experts forecast necessary information security priorities for the coming year. They will also look back at the mistakes made over the past decade.

Healthcare organizations continue to grow and change at an unprecedented velocity. With 2019 outpacing previous years for acquisitions, expansion, and partnerships, organizations have unfortunately opened up new vulnerabilities.

Healthcare organizations have also made key decisions around whether to use the cloud or keep data on-premises, how to implement new connected medical devices, and how to manage constant turnover.

This webinar will focus on the impact of all of those changes on information security. Mike and Drex will share stories of security incidents and how organizations handle them.

Join this session to hear Mike and Drex discuss:

- Mistakes and challenges of 2019, including InfoSec tool sprawl and overloading IT teams
- 2020 solutions and priorities for managing cyber-risk
- The latest threats toward healthcare entities, such as IoT botnet credential-stuffing and sophisticated phishing
- Timely Incident Response in action, including recommendations for improving your incident response plans
- New ways organizations are monitoring and responding to threats

To register for this free webinar on Wednesday, December 11 at 2:00 PM ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Charity scams, also known as donation scams or charity fraud, are a type of social engineering scheme in which the perpetrator elicits money or personal information from victims through fake charities and popular social causes.Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Web Skimmer Phishes Credit Card Data via Rogue Payment Service Platform

Analytic Comment: Online merchants often outsource their payment process using a payment service platform (PSP) and threat actors have started to masquerade as PSPs to steal customer payment information. To add legitimacy to their scheme, these fraudulent payment sites will check if all fields are complete and valid before processing and have the ability to redirect victims to the legitimate site afterwards to display the recent purchase amount. This highlights the importance of regularly monitoring financial account statements as it is becoming increasingly difficult for users to discern complex phishing schemes from legitimate services and webpages.

Google: Government-Backed Hackers Targeted 12,000 Users

Analytic Comment: Google's Threat Analysis Group (TAG) analyzed more than 270 government-backed groups from more than 50 countries known for intelligence collection, spreading disinformation, and stealing intellectual property. Google detected threat actors targeting the full spectrum of their products including YouTube and Google Drive and has warned more than 12,000 users across 149 countries that they have been targeted by government-backed hackers. Threat actors used phishing emails over 90 percent of the time to target users including activists, journalist, and politicians. These findings underscore the importance of establishing strong operational security and using multifactor authentication on every account that offers it to reduce the risk of compromise.

Patches and Updates

Microsoft Office 2016

Mozilla Releases Security Updates for Firefox and Firefox ESR

ICS-CERT Advisories

Moxa AWK-3121

Reliable Controls LicenseManager

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2019-12-011

HSEC-1 | NTIC SIN No. 2.5, 5.4

December 12, 2019

National Capital Region Cyber Threat Spotlight

Dridex Trojan Targets Financial Services Sector

The US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) recently issued an alert about ongoing Dridex malware campaigns targeting the Financial Services Sector. Dridex is a type of Trojan designed to steal online banking credentials from unsuspecting victims. Dridex is typically distributed via phishing email campaigns that contain malicious attachments – either Microsoft Word and Excel documents embedded with malicious macros or compressed ZIP or RAR files. Once a system is infected, Dridex installs a keylogger to collect banking information and then sends that information back to the attacker's command-and-control (C2) server to be used to commit theft and financial fraud. Dridex first appeared in 2012 under the moniker "Cridex" and has since evolved to become a highly sophisticated variant of malware. ***To reduce the risk of becoming infected by Dridex, the NTIC Cyber Center recommends***

never opening or enabling macros in attachments from unknown or unexpected sources, disabling macros by default on Microsoft Office applications, and keeping all software, operating systems, and antivirus solutions updated. We also recommend all network administrators review CISA's Alert AA19-339A and proactively block the associated indicators of compromise (IoCs).

Current and Emerging Cyber Threats

TrickBot Delivered via Payroll Phishing Campaign

Palo Alto Networks Unit 42 research group uncovered a malicious email campaign that delivers Trickbot malware embedded in emails masquerading as payroll correspondence. TrickBot is a modular information-stealing Trojan and, in this campaign, threat actors send malicious email from compromised accounts to appear legitimate. Recipients are urged to click a URL within an email that forwards them to a Google Doc document that contains another link to a file in Google Drive. This file contains a downloader that downloads Trickbot onto the victim's system. Threat actors are able to add legitimacy to the campaign and bypass email security filters by leveraging Google Drive, Google Docs, and SendGrid to host and deliver malicious content. ***The NTIC Cyber Center recommends users remain vigilant for malspam disguised as official payroll correspondence, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. If you receive an email that you suspect may be malicious, notify your IT security team immediately. Additionally, we recommend network administrators keep all systems and software up-to-date with the latest security patches and to proactively block the IoCs provided in Unit 42's report 's post.***

Ransomware Roundup

Welcome to Ransomware Roundup, a new feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

Sodinokibi/REvil Ransomware Impacts Large US Data Center Provider

Data center provider, CyrusOne, is one of the latest to fall victim to the Sodinokibi ransomware, also known as REvil. Sodinokibi was first observed in April 2019 and encrypts data on computers

running the Windows operating system, disables recovery mode, and deletes Volume Shadow Copies to prevent victims from trying to restore impacted files without paying the ransom. During the infection process, Sodinokibi ransomware renames the encrypted files using a random extension that is used as a unique victim identifier. It also drops a text file named *[extension]-HOW-TODECRYPT* on the infected system that includes instructions on how to download the Tor web browser, visit the payment portal, and pay the ransom. It currently unknown how the threat actors initially compromised CyrusOne and the company is currently working with law enforcement and forensics firms for further investigation and to restore systems. For more information about REvil/Sodinokibi ransomware, visit the NTIC Cyber Center's intelligence product and the Secureworks website.

Sodinokibi/REvil Ransomware Disrupts More Than 100 Dental Offices

A Sodinokibi ransomware attack on a managed service provider (MSP) has resulted in the disruption of services at over 100 dental offices nationwide. The attack that occurred on November 25 targeted Colorado-based IT services company Complete Technology Solutions (CTS), an MSP that provides network security, data backups, and voice-over-IP (VoIP) phone services to dental offices. Experts believe that attackers abused CTS's remote administration tool to spread Sodinokibi to client systems, encrypt valuable data, and leave notes demanding ransom payments. Though the attack occurred over two weeks ago, dental offices nationwide are still struggling to recover encrypted data, rebuild systems, and restore services. The NTIC Cyber Center reminds customers of MSPs to maintain a robust and comprehensive data backup strategy, which includes scheduling backups often and keeping them stored off the network in a separate and secure location. For a full list of prevention and mitigation strategies, please download our Ransomware Mitigation Guide available on our website.

Ryuk Ransomware Infects Emergency Care Facilities' IT Provider

An end-to-end IT service provider for emergency care facilities is among the latest organizations to fall victim to a Ryuk ransomware attack. Researchers believe that T-Systems, a company that provides services to over 1,900 emergency care facilities throughout the country, was impacted by Ryuk at the end of November, with company systems still inaccessible nearly two weeks later. Other entities impacted by recent Ryuk attacks include a school district in Lincoln, MS and several organizations in Spain, including a radio station, a manufacturing company, a construction company, and a private security company. More information about Ryuk ransomware is available on CrowdStrike's website. It is important to note that, even if Ryuk victims pay the ransom amount, they may not be able to recover all of their encrypted data as there is a flaw in the decryption tool that prevents data restoration in some cases, according to researchers at cybersecurity firm Emsisoft. The NTIC Cyber Center always discourages paying the ransom as it perpetuates this type of crime

and data recovery is not guaranteed.

New Snatch Ransomware Strain Reboots Computers into Safe Mode

Security researchers at cybersecurity firm Sophos discovered a new version of Snatch ransomware that reboots infected computers running Windows 7 through 10 into Safe Mode to disable and bypass any security tools present on the system. Snatch ransomware appears to be distributed manually by threat actors who conduct brute-force attacks against vulnerable and exposed systems and pivot within compromised networks. To avoid detection and maintain persistence, this variant installs itself as a Windows service named "SuperBackupMan" and adds a registry key to ensure it starts in Safe Mode during a system reboot. Snatch ransomware appends a partially random string of five alphanumeric characters to the names of encrypted files and drops a similarly-named ransom note on the infected system. There is currently no publicly available decryption tool for Snatch ransomware. More information about this variant, including associated IoCs, is available on the Sophos website.

Vulnerabilities

Linux Vulnerability Allows Hackers to Hijack VPN Connections

Security researchers discovered a vulnerability affecting virtual private network (VPN) connections on Linux distributions and numerous Unix-like operating systems including FreeBSD, OpenBSD, macOS, iOS, and Android. This vulnerability, tracked as CVE-2019-14899, may allow an attacker to determine if a connected user is using a VPN, make inferences about websites they are visiting, inject data into the TCP stream, and hijack active VPN connections. ***The NTIC Cyber Center advises administrators to reference security researchers' documentation for a full list of operating systems affected as well as mitigation strategies to guard against the malicious exploitation of this vulnerability.***

Data Leaks and Breaches

Security researchers at Fidus Information Security discovered an exposed database containing over 261,300 phone bills belonging to AT&T, Sprint, T-Mobile, and Verizon Wireless customers. The database, which is owned by Sprint contractor Deardorff Communications and was left unsecured without a password, included information such as names, addresses, call histories and, for some customers, usernames, passwords, PINs, and bank statements. The data was publicly exposed for an unknown period of time in an improperly secured AWS cloud storage bucket, which left information contained within it available for anyone to see and download. Currently, it is not known if Deardorff Communications has plans to notify affected customers of this security incident. ***The NTIC Cyber Center recommends that AT&T, Sprint, T-Mobile, and Verizon Wireless customers remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure. Additionally, we strongly recommend proactively changing passwords and PINs associated with mobile accounts to prevent unauthorized access and SIM-swap attacks.***

Security researchers at Fidus Information Security discovered an exposed and unsecured Amazon Web Services (AWS) cloud storage bucket belonging to an unnamed third-party government supplier that contains over 752,000 applications for copies of US birth certificates. These applications include sensitive personal information such as names, addresses, email addresses, phone numbers, birth dates, and associated family member information. Both Fidus and technology news source TechCrunch reportedly notified the owner of the storage bucket but have received no response and the data remains exposed. ***As it is currently unknown whose data, specifically, is affected in this leak, the NTIC Cyber Center recommends all readers remain vigilant for phishing campaigns associated with this incident and to consider placing a fraud alert or security freeze on***

their credit files with Equifax, Experian, or TransUnion to proactively guard against potential identity theft.

Upcoming Webinars

Data Breach Today
Prevention. Response. Notification.

The Ripple Effect - An Examination of Multi-Party Security Incidents

Software integrations, open APIs, and data sharing between different businesses are a staple of the modern digital organization. Unfortunately, as organizations increase their digital footprint across numerous third-party and fourth-party relationships, their risk of downstream data breaches multiplies. These ripple events are often hidden from the public eye and may not be uncovered for years after the initial event.

During this webinar, Kelly White, CEO of RiskRecon, Wade Baker, Co-Founder at the Cyentia Institute, and David Severski, lead data scientist from the Cyentia Institute, will discuss the findings from a new research report that analyzed over 800 multi-party security incidents to determine how organizations were impacted from the ripple of a security event.

Register for this webinar and you will learn:

- How another firm's breach could impact your organization;
- The methodology behind this exclusive security report;
- Recommendations for protecting your organization from ripple events

To register for this free webinar on Monday, December 16 at 2:00 PM ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Unsolicited robocalls and scam calls are an increasing and pervasive threat to residents within the National Capital Region and across the United States and recent legislation efforts have done little to curb the problem. Unfortunately, distinguishing between scam calls and legitimate calls can be difficult as many of these nuisance calls employ caller ID spoofing techniques to trick recipients into answering the phone. However, mobile phone carriers and communications technology companies have been working together to develop solutions for customers. This week, as part of the NTIC Cyber Center's Securing Our Communities initiative, we are providing our readers with a list of tools and services offered by each major US mobile provider to help combat these unwanted calls. Click here to see what solutions your mobile carrier provides to protect customers from scam calls.

Cyber in the News

FBI Recommends Securing Your Smart TVs and IoT Devices

Analytic Comment: This holiday season, many shoppers will purchase a variety of Internet-connected devices for personal and professional use. However, if not properly configured, these devices can put sensitive data and networks at risk of a cyber attack. The Federal Bureau of Investigation (FBI) advises consumers to take basic precautions when introducing an Internet-connected device to a network for the first time, such as immediately changing default login credentials, segregating them from networks used to transmit sensitive or personal data, disabling or covering cameras and microphones when not in use, applying software and firmware updates when available, and checking the manufacturer's data privacy policies. For more recommendations, please visit the FBI's website.

Criminals Hide Fraud Behind the Green Lock Icon

Analytic Comment: Although the green padlock icon located next to a website's domain name in the URL field of a web browser used to be a valid way to identify secure websites, criminal hackers have begun using these symbols to trick visitors into believing malicious websites are legitimate. Some website certificate authorities allow anyone to apply encryption to their websites, which results in the display of the green lock symbol, and criminals can apply these symbols to malicious websites unbeknownst to most Internet users. To avoid being impacted by these campaigns, it is important to scrutinize the URL when visiting a website.

Patches and Updates

Adobe Releases Security Updates

Apple Releases Multiple Security Updates

Google Releases Security Updates for Chrome

Intel Releases Security Updates

Microsoft Releases December 2019 Security Updates

Samba Releases Security Updates

VMware Releases Security Updates for ESXi and Horizon DaaS

ICS-CERT Advisories

Interpeak IPnet TCP/IP Stack (Update B)

Siemens EN100 Ethernet Module

Siemens Industrial Products (Update C)

Siemens RUGGEDCOM ROS

Siemens S7-1200 and S7-200 SMART CPUs (Update A)

Siemens SCALANCE W700 and W1700

Siemens SIMATIC Products

Siemens SIMATIC S7-1200 and S7-1500 CPU Families

Siemens SiNVR 3

Siemens XHQ Operations Intelligence

We welcome your feedback.

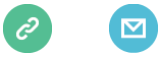
Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on ***Subscribe*** *to Receive Our Products* at the top of the page, and enter your information.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

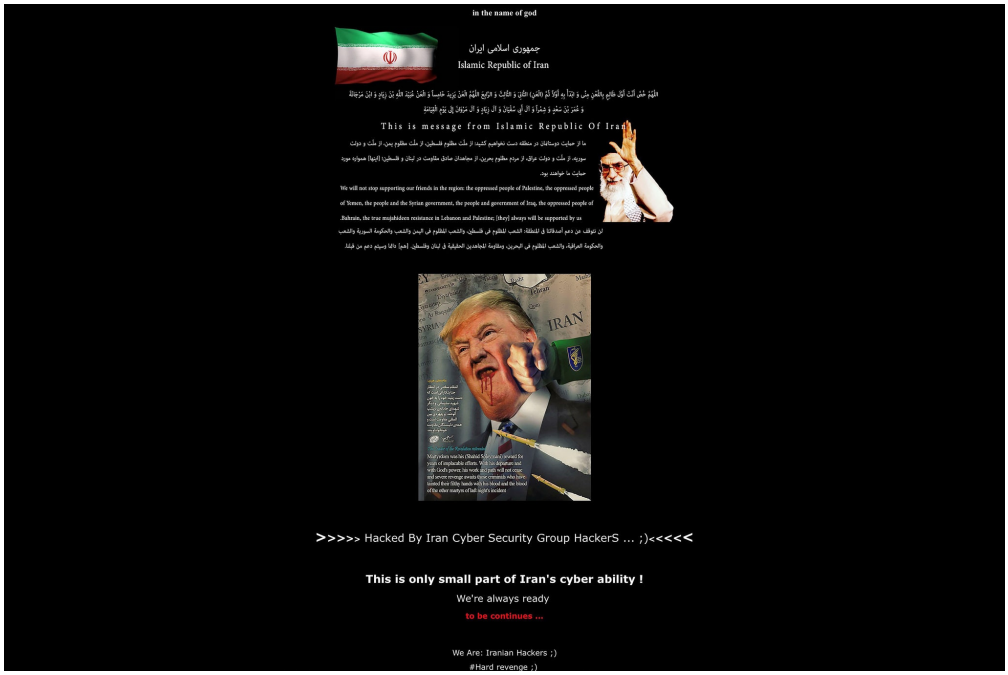
TLP:WHITE

Product No. 2020-01-017

HSEC-1 | NTIC SIN No. 2.5, 5.4

January 9, 2020

National Capital Region Cyber Threat Spotlight



(screen capture of defaced website; image source: New York Times)

Federal Government Website Defaced after US Drone Airstrike Kills Iranian Commander

A federal government website belonging to the Federal Depository Library Program was recently defaced and replaced with messaging vowing retaliation for the January 2 US airstrike that killed Iranian Commander Qasim Suleimani. Some officials believe the defacement may have been the work of a low-level Iranian nationalist hacking group, though there are currently no indications that

Iran officially sponsored the cyber attack. Fortunately, none of the website's data appears to have been compromised, and the attack was likely the result of a misconfiguration in the website's content management system. Nevertheless, a spokesperson for the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) cautioned organizations nationwide to increase safeguards against possible attacks in the wake of last week's events.

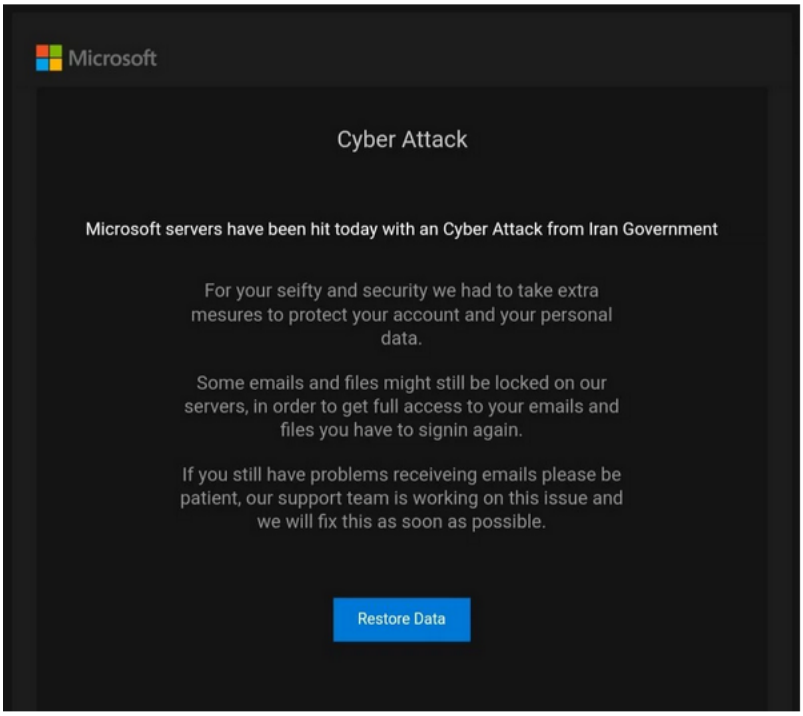
As experts believe an official Iranian response could feature a significant cyber attack against US government agencies, technology or financial services companies, industrial control systems, or other targets, we advise organizations to reference the NTIC Cyber Center's overview of Iran's cyber capabilities to ensure preparedness, resiliency, and defense in the event of malicious cyber activity in the coming days or weeks.

US Coast Guard Issues Bulletin Offering Tips for Cyber Defense

A recent ransomware infection at an unnamed port facility has prompted the US Coast Guard to issue a Marine Safety Information Bulletin offering guidance for cyber attack defense. According to the bulletin, the ransomware disrupted the port's industrial control systems, the monitoring and controlling of cargo transfer, the camera and physical access control systems, the process control monitoring systems, and the port's entire corporate IT network beyond the facility, halting primary operations for over 30 hours. The Coast Guard believes that the ransomware, identified as Ryuk, may have entered the facility's network via a malicious link in a phishing email.

The NTIC Cyber Center encourages organizations to reference the Coast Guard's bulletin for recommendations on the use of intrusion prevention and detection systems, updated virus detection, security logs, network segmentation, updated network diagrams, and regular backups of critical files and software to protect against the threat of ransomware. We also advise organizations to heed recommendations to implement cyber risk management programs in accordance with standards outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and NIST Special Publication 800-82 and to avoid opening emails, clicking links, or downloading attachments from unknown or untrusted sources.

Current and Emerging Cyber Threats



(image source: BleepingComputer.com)

Phishing Campaign Exploits Iranian Cyber Attack Warnings to Steal Microsoft Credentials

A new phishing campaign was recently observed exploiting recent warnings about the possibility of Iran-based cyber attacks to scare victims into revealing their Microsoft account login credentials. Emails from this campaign include the subject "Email users hit by Iran cyber attack" and claim that a cyber attack from the government of Iran impacted Microsoft servers. The emails then attempt to convince users to click on en embedded link to restore their accounts and data, which ultimately leads to a fraudulent website designed to steal victims' login credentials. According to Bleeping Computer, these emails were able to bypass Microsoft Outlook's spam filters. ***The NTIC Cyber Center recommends users remain vigilant for phishing emails claiming their accounts or data were impacted by an Iran-based cyber attack, avoid opening unexpected emails, and refrain from clicking on links or opening attachments from unknown or untrusted sources. If you receive an email that you suspect may be malicious, notify your IT security team immediately.***

New PayPal Phishing Scam Steals Victims' Credentials and Financial Information

ESET researchers discovered a PayPal phishing campaign that, in addition to stealing a target's login credentials, also tricks users into submitting their name, phone number, date of birth,

credit/debit card number, mother's maiden name, email address, and email account password. These phishing emails masquerade as official PayPal correspondence notifying users of an actionable security alert that requires victims to provide credentials and other details in order to regain full account functions. Recipients who click on the notification are forwarded through a series of fraudulent phishing pages that subsequently harvest the victim's data. To add legitimacy to the scheme, threat actors use phishing sites that feature HTTPS websites and green padlocks denoting secure connections. ***The NTIC Cyber Center recommends users remain vigilant for phishing emails disguised as official PayPal correspondence, avoid opening unexpected emails, and refrain from clicking on links or opening attachments from unknown or untrusted sources. If you receive an email that you suspect may be malicious, notify your IT security team immediately.***

Scammers Sending Sextortion Emails in Foreign Languages to Bypass Email Security Filters

Scammers have found a new way to bypass email security filters when targeting English speaking users with sextortion emails. They have started to draft extortion emails in foreign languages with directions in English reading, "Use google translator" in order to bypass security filters that scan for suspicious language associated with these scams. Once the recipient translates the email into English, the text includes threats to release a compromising video of the recipient if they do not remit payment of approximately $1,053 in Bitcoin. In most sextortion scam cases there is no such content recorded; scammers are simply seeking to scare potential victims into paying the extortion fee. ***The NTIC Cyber Center would like to remind our members to ignore sextortion scam attempts. We also encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication on any account that offers it to limit the impact of credential compromise. For more information on sextortion scams, please review our product titled Securing Our Communities: Sextortion Scams.***

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

Sodinokibi/REvil Ransomware Campaign Deployed through Vulnerable Pulse Secure VPN Systems

Security researchers are warning that cyber criminals are exploiting vulnerabilities in Pulse Secure Virtual Private Network (VPN) systems to deploy Sodinokibi ransomware, also known as REvil. The vulnerabilities allow remote attackers to connect to corporate networks, disable multi-factor authentication, and view logs and Active Directory account passwords in plain text. After gaining a foothold, attackers have been observed deleting backups, disabling endpoint security tools, and pushing ransomware to systems on the network. Though a fix for the vulnerabilities was released in April 2019, researchers believe over 1,300 Pulse Secure VPN servers in the United States still remain unpatched and vulnerable to the security flaws. ***The NTIC Cyber Center advises administrators of Pulse Secure VPN systems to ensure all systems are updated with the latest security patches to protect against network intrusions, ransomware, and other cyber threats.***

FBI Issues Alerts for LockerGoga, MegaCortext, and Maze

The FBI has issued alerts for three strains of ransomware, LockerGoga, MegaCortex and Maze, that are currently targeting organizations in the private sector. Threat actors deploying ransomware may first target corporate networks using stolen credentials, phishing campaigns, exploits, SQL injections, and fraudulent cryptocurrency sites. After initially infecting a target, threat actors can maintain persistence for months while spying, exfiltrating data, disabling security-related services, and deploying additional malware before encrypting systems with ransomware. Common signature-based antivirus tools are less likely to detect the infection as threat actors may abuse legitimate tools and services, a technique known as living-off-the-land binaries (LOLBins). In some cases, threat actors may publish stolen information if ransom demands are not met. ***The NTIC Cyber Center recommends administrators regularly back up files, disable unnecessary remote desktop services and close unneeded ports, and keep all hardware, software, plugins, and operating systems patched and updated to reduce the risk of compromise. In addition, administrators are encouraged to use complex and unique login credentials and enable multi-factor authentication for all administrator accounts and control panels, if possible.***

Clop Ransomware Now Capable of Terminating 633 Windows Processes

Discovered earlier last year, Clop ransomware, a version of the CryptoMix variant, has recently been observed with new capabilities to terminate 663 processes for Windows systems. These processes include debuggers, popular text editors, the SecureCRT terminal application, programming languages, terminal programs, Windows 10 apps, and Microsoft Office applications. Clop performs these functions prior to encrypting files to prevent behavior-based detection systems from blocking the malware. Clop appends a new extension, .CL0P, instead of the former .CLOP or .CIOP extensions. There is currently no free decryption tool available for this variant. More information about CLOP ransomware is available on Bleeping Computer's website.

New Ryuk Variant Does Not Encrypt Linux Folders During Ransomware Attack

A new Ryuk ransomware variant does not encrypt Linux folders on operating systems (OS) during a ransomware attack. It is believed that past Ryuk variants that encrypted Linux folders crippled the functionality of the OS, making it difficult for ransomware victims to pay ransom demands. For example, Windows 10 features a way to install various Linux distributions in its OS known as Windows Subsystem for Linux (WSL). When Ryuk compromises this system, it abstains from encrypting *NIX folders, ensuring maximum OS functionality while still keeping the victim's data locked to ensure maximum chance of receiving payment. There is currently no known Linux/Unix Ryuk variant.

Vulnerabilities

SQLite

Security researchers at Tencent Blade Team have discovered several vulnerabilities in the database management system SQLite that affect all programs that use SQLite as a component in their software. If exploited, these vulnerabilities could allow attackers to remotely execute commands and fully compromise a computer. Because SQLite is widely used in many operating systems and software packages, including Google Chrome, Mozilla Firefox, and Windows 10, the vulnerabilities are potentially wide-reaching, though the researchers have not observed any indications to date that the vulnerabilities have been exploited by attackers in the wild. ***As the vulnerabilities may exist anywhere SQLite is used as a software component, the NTIC Cyber Center advises organizations to keep all operating systems and programs updated with the latest security patches to remain protected from these vulnerabilities.***

Citrix ADC and Gateway

Researchers at security company Positive Technologies discovered a flaw in two of Citrix's products, the application delivery and load balancing tool Application Delivery Controller (ADC) and the remote access tool Gateway. The vulnerability, tracked as CVE-2019-19781, allows threat actors to access a target's enterprise network and execute arbitrary code. The vulnerability affects Citrix ADC and Citrix Gateway 13.0, 12.1, 12.0, 11.1, and 10.5, potentially placing at least 80,000 companies across 158 counties at risk. Citrix has released a stopgap mitigation solution and indicates that a firmware update to fully resolve the issue is currently in development. ***The NTIC Cyber Center advises Citrix administrators to apply the stopgap mitigation solution and to keep all systems and software up-to-date with the latest security patches.***

Data Leaks and Breaches

Food service parent company Landry's Inc has reported data breaches at numerous locations of the company's 63 chain restaurant brands including those with a presence in the National Capital Region such as Bubba Gump Shrimp Company, Chart House, Joe's Crab Shack, McCormick & Schmick's, Maestro's Restaurants, Morton's Grille, Morton's Steakhouse, Rainforest Café, and others. The company believes that malware installed on the stores' order-entry systems allowed cyber criminals to steal the payment card numbers, expiration dates, card verification codes, and, in some cases, the cardholder names of an undisclosed number of customers. Payments made from March 13, 2019 to October 17, 2019 are believed to be at risk, though some restaurants may have been affected as early as January 18, 2019. A complete list of affected Landry's Inc. locations can be found here. ***The NTIC Cyber Center recommends that customers who may have made purchases at these stores during the affected time frame monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.***

A security researcher discovered a misconfigured Elasticsearch database exposing the account information of over 2.4 million users of Wyze smart home devices. The database includes user names, email addresses, lists of all devices, nicknames of devices, device models and firmware versions, WiFi network names, API access tokens, and more information. The database was exposed from December 4 to December 26 and was publicly accessible without credentials. ***The NTIC Cyber Center recommends Wyze smart home device users remain vigilant for phishing attempts perpetrated through email, social media, or other avenues. In addition, we recommend changing passwords and enabling two-factor authentication on Wyze smart home device accounts.***

Upcoming Webinars

Data Breach Today
Prevention. Response. Notification.

2020 Outlook for Healthcare Security

As 2020 approaches, healthcare experts forecast necessary information security priorities for the coming year. They will also look back at the mistakes made over the past decade.

Healthcare organizations continue to grow and change at an unprecedented velocity. With 2019 outpacing previous years for acquisitions, expansion, and partnerships, organizations have unfortunately opened up new vulnerabilities.

Healthcare organizations have also made key decisions around whether to use the cloud or keep data on-premises, how to implement new connected medical devices, and how to manage constant turnover.

This webinar will focus on the impact of all of those changes on information security. Mike and Drex will share stories of security incidents and how organizations handle them.

Join this session to hear Mike and Drex discuss:

- Mistakes and challenges of 2019, including InfoSec tool sprawl and overloading IT teams
- 2020 solutions and priorities for managing cyber-risk
- The latest threats toward healthcare entities, such as IoT botnet credential-stuffing and sophisticated phishing
- Timely Incident Response in action, including recommendations for improving your incident response plans
- New ways organizations are monitoring and responding to threats

To register for this free webinar on Thursday, January 9 at 2:00 PM ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Peer-to-Peer (P2P) payment scams are schemes in which perpetrators elicit money from victims via P2P payment apps such as Apple Pay, CashApp, Facebook Payments, Google Pay, Venmo, and Zelle. With just a mobile number or email address connected to a financial account, P2P payment apps allow transactions to be made easily and immediately between individuals and can be used to split bills such as bar tabs or housing expenses. These apps are available for download onto smartphones, tablets, and smartwatches. Although there are very legitimate uses for these apps, scammers have targeted P2P payment app users for financial gain and to steal login credentials or install malware on users' devices. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Please Don't Abbreviate the Year '2020' on Checks and Legal Documents

Analytic Comment: Experts on consumer fraud caution against abbreviating the year 2020 with the shorter two-digit form, "20", on checks, legal documents, and other official forms. They warn that an incomplete date format could leave avenues open for malicious actors to append additional numbers to the date and thus modify the arrangements of a transaction or a contract. In addition to warnings issued by organizations devoted to combatting consumer fraud, law enforcement officials nationwide have also brought attention to this risk, citing that awareness could save consumers "trouble down the road." This issue, though it may not immediately appear relevant for the digital realm, could have implications for uploading signed forms or for steering clear of fraudulent transactions conducted online or through social networking sites this coming year.

Five Cyber Risks that Will Define 2020

Analytic Comment: HelpNet Security has identified five cyber risks that are likely to endanger company data in 2020. The first is insider threats, as research estimates that employees are to blame for over one third of all data breaches. Next is phishing scams, which researchers believe will be made more dangerous by increasingly deceptive and personalized messaging. Exposed databases will also present a risk as more and more organizations move operations and data storage to cloud solutions. The problem of fatigued and overwhelmed IT administrators, and the high turnover rate that consequently plagues the cyber security industry, also presents a risk, though this may be

countered with automated processes that can protect networks against threats and obviate the need for continuous manual engagement with risk assessment tasks. Lastly, misaligned priorities between CEOs and CISOs may contribute to threats to an organization's data security in the year ahead. This list offers insight into possible issues and solutions companies and organizations should consider in 2020 to avoid costly data loss, brand erosion, and reputational damage associated with catastrophic data breaches.

Patches and Updates

Cisco Releases Security Updates

Citrix Application Delivery Controller and Citrix Gateway Vulnerability

Google Releases Security Updates for Chrome

Mozilla Patches Critical Vulnerability

Mozilla Releases Security Updates for Firefox and Firefox ESR

ICS-CERT Advisories

AVEVA Vijeo Citect and Citect SCADA (Update A)

Equinox Control Expert

Interpeak IPnet TCP/IP Stack (Update D)

Moxa EDS Ethernet Switches

Omron CX-Supervisor (Update A)

Philips Veradius Unity, Pulsera, and Endura Dual WAN Routers

Reliable Controls MACH-ProWebCom/Sys

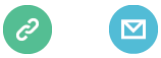
WECON PLC Editor

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on ***Subscribe*** *to Receive Our Products* at the top of the page, and enter your information.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-01-037

HSEC-1 | NTIC SIN No. 2.5, 5.4

January 16, 2020

National Capital Region Cyber Threat Spotlight

CISA Issues Emergency Directive to Patch Windows Systems Against Critical Vulnerabilities

The US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has issued an emergency directive requiring Federal agencies to implement patches that mitigate critical vulnerabilities identified in Windows operating systems. These patches, issued during Microsoft's January 14 "Patch Tuesday" release, provide fixes for vulnerabilities affecting Elliptic Curve Cryptography certificate validation in Windows 10, Server 2016, and Server 2019; Windows Remote Desktop client in all supported versions of Windows and Server; and RDP Gateway Server in Server 2012, 2016, and 2019. CISA warns that, though the Agency has not identified active exploitation of the vulnerabilities, attackers could reverse-engineer the patches to create exploits with which to target vulnerable systems. If left unpatched, these vulnerabilities could expose systems to malware, allow attackers to remotely execute arbitrary code, or convince users to connect to malicious servers. In addition to requiring the implementation of patches, the directive also requires Federal agencies to submit status reports documenting plans, procedures, and actions taken.

Federal agencies are encouraged to review Emergency Directive 20-02 for required actions and reporting procedures.

Current and Emerging Cyber Threats

Fraudulent Amazon Support Hides in Google Search Results

Unknown threat actors have registered fraudulent ads that masquerade as legitimate Amazon customer service and tech support links within Google search results. These ads may be provided as the first links under search results and, when users click these ads, they are redirected to fraudulent Amazon support pages that may attempt to steal victims' money or sensitive information. ***The NTIC Cyber Center recommends users remain vigilant for tech support scams disguised as online ads and fraudulent search results. We also recommend remaining vigilant when browsing the internet and to scrutinize websites for legitimacy prior to entering login credentials and other sensitive information. In addition, the NTIC Cyber Center encourages readers to reference our Securing Our Communities blog post for information on how to recognize and prevent becoming victimized by tech support scams.***

New Android Banking Trojan Uses Stolen Funds to Self Propagate

Security researchers recently observed Faketoken, an Android banking Trojan that generates custom mobile phishing pages, steals victim funds, and propagates itself. An infected device can generate malicious overlay menus that requests credentials that target over 2,200 financial apps and pilfers the user's Mobile Transaction Authentication Number (mTAN) that banks use to validate online transactions. Faketoken operators take a portion of the stolen funds for themselves and may use the rest to pay for international text messages or SMS messages, that contain malicious links that infect more recipients with Faketoken. Some Faketoken versions include ransomware as well. ***The NTIC Cyber Center recommends that users only download applications from trusted and vetted sources, keep device operating systems up to date, backup data on mobile devices regularly, refrain from clicking on links from unknown or untrusted sources and scrutinize unexpected links sent via text message. Enable two-factor authentication on any account that offers it to reduce the risk of compromise resulting from stolen login credentials. Users who suspect that their devices have been compromised should perform a factory reset and restore devices to manufacturer default settings and are strongly encouraged to change their account credentials and monitor accounts for suspicious or unauthorized activity.***

Home Surveillance Customers Threatened with Sextortion Scams

Researchers at Mimecast discovered a sextortion scheme that threatens victims with a release of their home surveillance footage. Threat actors emailed recipients with instructions to view their

footage that is hosted on a website and threatens to release the compromising video if they do not remit payment of approximately $500 in Bitcoin or gift cards. The extortionist-provided footage does not contain actual video from the victim's camera, however. In most sextortion scam cases, there is no such content recorded; scammers are merely seeking to scare potential victims into paying the extortion fee. ***The NTIC Cyber Center would like to remind our members to ignore sextortion scam attempts. We also encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication on any account that offers it to limit the impact of credential compromise. For more information on sextortion scams, please review our product titled Securing Our Communities: Sextortion Scams.***

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

Sodinokibi/REvil Ransomware Actors Now Publishing Stolen Data

Cyber threat actors associated with Sodinokibi/REvil ransomware campaigns have begun publishing data stolen from victims who do not remit payment in time. Though the group has been threatening the release of victims' data since last month, they finally acted on these threats this week by publishing 337MB of stolen data belonging to a US-based IT staffing company on a Russian hacking and malware forum. This incident illustrates that Sodinokibi ransomware actors have adopted tactics similar to those recently used by Maze ransomware actors, who also published data stolen in recent notable ransomware attacks from victims such as Allied Universal in November 2019 and the city of Pensacola, FL, in December 2019. Researchers warn that this disturbing new practice provides cyber threat groups with more leverage to collect payments and is likely to increase among ransomware operators in the future.

Maze Ransomware Operators Publish Stolen Data

The threat actors behind Maze ransomware who compromised wire and cable manufacturer Southwire reportedly stole 120GB worth of files and has since posted a portion of that data to a Russian hacking forum, threatening to publish additional data if demands are not met. Southwire sought injunctive relief to take the threat actors' website down and, in response, the threat actors

stated they would retaliate with "something more interesting," but did not give specifics. ***The NTIC Cyber Center encourages network administrators to review our Ransomware Mitigation Guide and implement the recommendations provided to reduce the risk of a ransomware infection. Additionally, we recommend network administrators proactively block the indicators of compromise (IoCs) provided in Bleeping Computer's post.***

Vulnerabilities

Citrix ADC and Gateway

Security researchers warn that cyber threat actors are actively using and sharing tools to exploit Citrix Application Delivery Controller (ADC) and Citrix Gateway devices vulnerable to CVE-2019-19781. This vulnerability, if exploited, could allow remote attackers to execute arbitrary commands and take full control of vulnerable devices. Though Citrix has not yet released patches addressing this vulnerability, the company has provided a temporary solution to mitigate the associated risks and advises customers to apply the fix as soon as possible. ***The NTIC Cyber Center advises Citrix administrators to apply the temporary mitigation solution and to keep all systems and software up-to-date with the latest security patches. We also encourage administrators to review TrustedSec's post for IoCs associated with exploitation of this vulnerability.***

Data Leaks and Breaches

Peekaboo Moments

A security researcher discovered a misconfigured Elasticsearch database containing more than a 100 GB worth of data from Peekaboo Moments, an infant-monitoring app. The database includes user log files, email addresses, device data, geographic location data, and links to photos and videos. It is uncertain how long the database has been exposed or who may have accessed the data. ***The NTIC Cyber Center recommends Peekaboo Moments users remain vigilant for phishing attempts perpetrated through email, social media, or other avenues. In addition, we recommend changing passwords and enabling two-factor authentication on any application that offers it. Furthermore, the NTIC Cyber Center recommends administrators of Elasticsearch databases reference instructions for configuring Elasticsearch cluster security to reduce the risk of unauthorized access.***

Upcoming Webinars

Data Breach Today
Prevention. Response. Notification.

Data Breach Myth vs. Reality

Data breaches can happen to any organization, so it's important to understand your organization's risk of a data breach. But where should you start your assessment? What practical and pragmatic steps can you take?

Register for this live webinar on data breach myths vs. realities and you will learn about:

- Why breaches happen;
- How rapidly growing cloud and SaaS adoption changes the game for defenders;
- Identity-driven security and the probability of a breach happening to your organization.

To register for this free webinar on Wednesday, January 29 at 2:00 PM ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Sextortion is a cybercrime in which criminals threaten to distribute sensitive or incriminating content if a victim does not comply with certain demands. There are several ways criminals can perpetrate these scams, but their objective remains the same: to profit from the extortion of innocent victims. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Lawmakers Prod FCC to Act on SIM Swapping

Analytic Comment: Democrats in the House and Senate have contacted the Federal Communications Commissions (FCC) asking the agency to require wireless phone carriers to protect consumers from the threat of SIM swapping attacks. In these attacks, malicious actors convince mobile phone store employees to transfer ownership of victims' mobile phone accounts to the attacker's mobile device, granting attackers access to victims' phone numbers and allowing them to intercept one-time passwords sent via phone or SMS-based two-factor authentication methods. Attackers have used SIM swapping to reset passwords to victims' online accounts, access victims' emails, hijack social media accounts, and in some high-profile cases, to siphon money from victims' financial accounts. As Congress notes, SIM swapping attacks remain a serious threat to mobile phone customers.

Patches and Updates

Adobe Releases Security Updates

Critical Vulnerabilities in Microsoft Windows Operating Systems

Intel Releases Security Updates

Microsoft Releases January 2020 Security Updates

Oracle Releases January 2020 Security Bulletin

VMware Releases Security Update

ICS-CERT Advisories

GE PACSystems RX3i

Siemens CP, SIMATIC, SIMOCODE, SINAMICS, SITOP, and TIM (Update E)

Siemens EN100 Ethernet Module (Update A)

Siemens Industrial Products with OPC UA (Update D)

Siemens Industrial Real-Time (IRT) Devices (Update A)

Siemens PROFINET Devices (Update B)

Siemens SCALANCE X (Update A)

Siemens SCALANCE X (Update B)

Siemens SCALANCE X Switches

Siemens SCALANCE X Switches (Update A)

Siemens SCALANCE X Switches, RUGGEDCOM WiMAX, RFID 181-EIP, and SIMATIC RF182C (Update C)

Siemens SIMATIC WinAC RTX (F) 2010 (Update A)

Siemens SINAMICS PERFECT HARMONY GH180

Siemens SINEMA Server

We welcome your feedback.

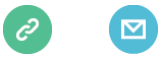
Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit US-CERT.

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on *Subscribe to Receive Our Products* at the top of the page, and enter your information.



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-01-051

HSEC-1 | NTIC SIN No. 2.5, 5.4

January 23, 2020

National Capital Region Cyber Threat Spotlight

US Government and Military Experience Uptick in Emotet Attacks

The threat actors behind Emotet, a modular banking Trojan designed to steal network and account login credentials, are increasingly targeting the US government and military due to an increase of outbound Emotet-laced messages aimed at .gov and .mil top-level domains (TLD). Emotet can hijack email accounts and masquerade as stolen accounts to send more malicious emails as it copies itself in a reply-message for self-propagation. Recipients may not be suspicious of these malicious emails as they appear to originate from trusted sources. To add even more legitimacy to the scheme, threat actors may include communication from a previous email thread from targeted recipients. The victim's data associated with the email account may also be exfiltrated to Emotet's command and control (C2) infrastructure. ***The NTIC Cyber Center recommends users remain vigilant for Emotet email campaigns, avoid opening and unexpected emails, and refrain from clicking on links or opening attachments from unknown or untrusted sources. If you believe you have been infected with Emotet, notify your organization's IT security team immediately so they may contain and remediate the infection.***

Current and Emerging Cyber Threats

NOTROBIN Targets Citrix Systems

Threat actors are currently infecting Citrix systems with NOTROBIN, a backdoor that also blocks other threat actors' access. NOTROBIN prevents other threat actors from exploiting CVE-2019-19781 that grants unauthenticated users rights to perform arbitrary code execution on the Citrix Application Delivery Controller (ADC), Citrix Gateway, and Citrix SD-WAN WANOP appliances. NOTROBIN threat actors are able to access the Citrix backdoor with their own credentials that are unique to separate infected devices. FireEye believes that the threat actors behind NOTROBIN are doing this in preparation of a subsequent campaign they plan to launch. CVE-2019-19781 affects approximately 10,000 vulnerable systems within the US. ***The NTIC Cyber Center advises Citrix administrators to keep all systems and software up-to-date with the latest security patches.***

Sophisticated Phishing Campaign Targets Citibank Customers

Security researchers warn of a new and sophisticated phishing campaign targeting bank account login credentials and personal information of Citibank customers. This campaign clones the official Citibank website and prompts unsuspecting visitors for their login credentials and personal information such as full names, dates of birth, addresses, and the last four digits of their Social Security numbers. It then uses this information to log into the customer's Citibank account which, subsequently, triggers an authentication code to be sent to the customer's associated cell phone via an SMS message. The website then prompts customers to input this code to verify their identity, ultimately allowing attackers to gain full control over victims' Citibank accounts to steal money, change account details, or open additional accounts using the victims' information. To make the phishing website appear more legitimate, attackers configured the domain with a certificate that displays a padlock icon in the browser's address bar, fooling customers into believing the website is secure. ***The NTIC Cyber Center recommends CitiBank customers remain vigilant for phishing campaigns, avoid opening unexpected emails, and refrain from clicking on links or opening attachments from unknown or untrusted sources. We also remind customers to double check the URLs of all websites to ensure their legitimacy prior to entering any personal or sensitive information.***

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

FTCode Enabled to Steal Information

The developers of FTCode ransomware have updated the malware's code to add information-stealing functionality before encrypting victims' files. This change allows FTCode to harvest user credentials from email clients including Mozilla Thunderbird and Microsoft Outlook and common web browsers such as Internet Explorer, Mozilla Firefox, and Google Chrome. FTCode is commonly distributed through spam emails containing malicious Microsoft Word documents disguised as invoices, document scans, and resumes. Security firm Certego provides a free decryption tool for some versions of FTCode here.

Ako Prevents Victims from Restoring Encrypted Files

Ako is a newly emerging ransomware variant that targets computers running the Windows operating system. Upon execution, Ako deletes shadow volume copies, clears recent data backups on the system, and disables Windows Recovery to prevent victims from restoring encrypted files. It then begins the encryption process, appending *.Ci3Qn3* to the names of affected files. Ako collects a list of network adapters and IP addresses from infected systems, scans for local networks, and attempts to encrypt files on network shares. Lastly, it drops a ransom note named ak-readme.txt containing a "Personal ID" to identify paying victims. Researchers determined that Ako ransomware is currently distributed via malicious emails using subject lines such as "Agreement 2020 #1775505." These emails arrive with attached password-protected ZIP files containing the ransomware executable and require user-initiated action to install. There is currently no known decryption tool available for Ako. More information about Ako ransomware is available on Bleeping Computer's website here and here.

Vulnerabilities

Database Reset WordPress Plugin

Security researchers warn that critical bugs identified in the Database Reset WordPress plugin could allow attackers to escalate privileges and wipe all data stored in databases of vulnerable websites. The vulnerabilities, tracked as CVE-2020-7047 and CVE-2020-7048, were patched in last week's

update to the plugin, WP Database Reset 3.15. However, researchers indicate that of the 80,000 WordPress websites currently configured with the plugin, approximately 71,000 have not been updated and currently remain vulnerable. ***The NTIC Cyber Center encourages administrators of WordPress websites that have the Database Reset plugin installed to immediately apply the update and to maintain regular website backups that are stored securely off the network.***

Internet Explorer

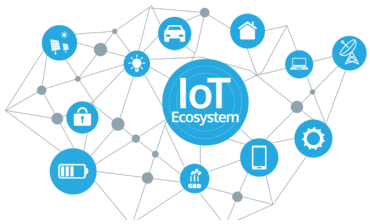
Microsoft warns that attackers are actively exploiting a zero-day critical vulnerability in Internet Explorer to execute arbitrary code on and take control of a target's computer. Attackers have succeeded in compromising machines by sending phishing emails that forward victims to websites crafted to exploit vulnerable Internet Explorer browsers. The vulnerability, tracked as CVE-2020-0674, affects Internet Explorer version 9, 10, and 11 for all Windows desktop and server versions, including Windows 7 and Server 2008—both of which recently reached End-of-Life support. Though Microsoft has yet to issue an official patch mitigating this vulnerability, they have released a temporary workaround. ***The NTIC Cyber Center advises users and administrators of systems installed with Internet Explorer to implement the temporary workaround or to discontinue the use of Internet Explorer until an official patch becomes available.***

Data Leaks and Breaches

Children's clothing retailer Hanna Andersson announced a breach of customer data from their ecommerce website as a result of Magecart payment skimming attacks. By infecting the company's website with malicious code, attackers were able to steal names, addresses, email addresses, and payment card information from any visitor who entered the data on hannaandersson.com between September 16, 2019 and November 11, 2019. Researchers believe attackers infected the website by compromising Salesforce Commerce Cloud, a third-party ecommerce platform currently used by over 2,800 ecommerce websites. Upon discovery of the customer payment card information in dark web marketplaces, law enforcement notified Hanna Andersson, who removed the malicious code and began notifying affected customers of the incident. ***The NTIC Cyber Center recommends that customers who may have made purchases through Hanna Andersson's ecommerce website***

during the affected time frame monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity.

To read more about the threat of Magecart attacks and for additional mitigation strategies, please see our recent Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.



An unknown threat actor has published more than 515,000 remote-access login credentials for home routers, servers, and other Internet of Things (IoT) devices on a hacking forum. The compromised data includes device IP addresses, usernames, and passwords collected between October 2019 and November 2019. The threat actor scanned the Internet for devices with port 23 exposed, a port assigned to the Telnet remote access protocol, and published the list of devices along with known default credentials and commonly used username and password combinations. Telnet is a port used to remotely connect to a system or device and is known to have weak security that can be easily abused to create backdoors into a system or device. ***The NTIC Cyber Center recommends all owners and administrators of Internet-connected devices immediately disable Telnet connections, use lengthy, complex, and unique administrator credentials, and regularly monitor devices for unauthorized user accounts and access. We recommend network administrators block inbound network traffic to port 23 and other unneeded remote access ports at the firewall.***

Upcoming Webinars

Data Breach®
Prevention. Response. Notification. TODAY

Your Ultimate Guide to Phishing Mitigation

Spear phishing emails remain the most popular attack avenue for the bad guys, yet most companies still don't have an effective strategy to stop them. This enormous security gap leaves you open to business email compromise, session hijacking, ransomware and more. Don't get caught in a phishing net! Learn how to avoid having your end users take the bait.

This webinar, hosted by Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, will cover a number of techniques you can implement now to minimize cybersecurity risk due to phishing and social engineering attacks. We won't just cover one angle. We'll come at it from all angles!

Strategies include:

- Developing a comprehensive, defense-in-depth plan
- Technical controls all organizations should consider
- Gotchas to watch out for with cybersecurity insurance
- Benefits of implementing new-school security awareness training
- Best practices for creating and implementing security policies

To register for this free webinar on Tuesday, February 18 at 2:00 PM ET, click here.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.

Ticket scams are a type of social engineering scheme in which the perpetrator sells fake tickets to steal money, elicit personally identifiable information (PII), and/or place malware on the victim's computer. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

FBI Seizes WeLeakInfo, a Website that Sold Access to Breached Data

Analytic Comment: US law enforcement authorities coordinating with international partners have seized a website that sold access to billions of user credentials stolen in previous data breaches. This website provided paid subscribers with the ability to search for names, emails, and usernames and obtain any associated information, including plaintext passwords, from a database of more than 12 billion user records comprising over 10,000 data breaches. Hackers commonly used this information in credential stuffing attacks to access online accounts in which a user may have reused a password leaked in a previous breach. The website allegedly offered subscribers access to an unlimited number of searches for as little as two dollars per day. While the takedown of this website represents a win for all those concerned with information security, the existence of several other websites that

currently operate with the same business model ensures that the fight to dismantle criminal marketplaces and protect user data from theft and illicit sale will likely continue.

Patches and Updates

Adobe Releases Security Updates

Citrix Adds SD-WAN WANOP, Updated Mitigations to CVE-2019-19781 Advisory

Critical Vulnerability in Citrix Application Delivery Controller, Gateway, and SD-WAN WANOP

Google Releases Security Updates for Chrome

Microsoft Releases Security Advisory on Internet Explorer Vulnerability

Oracle Releases January 2020 Security Bulletin

Samba Releases Security Updates

ICS-CERT Advisories

GE PACSystems RX3i

Honeywell Maxpro VMS & NVR

OSIsoft PI Vision

Schneider Electric Modicon Controllers

Siemens EN100 Ethernet Module (Update A)

Siemens Industrial Real-Time (IRT) Devices (Update A)

Siemens SCALANCE X Switches

Siemens SINAMICS PERFECT HARMONY GH180

Siemens SINEMA Server

Siemens TIA Portal

We welcome your feedback.

Please click here to complete a brief survey and let us know how we're doing.

TLP:WHITE

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on ***Subscribe*** *to Receive Our Products* at the top of the page, and enter your information.