number, delivery address). This skimmer features self-cloaking capabilities and anti-tampering protection as it can hide from security tools and self-destruct when it detects tampering. ***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.***

To read more about the threat of Magecart attacks and for additional mitigation strategies, please see our Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

Extortion Scam Targets Website Owners

Researchers have discovered a campaign in which threat actors target website owners with a ransom scam, claiming to have hacked their websites and extracted databases, and threatening to release the stolen data unless a specified ransom amount is paid in Bitcoin. If the ransom is not paid, the scammers threaten to de-index victims' websites from search engines using "blackhat" SEO techniques. Researchers at web app security firm WebARX observed that there has been no proof to support claims that data has been stolen and that threat actors are using fear to extort victims. ***The NTIC Cyber Center recommends never paying any ransom and regularly auditing websites for vulnerabilities that could be exploited. We also recommend creating lengthy, complex, and unique website administrator account passwords and enabling two-factor authentication on these accounts, if available. Additionally, keep all website plugins patched and updated with the latest versions and remove any unneeded, unsupported, or outdated plugins and components. The use of web application firewalls is also encouraged as these can proactively filter potential threats and malicious activity.***

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.

Thanos Employs Security Evasion Technique

The ransomware variant known as Thanos is the first to employ a researcher-disclosed anti-ransomware evasion technique. First observed in 2019, Thanos also contains sophisticated features such as an embedded data theft mechanism and the ability to automatically spread laterally throughout a network. Promoted on Russian-speaking hacker forums, Thanos falls under the category of Ransomware-as-a-Service (RaaS), a revenue-generating platform that allows low-skilled third-parties to create and manage the ransomware campaign for either a monthly rental fee or a percentage of each ransom amount paid. More information about Thanos ransomware is available on BleepingComputer's website here.

Black Kingdom Ransomware Targets Vulnerable Pulse Secure VPN Servers

Malware researchers discovered Black Kingdom Ransomware threat actors exploiting a vulnerability in unpatched instances of the Pulse Secure Virtual Private Network (VPN) software to gain access to enterprise networks and deploy ransomware. This vulnerability was patched in 2019, but many organizations delayed updating their servers. After the threat actors initially gain access to the network through the Pulse Secure VPN vulnerability, they impersonate a legitimate scheduled task for Google Chrome by making a small modification to the task's naming convention. Researchers also determined that the scheduled task runs a Base64-encoded string code in a hidden PowerShell window to fetch a script named "reverse.ps1" that establishes a reverse shell on the infected machine. For more information about this campaign, including indicators of compromise (IoCs), please see BleepingComputer's article here.

Vulnerabilities

D-Link DIR-865L Wireless Routers

Researchers from Palo Alto Networks' Unit 42 uncovered six security vulnerabilities for the D-Link DIR-865L wireless router that may allow threat actors to execute arbitrary commands, steal sensitive information, upload malware, or delete data. One vulnerability was rated as critical while the others were rated as high-severity. It is possible for threat actors to have exploited a combination of these flaws to sniff network traffic and steal session cookies. While the D-Link DIR-865L wireless router has reached its end-of-life (EOL), a patch has been released to only fix three out of the six security vulnerabilities thus far. ***The NTIC Cyber Center recommends decommissioning any unsupported or end-of-life (EOL) hardware and software. We urge affected D-Link customers to update to a different device model that is unaffected by these vulnerabilities.***

IoT Devices Affected by Ripple20 Vulnerabilities

Researchers at security firm JSOF have discovered 19 vulnerabilities in software that is designed to enable internet connections, leaving hundreds of millions of Internet-of-Things (IoT) devices across the globe exposed to a broad array of attacks. These 19 vulnerabilities have since been dubbed "Ripple20" and, if exploited, threat actors can take complete control of any of the affected devices. JSOF states that they have contacted all affected vendors, prompting many to release software updates to patch the vulnerabilities. It is unknown how many devices that include Ripple20 bugs are directly hackable via the internet. ***The NTIC Cyber Center recommends affected IoT device owners and administrators review US CERT Coordination Center's Vulnerability Note VU#257161 and implement their recommended mitigation strategies.***

Upcoming Webinars

Combating Cyber Fraud: Best Practices for Increasing Visibility and Automating Threat Response

The lines are rapidly blurring between traditional fraud and rising cybersecurity threats. Financial services leaders are challenged to find ways to rapidly increase visibility across their environments while accelerating responses to threats effectively and efficiently.

Join Jason Pfeiffer, VP of Product Management at ReliaQuest, as he discusses:

- How the evolution of cyber exploits has changed the way we need to think about and tackle financial crime
- How financial services companies are using automation to combat these types of threats
- Potential visibility challenges for large multi-national organizations as the threat landscape changes and how to overcome them

To register for this free webinar on Thursday, June 25 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.

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

Why Securing Endpoints Is the Future of Cybersecurity

Analytic Comment: Key highlights from Verizon's 2020 Data Breach Investigations Report (DBIR) reveal insights about cyber threat actors and endpoint security. In their summary of findings, 70 percent of breaches were perpetrated by external actors, 86 percent of all breaches were financially motivated, and attacks in which web apps were endpoint accessible comprise 43 percent of breaches. Additionally, it was revealed that financially motivated cyber threat actors relentlessly search for unprotected endpoints to exploit. All of this combined with the lack of asset management oversight underscores the importance of organizations prioritizing endpoint security with audits, automation, and proper asset management systems.

No, That Wasn't a DDoS Attack, Just a Cellular Outage

Analytic Comment: On Monday, June 15, reports of a nationwide mobile carrier outage began to surface on social media. Soon after, misinformation about the outage began to spread, with many social media users citing a hacktivist Twitter account that erroneously claimed a distributed denial-of-service (DDoS) attack was the cause. Although a representative from the mobile carrier addressed the issue on Twitter and stated that engineers were working to fix the problem, an increasing number of social media users feared the worst and believed that the United States was under a "cyber attack." The following day, the affected mobile carrier issued a statement about the incident, citing a leased fiber circuit failure as the culprit. This incident highlights the increasing need for people to scrutinize sources and wait for additional information before jumping to conclusions and propagating the spread of misinformation.

Patches and Updates

Adobe Releases Security Updates for Multiple Products

Google Releases Security Updates for Chrome

[WordPress Releases Security and Maintenance Update]

ICS-CERT Advisories

[Mitsubishi Electric MELSEC iQ-R series (Update A)]

[OSIsoft PI Web API 2019]

[Philips IntelliBridge Enterprise IBE]

[Rockwell Automation FactoryTalk Linx Software]

[Treck TCP/IP Stack]

We welcome your feedback.

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

Receive this email from a friend or colleague and want to subscribe? Sign up here!

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-06-038

HSEC-1 | NTIC SIN No. 2.5, 5.4

June 25, 2020

National Capital Region Cyber Threat Spotlight

Threat Actors Increasingly Targeting Microsoft Exchange Servers

The Microsoft Defender ATP Research Team has observed threat actors increasingly target and attack Microsoft Exchange servers in an effort to gain unauthorized access into networks and steal account credentials. These threat actors typically target Exchange servers in one of two ways, either by gaining access to an endpoint that allows them to move laterally through the network until they reach the target server or by locating an vulnerable or misconfigured server that is exposed to the open internet. Improperly configured, vulnerable, and exposed servers pose a high risk to enterprise networks as they can allow an attacker an entry point to steal data and deploy destructive malware such as ransomware. ***The NTIC Cyber Center recommends all Exchange server administrators keep their servers updated with the latest security patches, use a reputable and up to date antivirus software solution, place servers behind a firewall, regularly audit user accounts for unauthorized privilege escalation or access, and protect accounts by enabling multifactor authentication.***

Federal Partner Announcement

CISA Releases COVID-19 Election Security Resources

In response to COVID-19 consequences on election operations and administration, the Cybersecurity and Infrastructure Security Agency (CISA) is working with election officials and government and industry partners to ensure upcoming elections are accessible and secure, and that voters can safely cast their votes.

CISA supported the development of the Election Security Subsector Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) resources which are on the U.S. Elections Assistance Commission website.

CISA's Protect2020 webpage provides the latest government and industry resources and up-to-date information on how to assess risk, secure election infrastructure systems, and respond to cyber-related incidents. Learn how to manage inbound/outbound ballots, prepare electronic ballot delivery and marking, ensure signature verification, and more.

Explore these resources and more at https://go.usa.gov/xw4Nd.

Current and Emerging Cyber Threats

Phishing Campaign Masquerades as Wells Fargo to Deliver Malicious Calendar Invites

Researchers from Abnormal Security discovered a phishing campaign that leverages fraudulent calendar invites targeting Wells Fargo customers. Threat actors are masquerading as the Wells Fargo Security Team and threatening recipients with an account suspension if they do not update their security. Recipients are urged to click an attached .ics calendar file that, when opened, redirects victims to a phishing page designed to harvest user credentials. Additionally, recipients are encouraged to open the .ics file on their mobile devices so that it may be automatically added to the mobile calendar in order to appear more legitimate. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns disguised as official Wells Fargo 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.***

Vulnerabilities

Cisco WebEx Meetings

Cisco's Webex Meetings application on Windows devices has a newly discovered vulnerability (CVE-2020-3347) that could allow local authenticated attackers the ability to gain access to personal and sensitive information. This vulnerability exposes a shared memory space where threat actors are able to view highly sensitive information including authentication tokens, usernames, and meeting information that could be stolen or used to log in using the victim's WebEx account. Security researchers found that improperly securing trace files will expose e-mail accounts, URLs used to host meetings, as well as the WebExAccessToken, so that threat actors can gain access to the victim's WebEx account. Cisco has since released a patch for CVE-2020-3347. ***The NTIC Cyber Center recommends administrators of Cisco's Webex Meetings clients update to the latest version as soon as possible.***

USB for Remote Desktop

Researchers from SentinelOne uncovered a vulnerability for the bus driver for "USB for Remote Desktop" developed by FabulaTech that may allow threat actors to elevate privileges on a target machine by adding fake devices. This vulnerability, known as CVE-2020-9332, is attributed to the absence of security checks that block access from less privileged entities in FabulaTech's bus driver, IoCreateDevice. Since the driver labels IoCreateDevice as routine, it grants non-privileged users the ability to add and control software trust devices. Additionally, FabulaTech features extensive privileges on the computer as services are run under the LocalSystem account. FabulaTech released a fix to remediate the flaw. ***The NTIC Cyber Center urges affected FabulaTech customers to upgrade "USB for Remote Desktop" to the latest build.***

NETGEAR R6700 WiFi Router

NETGEAR discovered a zero-day vulnerability with their R6700 WiFi routers that allows threat actors to bypass authentication on adjacent networks. This vulnerability exists within the httpd (HTTP Daemon) service on port 80 where the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length creates a stack-based buffer overflow condition. Threat actors can leverage this vulnerability to execute code in the context of root. At this time, NETGEAR has not issued a patch to resolve this issue. ***As the vulnerability currently remains exploitable, the NTIC Cyber Center recommends discontinuing the use of the R6700 WIiFi Router and remove any device affected from within your environment until a patch resolving the issue is released.***

Data Breaches and Leaks

Twitter Billing Data Leak

Twitter has recently disclosed a breach resulting in the exposure of billing data belonging to Twitter advertisers. The exposed data includes email addresses, phone numbers, the last four digits of credit card numbers, and billing addresses. The breach is attributed to a bug that stored the sensitive data into the browser cache making it accessible to other users on the computer. Twitter has since then fixed the bug. It is unknown if any threat actors abused the exposed data. ***The NTIC Cyber Center recommends affected Twitter business 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. We also recommend affected Twitter business customers to clear their web browser cache.***

#BlueLeaks

On June 19, 2020, the NTIC Cyber Center became aware of a data breach impacting several fusion centers, law enforcement agencies, and government organizations across the United States. Since that time, we have been working with our counterparts in the National Fusion Center Association and Cyber Intelligence Network to identify the source of the breach and determine the scope and impact to our stakeholders. We have been providing relevant stakeholders with updates to the ongoing situation. If you are relevant public sector stakeholder who recently subscribed to our distribution list and would like a copy of our most recent update, please send an email to NTICCyberCenter@dc.gov with your request.

Upcoming Webinars

How to Secure Remote Works for the Long Haul: Protecting VPN, RDP, Webcams, and Beyond

Recent, rapid transformations in remote work have been challenging for enterprises, and for some of them, the new work-from-home reality is going to become a permanent adaption for their business.

Those that adapted quickly now need to look at keeping their new remote workforces happy and secure for the long haul. Join this webinar to learn about some of the biggest changes businesses have experienced, and how they're working to secure the new shifting and expanding attack surface, including:

- 88 percent of respondents rely on VPN tunneling for their work, but how are those VPN tunnels secured at scale?
- 30 percent rely on RDP, a protocol notorious for being abused by attackers. How are businesses assuring that RDP sessions are legitimate, and being used securely?
- Only ~13percent of respondents indicated that their organization fully manages webcams in their environment. How are businesses ensuring that sensitive, connected devices and IoT in workers' homes aren't providing a vector for stealthy attackers?

To register for this free webinar on Thursday, June 25 at 3:30 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.

Utility scams are fraudulent acts conducted by profit-motivated criminals who impersonate 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. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Why Did This Bank of America Phishing Email Bypass Spam Filters?
Analytic Comment: Bank of America phishing emails have bypassed security controls despite typical phishing signs, such as fraudulent email addresses, URLs, and graphic designs. Threat actors are leveraging email marketing platforms such as SendGrid for distribution as they use technologies such as SPF, DKIM, and DMARC that facilitate email authentication and integrity. Additionally, these emails are distributed in low volumes as to not trigger Microsoft's email security and Secure

Email Gateway (SEG), and feature SSL certificates that have yet to be flagged as malicious. This highlights the importance of remaining vigilant to incoming email and its validity despite current advanced email security features.

Cyber-Attacks Increasingly Threaten Schools - Here's What to Know

Analytic Comment: Cybersecurity researchers have noticed a rise in cyber-attacks focused on the education sector as teachers are using technology more frequently to provide remote education. Microsoft Security Intelligence researchers discovered that 61 percent of enterprise malware encounters came from the education sector, making it the most affected industry in the last 30 days. This cybersecurity gap in the education sector stems from a large number of school districts not having full-time employees assigned to effectively manage cybersecurity expectations. Without available cybersecurity staff or training, most teachers are left susceptible to phishing attacks. Threat actors are aware of the flaws and view this sector as an easy target, highlighting the urgent need of proper funding for cybersecurity resources in the education sector.

Turn on MFA before Crooks Do It for You

Analytic Comment: Threat actors are enabling multifactor authentication (MFA) on accounts not previously enabled in order to compromise them. MFA provides an extra layer of security by allowing customers to secure their accounts against fraudulent login attempts using unique codes delivered through email, text message, or phone call. However, if an account is already compromised, threat actors may enable this feature on a device they control, thereby denying account access to the rightful owner. In one such case in which a victim's Xbox account was compromised, the victim was unable to recover their account as the threat actor changed its associated email address and enabled MFA, thus blocking access. Additionally, the victim was unable to use their account recovery codes as well because the threat actor enabled MFA, rendering the codes useless. This underscores the importance of generating strong and unique passwords for every account and implementing MFA on all accounts that offer it as soon as they are created.

Patches and Updates

Adobe Releases Security Updates for Magento

Cisco Releases Multiple Security Updates

Drupal Releases Security Updates

Google Releases Security Updates for Chrome

Microsoft Releases Security Updates for Windows

VMware Releases Security Updates for Multiple Products

ICS-CERT Advisories

ABB Device Library Wizard

Baxter ExactaMix (Update A)

Baxter Phoenix Hemodialysis Delivery System (Update A)

Baxter PrismaFlex and PrisMax (Update A)

Baxter Sigma Spectrum Infusion Pumps (Update A)

BD Alaris PCU (Update A)

BIOTRONIK CardioMessenger II

Honeywell ControlEdge PLC and RTU

Johnson Controls exacqVision

Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L and FX Series CPU Modules

---

We welcome your feedback.

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

Receive this email from a friend or colleague and want to subscribe? Sign up here!

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-06-046

HSEC-1 | NTIC SIN No. 2.5, 5.4

July 2, 2020

National Capital Region Cyber Threat Spotlight

Daily Brute-Force Attacks Against RDP Nearly Doubled during Pandemic

As the COVID-19 pandemic forced employees across the United States to work from home, cyber threat actors increasingly targeted Windows Remote Desktop Protocol (RDP) services to gain access into enterprise networks. Cybersecurity firm ESET recorded telemetry data showing that, beginning in February 2020, brute-force attacks against RDP services rose to 80,000 per day. Organizations that did not enforce strong password policies or provide multifactor authentication were more vulnerable to these types of attacks. Once attackers gain access, they often steal data or deploy malware such as ransomware to further victimize their targets. ***The NTIC Cyber Center recommends all enterprise administrators proactively block connections to unneeded RDP ports, enforce strong password policies for all employees, enable multifactor authentication for all user accounts, and require the use of a Virtual Private Network (VPN) to connect to internal resources. We also recommend monitoring networks for suspicious activity and unauthorized access.***

Federal Partner Announcement

Defending Against Malicious Cyber Activity Originating from Tor

This advisory—written by the Cybersecurity Security and Infrastructure Security Agency (CISA) with contributions from the Federal Bureau of Investigation (FBI)—highlights risks associated with Tor, along with technical details and recommendations for mitigation. Cyber threat actors can use Tor software and network infrastructure for anonymity and obfuscation purposes to clandestinely conduct malicious cyber operations.

Tor (aka The Onion Router) is software that allows users to browse the web anonymously by encrypting and routing requests through multiple relay layers or nodes. This software is maintained by the Tor Project, a nonprofit organization that provides internet anonymity and anti-censorship tools. While Tor can be used to promote democracy and free, anonymous use of the internet, it also provides an avenue for malicious actors to conceal their activity because identity and point of origin cannot be determined for a Tor software user. Using the Onion Routing Protocol, Tor software obfuscates a user's identity from anyone seeking to monitor online activity (e.g., nation states, surveillance organizations, information security tools). This is possible because the online activity of someone using Tor software appears to originate from the Internet Protocol (IP) address of a Tor exit node, as opposed to the IP address of the user's computer.

CISA and the FBI recommend that organizations assess their individual risk of compromise via Tor and take appropriate mitigations to block or closely monitor inbound and outbound traffic from known Tor nodes. For more information, please see CISA Alert AA20-183A.

Current and Emerging Cyber Threats

New Lucifer DDoS Malware Exploits Windows Vulnerabilities to Build Botnets

Palo Alto Networks Unit 42 research group uncovered a new botnet variant, dubbed Lucifer, which is a cryptojacking and distributed denial-of-service (DDoS) malware hybrid that exploits vulnerabilities to propagate through networks and conduct malicious activities on Windows platforms. Once a system is compromised with Lucifer, threat actors may execute arbitrary commands and spread through the network via weaponized exploits. While numerous patches have hindered Lucifer, some variants feature anti-analysis protection. ***The NTIC Cyber Center***

recommends all network and system administrators change default passwords to include a strong variety, monitor networks for suspicious activity, and ensure that all software, including operating systems, are patched and up-to-date.

Phishing Campaign Targets Employees Returning to the Office

Researchers at Security firm Check Point have been investigating an ongoing phishing campaign that is targeting the Microsoft credentials of employees returning to their offices using a malicious email that promises COVID-19 training material. Recipients of this phishing campaign receive an email welcoming workers back to the office, promoting testing programs and new workplace social distancing rules, often containing a malicious link. If clicked, the link delivers victims to a malicious website designed to steal their Microsoft login credentials. Researchers have also determined that the number of coronavirus-related cyberattacks have decreased 130,000 per week during the first week of June, a drop of 24 percent from the average number in May. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns disguised COVID-19 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.***

Android Apps Discovered Stealing Facebook Login Credentials

The Google Play app store recently removed 25 Android applications that were found to be stealing Facebook login credentials. The malicious applications offered legitimate functions posing as step counters, image editors, video editors, wallpaper apps, flashlight applications, file managers, and mobile games. These apps contained malicious code that detected what other applications a user recently opened and, if it detected the use of Facebook, it would load a fraudulent Facebook login page over the existing display to trick victims into divulging their credentials. ***The NTIC Cyber Center recommends Android users that have installed any of the listed applications immediately delete them and then change their passwords to their Facebook account and any other accounts that use the same credentials. We always recommend using passwords that are unique to each account.***

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.

WastedLocker Targets US Organizations

A new ransomware dubbed WasteLocker is being leveraged to target US businesses and extort millions of dollars. Created by the Russian cybercrime group known as Evil Corp or Indrik Spider, WastedLocker has already compromised at least 31 companies, eight of which are Fortune 500 companies. WastedLocker initially compromises targets via fraudulent software updates hosted on hijacked websites. Once compromised, WastedLocker combines the word “wasted” with the company's initials to generate an extension that is appended to a victim's encrypted files. There is currently no publicly available decryption tool for this variant. More information, including indicators of compromise (IoCs) are available in Symantec's report.

EvilQuest Targets MacOS

EvilQuest, a new data-wiping and information-stealing malware is using ransomware as a decoy to target and steal files from macOS users. Victims compromised in this campaign become infected after unknowingly downloading a malicious trojan installer from popular applications obtained through torrent sites. EvilQuest is capable of identifying whether the MacOS instance is running in a virtual machine, and can also identify the presence of common security tools and antimalware solutions. It also opens a reverse shell used for communicating with its command-and-control (C2) server. After the MacOS system becomes comprised, EvilQuest deploys an altered copy of itself and encrypts files attaching a BEBABEDD marker at the end. It then displays a ransom note demanding $50 worth of Bitcoin to be paid within three days to recover encrypted files.

Vulnerabilities

Palo Alto Networks

The US Department of Homeland Security and US Cyber Command are highlighting a patch released by Palo Alto Networks that, if not applied, would allow threat actors “with network access” to exploit vulnerability CVE-2020-2021 for the purposes of obtaining sensitive information. CVE-2020-2021 is attributed to a flaw in the improper verification of signatures in PAN-OS and Security Assertion Markup Language (SAML) in which improper configuration allows unauthenticated network-based threat actors unfettered access without credentials. The US National Institute of Science and Technology rated the vulnerability a 10.0 in its National Vulnerability Database. ***The***

NTIC Cyber Center recommends administrators of affected Palo Alto Network systems apply the patch as soon as possible.

Data Breaches and Leaks

LG Electronics

LG Electronics has been allegedly compromised by Maze ransomware resulting in the theft of 40 GB of proprietary data, including source code. The threat actors behind this operation have issued a statement saying that they will disclose part of the stolen source code. The initial attack vector is currently unknown. LG has yet to confirm if the alleged attack took place. ***The NTIC Cyber Center encourages all organizations maintain current data backups that are stored securely off the network, regularly audit third-party access to networks, and audit networks for unauthorized access and exposed ports, especially those that are used for remote access such as TCP port 3389. For a list of recommended strategies to reduce the risk of becoming a victim of a ransomware attack, please download the NTIC Cyber Center Ransomware Mitigation Guide.***

Lollicupstore

The largest US bubble tea supplier, Lollicupstore, experienced a breach resulting in the exposure of over 112 million client-related records. The exposed data includes client data such as names, email addresses, password tokens, shipping data, production logs, internal records and other data. The breach is attributed to an improperly exposed database that left the data publicly accessible. Lollicupstore has since then secured the database. It is unknown if any threat actors abused the exposed data. ***The NTIC Cyber Center recommends affected Lollicupstore business 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

Data Breach®
Prevention. Response. Notification. TODAY

Your Brand is Being Used as Bait - You Just Don't Know It Yet

Without ever confronting an organization's email perimeter, it's easy for cybercriminals to impersonate a brand on the internet. Even unsophisticated attackers can spoof your email domain or host a fake website designed to trick customers, suppliers and employees. Join us to learn about the tactics cybercriminals are using and how you can stop brand impersonation attacks in their tracks - often preventing them all together.

To register for this free webinar on Wednesday, July 15 at 6:30 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.

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

How Hackers Extorted $1.14 Million from University of California, San Francisco
Analytic Comment: The University of California San Francisco (UCSF) was recently victimized in a ransomware attack at the hands of the Netwalker ransomware group who extorted $1.14 million from the university. UCSF had been working on a cure for COVID-19 when their data, including associated medical research, was compromised and encrypted. The Netwalker variant is associated with at least two other university-related ransomware attacks in the past two months. This highlights the need for universities, especially those conducting high-profile scientific research, to strengthen their cybersecurity posture.

The More Cybersecurity Tools an Enterprise Deploys, the Less Effective Their Defense Is
Analytic Comment: New research from IBM indicates that enterprises that deploy over 50 cybersecurity tools rank themselves 8 percent lower in their ability to detect threats, and 7 percent

lower in their defensive capabilities than other companies using fewer tools. IBM's research states that, on average, enterprises maintain 45 cybersecurity tools and that bridging the gap that exists in planning and incident response testing should be the focus for enterprises that need to improve their defense posture. Fortunately, during the COVID-19 pandemic, many enterprises adopted Cyber Security Incident Response Plans (CSIRPs), which denotes an increase of 18 percent from five years ago.

Patches and Updates

Apache Releases Security Advisory for Apache Tomcat

Microsoft Releases Security Updates for Windows 10, Windows Server

Palo Alto Releases Security Updates for PAN-OS

ICS-CERT Advisories

Delta Industrial Automation DOPSoft

ENTTEC Lighting Controllers

Mitsubishi Electric Factory Automation Engineering Software Products

Philips Ultrasound Systems

Rockwell FactoryTalk Services Platform XXE

Rockwell FactoryTalk View SE

We welcome your feedback.

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

Receive this email from a friend or colleague and want to subscribe? Sign up here!

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-07-007

HSEC-1 | NTIC SIN No. 2.5, 5.4

July 9, 2020

National Capital Region Cyber Threat Spotlight

Valak Malware Targets Enterprise Networks

Researchers at Cisco Talos have identified threat actors distributing Valak malware worldwide via malicious email campaigns. Valak is a modular information-stealer that threat actors have leveraged to primarily target enterprises in the financial, manufacturing, health care, and insurance sectors and is usually delivered via malicious spam email campaigns with an attached password-protected ZIP archive. Threat actors use these ZIP archives as well as replies from existing email threads from compromised accounts to appear legitimate and to avoid security applications. The ZIP archive contains a malicious Microsoft Word attachment. The attachment urges recipients to click the *Enable Editing* and *Enable Content* functions and, if clicked, a malicious macro will be enabled to facilitate the delivery of Valak onto the victim's system. While the majority of these Valak malspam campaigns target enterprise users there have been attempts to target personal accounts as well. ***The NTIC Cyber Center recommends users remain vigilant for Valak 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 Valak notify your organization's***

IT security team immediately so they may contain and remediate the infection. Indicators of compromise (IoCs) associated with this campaign are available in Cisco's report.

Federal Partner Announcement

FBI Sees Spike in Fraudulent Unemployment Insurance Claims Filed Using Stolen Identities

The FBI has seen a spike in fraudulent unemployment insurance claims complaints related to the ongoing COVID-19 pandemic involving the use of stolen personally identifiable information (PII).

US citizens from several states have been victimized by criminal actors impersonating the victims and using the victims' stolen identities to submit fraudulent unemployment insurance claims online. The criminals obtain the stolen identity using a variety of techniques, including the online purchase of stolen PII, previous data breaches, computer intrusions, cold-calling victims while using impersonation scams, email phishing schemes, physical theft of data from individuals or third parties, and from public websites and social media accounts, among other methods. Criminal actors will use third parties or persuade individuals who are victims of other scams or frauds to transfer fraudulent funds to accounts controlled by criminals.

Many victims of identity theft related to unemployment insurance claims do not know they have been targeted until they try to file a claim for unemployment insurance benefits, receive a notification from the state unemployment insurance agency, receive an IRS Form 1099-G showing the benefits collected from unemployment insurance, or get notified by their employer that a claim has been filed while the victim is still employed.

For more information, along with mitigation recommendations, please see the FBI's July 6, 2020 press release here.

Current and Emerging Cyber Threats

Cosmic Lynx BEC Cybercrime Group

Researchers at Agari discovered a Russian business email compromise (BEC) cybercrime organization known as Cosmic Lynx. Operating undiscovered for at least a year, Cosmic Lynx has been involved in over 200 BEC scams targeting executives in 46 countries. Cosmic Lynx conduct sophisticated BEC campaigns as compared to other threat actors because they use professional jargon and target organizations without DMARC policies that facilitate email authentication and integrity. ***The NTIC Cyber Center recommends maintaining awareness of BEC schemes and scrutinizing any financial request that includes a change in normal, expected procedures. We highly recommend verifying all payment procedure changes with multiple people in your organization and contacting the sender via another means of communication, such as a direct phone call, to verify the legitimacy of the request. Additionally, we urge organizations to employ technologies such as SPF, DKIM, and DMARC to facilitate email authentication and integrity***.

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.

Avaddon Ransomware Exploits Excel 4.0 Macros

Researchers at Microsoft Security Intelligence recently highlighted a malicious email campaign that delivers Avaddon ransomware embedded in emails masquerading as official correspondence. Primarily targeting users in Italy, threat actors are distributing Avaddon via phishing emails that contain Microsoft documents embedded with a malicious Excel 4.0 macro. Once enabled, the malicious macro delivers Avaddon directly to the system without the need of a separate downloader. ***The NTIC Cyber Center recommends users remain vigilant for malicious emails disguised as official 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.

Try2Cry

A G DATA malware analyst has discovered a new ransomware variant dubbed "Try2Cry" that compromises Windows devices by initially infecting a USB flash drive and leveraging files that pose as shortcut links to the target's files to infect victims. This campaign also uses the default Windows icon folder and Arabic names as a lure, hoping to catch curious victims when the ransomware makes copies of itself onto the USB. Once a system is infected, the ransomware appends *.Try2Cry* to the names of encrypted files. The malware used in this campaign is a .NET ransomware with a variant of the open-source Stupid ransomware family that is commonly associated with low-skilled malware engineers. Try2Cry can be decrypted without paying the ransom. More information is available on BleepingComputer's website.

Vulnerabilities

.NET Core

A researcher from Context Information Security discovered a vulnerability in .NET Core that allows threat actors to launch malicious programs while evading detection from security applications. The vulnerability is attributed to a path traversal bug in Microsoft's .NET Core library, allowing malicious garbage collection dynamic link libraries (DLLs) to be loaded by users with low privileges. This bug affects the latest stable release of .NET Core and a patch or workaround is currently not available. Microsoft does not categorize this flaw as vulnerability as threat actors would need to have the ability the set environmental variables on a compromised system. ***The NTIC Cyber Center recommends system administrators immediately use official patches and workarounds if and when they become available. If you believe your system has been compromised, notify your organization's IT security team immediately.***

Exposed Printer IPP Ports

Security researchers have been investigating an Internet Printing Protocol (IPP) exposure of an estimated 650,000 -700,000 printers leaking device names, locations, models, firmware versions, organization names, and WiFi SSIDs daily. IPP is a secure printing communication protocol that supports advanced features like access control lists, authentication, and encrypted communications; however, the device owner must implement these features or risk threat actors obtaining this information through reconnaissance efforts. The information leaked from an exposed IPP port (TCP/631) can be used by threat actors to search through enterprise networks for future attacks. ***The***

NTIC Cyber center recommends that printer owners and administrators follow their printers' manuals to configure IPP properly and enable authentication, encryption, and limit access to the printer using access control lists. We also recommend blocking unneeded access to TCP port 631 at the perimeter firewall.

Upcoming Webinars

COVID-19 Response: Lessons Learned on Cybersecurity and Resilience in a Pandemic

Next Wednesday, join the Cybersecurity and Infrastructure Security Agency, the Regional Consortium Coordinating Council, and the State, Local, Tribal, and Territorial Government Coordinating Council for a webinar on cybersecurity and resilience lessons learned during the COVID-19 pandemic.

COVID-19 has forced state and local governments to rapidly change how they operate and adapt to a volatile new environment. Next Wednesday, join state, local, and federal government officials as they discuss lessons learned thus far about securing our communities during a pandemic -- including protecting our remote workforce and defending against cyber criminals and phishing campaigns.

To register for this free webinar on Wednesday, July 15 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.

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

One out of Every 142 Passwords is "123456"

Analytic Comment: A computer engineering student conducted a study analyzing over one billion leaked credentials. The results revealed that one out of every 142 passwords was "123456." While experts recommend a password length of at least 16 characters, the analysis revealed an average passwords length of 9.48 characters. Additionally, there was a lack of password complexity as only 12 percent of the analyzed passwords contained a special character. This highlights the need for 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.

Schools Already Struggled with Cybersecurity. Then Came COVID-19.

Analytic Comment: The COVID-19 crisis has exacerbated the cybersecurity deficiencies in the US education sector. Current problems of maintaining skilled personnel and maintaining secure systems have yet to be addressed while online education has become more commonplace. These factors combined with unsecured third-party education platforms provide multiple prime attack vectors that threat actors may exploit. According to Microsoft's Global Threat Activity tracker, more than 4.7 million malware incidents were detected in the global education industry in the past 30 days highlighting the urgent need of proper funding for cybersecurity resources in the education sector.

Patches and Updates

Cisco Releases Security Updates for Multiple Products

Citrix Releases Security Updates

Mozilla Releases Security Updates for Firefox and Firefox ESR

Samba Releases Security Updates

[VMware Releases Security Update for VeloCloud]

ICS-CERT Advisories

[ABB System 800xA Information Manager]

[Grundfos CIM 500]

[Mitsubishi Electric GOT2000 Series]

[Nortek Linear eMerge 50P/5000P]

[OpenClinic GA]

We welcome your feedback.

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

Receive this email from a friend or colleague and want to subscribe? Sign up here!

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

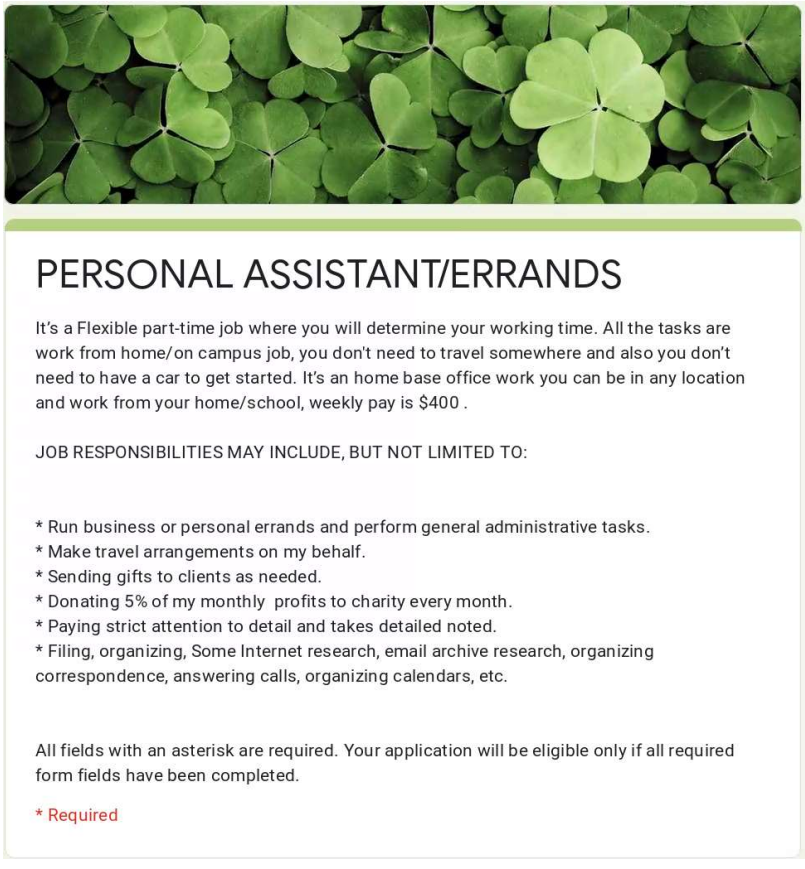
TLP:WHITE

Product No. 2020-07-017

HSEC-1 | NTIC SIN No. 2.5, 5.4

July 16, 2020

National Capital Region Cyber Threat Spotlight



PERSONAL ASSISTANT/ERRANDS

It's a Flexible part-time job where you will determine your working time. All the tasks are work from home/on campus job, you don't need to travel somewhere and also you don't need to have a car to get started. It's an home base office work you can be in any location and work from your home/school, weekly pay is $400 .

JOB RESPONSIBILITIES MAY INCLUDE, BUT NOT LIMITED TO:

* Run business or personal errands and perform general administrative tasks.
* Make travel arrangements on my behalf.
* Sending gifts to clients as needed.
* Donating 5% of my monthly profits to charity every month.
* Paying strict attention to detail and takes detailed noted.
* Filing, organizing, Some Internet research, email archive research, organizing correspondence, answering calls, organizing calendars, etc.

All fields with an asterisk are required. Your application will be eligible only if all required form fields have been completed.

* Required

Phishing Campaign Targets Government Agency, Promotes Possible Money Mule/Reshipping Scheme

The NTIC Cyber Center recently received a report of a phishing campaign targeting a DC government agency, promoting a possible "money mule" or "reshipping" scheme to potential job-seekers looking for work-at-home opportunities. The subject line of the phishing emails includes the

words *(JOB REFERRAL):Employment Opportunity* and the body of the email contains the following verbiage:
Due to the ongoing and dynamic nature of the COVID-19 (corona virus) outbreak, and in the interest of our community,you are invited to participate in a Part-time work offer,all the tasks are from home. Click here to find out more about this role.

It also contains an embedded link that, if clicked, leads to a phishing page hosted via Google Docs that advertises an open job position as a personal assistant with a list of job responsibilities. The landing page then provides fields for job-seekers to enter their name, mailing address information, email address, phone number, gender, and current occupation. The job ad contains several grammatical and spelling errors and includes a stock photo of clovers.

The email was sent using a compromised agency email account, suggesting that the perpetrators of this campaign are actively exploiting compromised enterprise email accounts to bypass email security gateways and add legitimacy to the scheme.

As the COVID-19 pandemic has resulted in job loss and financial instability for many people across the United States, the NTIC Cyber Center would like to remind all members to maintain awareness of this threat and to educate friends and family to help them avoid falling victim to this and similar scams. To learn more about how to identify and protect yourself from these types of schemes, please read our blog post titled Securing Our Communities: Money Mule Scams.

Federal Partner Announcement

Critical Vulnerability in SAP NetWeaver AS Java

On July 13, 2020 EST, SAP released a security update to address a critical vulnerability, CVE-2020-6287, affecting the SAP NetWeaver Application Server (AS) Java component LM Configuration Wizard. An unauthenticated attacker can exploit this vulnerability through the Hypertext Transfer Protocol (HTTP) to take control of trusted SAP applications.

Due to the criticality of this vulnerability, the attack surface this vulnerability represents, and the importance of SAP's business applications, the Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends organizations immediately apply patches. CISA recommends organizations prioritize patching internet-facing systems, and then internal systems.

Organizations that are unable to immediately patch should mitigate the vulnerability by disabling the LM Configuration Wizard service (see SAP Security Note #2939665). Should these options be unavailable or if the actions will take more than 24 hours to complete, CISA strongly recommends closely monitoring your SAP NetWeaver AS for anomalous activity.

CISA is unaware of any active exploitation of these vulnerabilities at the time of this report. However, because patches have been publicly released, the underlying vulnerabilities could be reverse-engineered to create exploits that target unpatched systems.

For more information, along with mitigation recommendations, please see CISA's Alert AA20-195A.

Microsoft Addresses "Wormable" RCE Vulnerability in Windows DNS Server

Microsoft has released a security update to address a remote code execution (RCE) vulnerability—CVE-2020-1350—in Windows DNS Server. A remote attacker could exploit this vulnerability to take control of an affected system. This is considered a “wormable” vulnerability that affects all Windows Server versions.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review Microsoft’s Security Advisory and Blog for more information, and apply the necessary update and workaround.

Current and Emerging Cyber Threats

Fraudulent Zoom Suspension Alerts

Researchers at the email security company Abnormal Security discovered a phishing campaign that uses fake Zoom notifications as a lure in a targeted cyber attack against corporate Microsoft Office 365 users to steal their credentials. The email used in this campaign impersonates an automated Zoom notification that warns users that their accounts have been suspended and urges them to click an “Activate Account” link. Once clicked, victims are directed to a phishing page where they are asked to input their Outlook credentials. The credentials are then sent to the threat actors server to be sold or reused to further compromise a network. What makes this campaign exceedingly persuasive is the use of a spoofed email address and an email body almost free of any grammatical or typographical errors making it potentially more effective against remote workers who attend daily online meetings. ***The NTIC Cyber Center recommends users remain vigilant for email phishing campaigns disguised as Zoom notifications, avoid opening unexpected emails, and refrain from***

clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. If you believe you have been targeted by this campaign, notify your organization's IT security team immediately.

Pre-Installed Malware Discovered on ANS UL-40 Mobile Phone

Malwarebytes researchers discovered another unremovable malware that is pre-installed on Virgin Mobile phones that are provided to low-income users from the government-funded Lifeline Assistance program. The first discovery was reported in January when Malwarebytes discovered Chinese malware on the Unimax U683CL, and now, ANS (American Network Solutions) UL40 has been discovered to have no fewer than two instances of embedded malware on them, marking this the second time this year. The pre-installed malware has the capability to automatically install applications without the user's permission or knowledge, leaving the device exposed to other potential malware installations. ***The NTIC Cyber Center recommends either decommissioning and replacing affected devices or uninstalling the WirelessUpdate for Current User using the instructions provided in the Malwarebytes*** *report*.

"Keeper" Magecart Threat Group Targets Online Merchants

Researchers from Gemini Advisory predict that the threat actors known as the "Keeper" Magecart group will conduct complex campaigns against online merchants globally in the next few months. Magecart group threat actors leverage Magecart payment skimmers – malicious code that enables the theft of customer payment card information from ecommerce stores and other websites. Keeper has already targeted over 570 victim e-commerce sites in 55 countries and its criminal enterprise consists of 64 attacker domains and 73 exfiltration domains. They have been observed to evolve their methods such as using more complex obfuscation methods to avoid detection. ***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*.

New Mirai Variant Exploits CVE-2020-10173

Researchers at Trend Micro discovered a new malware variant for Mirai, dubbed IoT.Linux.MIRAI.VWISI, that exploits nine vulnerabilities. These vulnerabilities affect various

internet-connected cameras, smart TVs, and routers and allow threat actors to conduct shell command execution and remote code execution, brute forcing and other malicious activities. A vulnerability not seen in previous Mirai variants, CVE-2020-10173, is a multiple authenticated command injection vulnerability found in Comtrend VR-3033 routers. While researchers have not observed any indications to date that the CVE-2020-10173 has been exploited by attackers in the wild, new variants show that threat actors are continuously upgrading their capabilities. ***The NTIC Cyber Center recommends network administrators keep all systems and software up-to-date with the latest security patches and to proactively block the IoCs provided in Trend Micro's report***.

M00nD3V Logger Trojan Discovered

Researchers at Zscaler ThreatLabZ detected a multifunctional information-stealing Trojan dubbed "M00nD3V Logger." M00nD3V Logger features the ability to steal passwords from 42 applications, gain access to the victim's webcam, copy clipboard contents, and capture keystrokes. It also functions as a botkiller, an antivirus killer, and can communicate over a SMTP/FTP/proxy and download additional plugins. Threat actors distribute M00nD3V to victims through various spam emails masquerading as legitimate businesses. The malware unpacks the encrypted payload using multibyte XOR decryption and null bytes in the XOR key leaving some bytes not ciphered. ***The NTIC Cyber Center recommends users always update systems and software with the latest security patches, remain vigilant for phishing campaigns, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. If you believe you have been targeted by this campaign, notify your organization's IT security team immediately***.

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.

AgeLocker Ransomware

A new ransomware variant, dubbed "AgeLocker," encrypts victims' files using Google's "Age" encryption tool. This encryption tool adds a text header that starts with the URL "age-

encryption.org" to each encrypted file and was created by a Google employee to replace GPG (GNU Privacy Guard) that encrypts files, backups, and streams and uses AES (Advanced Encryption Standard) + RSA (Rivest–Shamir–Adleman) algorithms. It is currently unknown how these threat actors are gaining access to their victims' devices but, after encryption process is finished, victims receive an email with the instructions on how to submit the ransom payment and obtain the decryption tool. There is currently no publicly available decryption tool for this variant.

Vulnerabilities

KingComposer WordPress Plugin

An active drag-and-drop page development WordPress plugin named KingComposer has a cross-site scripting (XSS) vulnerability (CVE-2020-15299) that has affected nearly 100,000 websites. This vulnerability can be exploited when threat actors use base64-encoding on a malicious payload and trick the victim into clicking a malicious link, which sends a request through a *kc-online-preset-data* parameter and allows the malicious payload to execute on the victim's web browser. ***The NTIC Cyber Center recommends WordPress website administrators who installed the KingComposer plugin to update it immediately. Changing the affected website's administrator password, enabling two-factor authentication, and properly vetting all plugins prior to and after installation are also recommended.***

C-Data Fiber-To-The-Home Optical Termination Devices

Researchers found severe vulnerabilities in 29 Fiber-To-The-Home Optical Line Termination (FTTH OLT) devices from Chinese equipment vendor C-Data. FTTH OLT is networking equipment that enables internet service providers (ISPs) to bring fiber optics as close to the end-users as possible. The vulnerabilities are found within the firmware of these FTTH OLT devices, the most severe of which allows threat actors to access backdoors, execute shell commands with root privileges, view credentials, and crash services. The researchers believe the Telnet backdoor accounts, hardcoded in the firmware, were intentionally put in place by the vendor. C-Data has yet to make an official statement. ***The NTIC Cyber Center recommends both public and private sector organizations decommission all affected devices and remove them from their networks as soon as possible.***

Data Leaks and Breaches

liveauctioneers

Auction site LiveAuctioneers has disclosed a data breach comprised of 3.4 million stolen user records after a threat actor posted it on a hacker forum for sale. Information compromised in the breach allegedly includes names, phone numbers, physical addresses, email addresses, usernames, IP addresses, and social media profiles. The threat actor selling the information claims that three million of the included accounts had their passwords decrypted. Customers had their information compromised on June 19, 2020 via security breach at a LiveAuctioneers data processing partner. LiveAuctioneers believes that credit card information and bidding history were not affected. ***The NTIC Cyber Center recommends that LiveAutioneers users monitor their accounts for any unauthorized or suspicious activity, change their credentials, and enable multifactor authentication on any account that offers it.***

Cybersecurity Training Opportunity

EAC Announces Online Cybersecurity Training for Election Officials

The US Election Assistance Commission (EAC) is offering free, self-paced, online cybersecurity training to election officials in all state, local, tribal, and territorial (SLTT) election offices. The training is tailored for election officials, and "provides foundational knowledge on cybersecurity terminology, best practices in election offices, practical application, and communication." The training, developed by the Center for Tech and Civic Life (CTCL), consists of both video and written material, and is made up of three modules:

1. Cybersecurity 101 offers a foundation of cybersecurity terminology and improvements to login practices."
2. Cybersecurity 201 introduces the National Institute of Standards and Technology (NIST) framework.
3. Cybersecurity 301 focuses on communication around an office's cybersecurity efforts to increase public trust in elections.

The training is accessible through the EAC website.

Upcoming Webinars

How to Protect all AWS Services and Surfaces

Multiple layers of defense are required to protect your AWS environment. The first step is to reduce your overall attack surface to reduce exposure, in ways such as hardening your Amazon EC2 operating systems and configuring your containers. Organizations can then implement tools, such as a cloud security posture management (CSPM) solutions, to monitor and manage risk.

In this prerecorded webcast, SANS instructor Dave Shackleford and AWS Marketplace explore best practices and provide practical guidance on how you can secure your entire AWS footprint. They will also present real-world use cases and examples of tools you can leverage to protect your investments.

Attendees at this webcast will learn how to:

- Decrease their attack surface to limit exposure
- Protect their AWS environment with configuration management, real-time assessment, and access control mechanisms.
- Implement automation for monitoring and continuous protection
- Leverage AWS services and seller solutions in AWS Marketplace to protect AWS services and surfaces

To register for this free webinar on Tuesday, July 28 at 3:30 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.

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

How to Protect Your Verizon Number from SIM-Swapping Attacks

Analytic Comment: Verizon offers a way for customers to freely enable a Number Lock protection feature via My Verizon app or the My Verizon website. This change will make Verizon 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 two-factor authentication (2FA) methods. The Number Lock feature works by blocking the number from being ported to another line/carrier or swapped to another SIM unless disabled. Verizon Wireless customers are encouraged to enable Number Lock on their accounts as soon as possible to reduce the risk of becoming victimized in a SIM-swapping attack.

Barack Obama, Joe Biden, Elon Musk, Apple, and Others Hacked in Unprecedented Twitter Attack

Analytic Comment: Several high-profile, verified Twitter accounts were compromised to display posts promoting cryptocurrency scams on July 15, 2020. Shortly after investigating the coordinated hack, Twitter revealed that an internal employee tool was used to exploit the various accounts. Twitter also identified a social engineering campaign that targeted the company's employees, which likely allowed the unidentified threat actors to gain access to accounts with elevated privileges. This incident highlights the importance of educating employees on how to identify and report social engineering attacks and regularly reviewing user account privileges, applying the principle of least privilege when possible.

Patches and Updates

Adobe Releases Security Updates for Multiple Products

Cisco Releases Security Updates for Multiple Products

Google Releases Security Updates for Chrome

Microsoft Releases July 2020 Security Updates

ICS-CERT Advisories

Advantech iView

Baxter PrismaFlex and PrisMax (Update B)

Capsule Technologies SmartLinx Neuron 2

Moxa EDR-G902 and EDR-G903 Series Routers

Siemens LOGO! Web Server

Siemens Opcenter Execution Core

Siemens SICAM MMU, SICAM T, and SICAM SGU

Siemens SIMATIC HMI Panels

Siemens SIMATIC S7-200 SMART CPU Family

Siemens UMC Stack

We welcome your feedback.

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

Receive this email from a friend or colleague and want to subscribe? Sign up here!

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-07-029

HSEC-1 | NTIC SIN No. 2.5, 5.4

July 23, 2020

National Capital Region Cyber Threat Spotlight

Emotet Resurfaces - Distributes TrickBot and Qbot/QakBot Trojans

After approximately five months of inactivity, the Emotet campaign resurfaced on July 17, 2020 distributing malware via large malicious email campaigns masquerading as payment reports, invoices, shipping information, and employment opportunities. Emotet is a sophisticated, modular banking Trojan that has previously been used in campaigns targeting various organizations throughout the United States. Initially, Emotet was designed solely to steal sensitive information from victims; however, it has been updated to include additional modules such as a money transfer system, a malicious email delivery service, and the ability to deliver additional malware, including ransomware, onto infected devices. Malicious emails delivering Emotet typically include a Word document containing malicious macros. If recipients open the attachment and enable the macros on a machine running the Windows operating system, Emotet will install itself on the machine and download additional malware. Reports indicate that the most recent Emotet campaign was observed downloading and installing either the TrickBot or Qbot/QakBot Trojans on infected systems. Both of these Trojans steal data such as banking information and login credentials, create backdoors into infected systems, and deliver additional malware - such as Ryuk or Conti ransomware - to victims. ***The NTIC Cyber Center recommends users keep software and operating systems up-to-date and encourage the use of a reputable and up-to-date anti-malware solution. Additionally, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. We also recommend enabling***

multifactor authentication on all online accounts, especially those associated with financial institutions, to prevent unauthorized access resulting from credential theft. If you believe you have been targeted by this campaign or infected with Emotet, TrickBot, or Qbot/QakBot, notify your organization's IT security team immediately.

Federal Partner Announcements

Malicious Activity Targeting COVID-19 Research, Vaccine Development

In response to malicious activity targeting COVID-19 research and vaccine development in the United States, United Kingdom (UK), and Canada, the Cybersecurity and Infrastructure Security Agency (CISA), UK's National Cyber Security Centre (NCSC), Canada's Communications Security Establishment (CSE), and the National Security Agency (NSA) released a Joint Cybersecurity Advisory to expose the threat. A malicious cyber actor is using a variety of tools and techniques to target organizations involved in COVID-19 research and vaccine development. Tools include SOREFANG, WELLMESS, and WELLMAIL malware.

CISA encourages users and administrators to review the Joint Cybersecurity Advisory and the following Malware Analysis Reports for more information and to apply the mitigations provided.

- SOREFANG
- WELLMESS
- WELLMAIL

CISA Releases Telework Guidance for Schools and Organizations

As the nation's risk advisor, the Cybersecurity and Infrastructure Security Agency (CISA) brings together its partners in industry and the full power of the federal government to improve American cyber and infrastructure security. To help secure schools and organizations during the unprecedented surge in telework and video conferencing, CISA recently released new telework guidance and resources.

The resources below are provided to assist organizations and teleworkers to be secure when working remotely.

- Guidance and Tips for Schools, Staff, and Students to Help Secure Video Teleconferencing
- General Guidance for Securing Video Conferencing

- Cybersecurity Recommendations for Federal Agencies Using Video Conferencing
- Cybersecurity Recommendations for Critical Infrastructure Using Video Conferencing
- National Security Agency (NSA) & DHS Telework Best Practices
- Video Conferencing Tips

Learn more on the CISA website.

Current and Emerging Cyber Threats

BlackRock Android Banking Trojan Discovered Targeting Social Media and Dating App Data

Researchers at ThreatFabric discovered an Android banking Trojan dubbed BlackRock that is known to steal credentials and credit card data from 337 apps. BlackRock is based on the Xerxes banking malware source code and targets social media, communication, networking, and dating platforms. Users are compromised via fraudulent Google Update requests that allow BlackRock to grant itself additional permissions. Additionally, BlackRock allows threat actors to log keystrokes, spam victims' contact lists, siphon system notifications, and block victims from using antivirus applications. ***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 updates. 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.***

Phishing Scam Masquerades as Bill & Melinda Gates Foundation

Researchers at Area 1 Security discovered an email phishing scam masquerading as the Bill & Melinda Gates Foundation. Threat actors are leveraging typosquatting – the deliberate use typographical errors or common misspellings to mimic legitimate organizations or domain names – in the originating email address to trick recipients. In this case, the threat actor registered gatesfoundatlon[.]com, using a lowercase “L” to resemble the “i” in “foundation.” The body of the email contains a fraudulent donation request in the form of Bitcoin. Additionally, the threat actor established an SPF record for the fraudulent domain to maintain consistent phishing distribution. ***The NTIC Cyber Center recommends users verify all charities and donation websites prior to submitting any personal or financial information. To read more about the threat of charity scams***

and for additional mitigation strategies, please read our blog post titled Securing Our Communities: Charity 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.

Conti Ransomware

Conti ransomware is reportedly the successor of the Ryuk ransomware variant given that it shares code, the ransom note template, and the Trickbot infrastructure with Ryuk campaigns. Conti has unique features such as anti-forensic capabilities that include applying string coding convention to almost every malware string text. Threat actors are able to snoop on the victim's network while conducting targeted attacks since Conti has command-line features. Conti can also leverage the Windows Restart Manger to unlock additional files and make them susceptible to encryption. More information about Conti ransomware is available on Bleeping Computer's website here.

BlackBaud Thwarted Ransomware Attack, Extorted for Deletion of Stolen Data

Cloud hosting provider BlackBaud reported that their cybersecurity team thwarted a ransomware attack before the malware started encrypting files, but still had to pay the ransom demand to ensure that threat actors would delete the data that was stolen from their network. BlackBaud's security team alongside independent forensics experts and law enforcement successfully prevented the ransomware attack and expelled the threat actors from the network, but not before the actors managed to steal data from the "self-hosted environment" where customers files were saved. BlackBad released a statement saying "Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed." At this time, there is no evidence to suggest the data was disseminated further or publicly released. However, this incident highlights the importance of encrypting data at rest as profit-motivated cyber threat actors are increasingly seeking opportunities to extort victims in multiple ways.

Nefilim Ransomware Targets French Telecommunications Firm

French telecommunications company Orange has confirmed that they were victims in a ransomware attack that resulted in threat actors accessing the data of 20 enterprise customers. The threat actors behind this attack belong to the Nefilim ransomware group who supposedly breached the company through their “Orange Business Solutions” division that offers businesses virtual hosting services. Nefilim leaked a 339MB archive file that was titled 'Orange_leak_part1.rar' that contained a snippet of the alleged exfiltrated data from Orange’s Business Solutions customer database. The company said it has informed affected customers and will continue to monitor and investigate the breach.

Vulnerabilities

Bluetooth Reconnection Flaw Impacting IoT Devices

Researchers at the Purdue University’s Center for Education and Research in Information Assurance and Security (CERIAS) discovered a vulnerability affecting numerous Bluetooth-enabled Internet-of Things (IoT) devices. This vulnerability allows threat actors to launch a spoofing attack and impersonate an IoT device and feed fraudulent data to a user’s device with forged data. This vulnerability is attributed to a design flaw in the reconnection procedure between two already paired devices that feature Bluetooth Low Energy (BLE), a low-energy communication protocol widely used in mobile and IoT devices. According to a recent study, application-layer security could defend against this flaw; however, one billion BLE devices do not incorporate application-layer security. A patch is available for iOS 13.4 and iPadOS 13.4 while other platforms have yet to receive a patch or workaround. ***The NTIC Cyber Center recommends users monitor BLE-enabled devices for unusual and suspicious activity and update their devices if and when a patch becomes available.***

Fast Chargers Vulnerable to BadPower Attack

A vulnerability has been discovered within the firmware of fast chargers that allows threat actors the ability to manipulate the default five voltage charging parameters into delivering more voltage than the receiving device can handle, damaging the user’s device. This type of attack has been labeled “BadPower” attack and the threat actor deploying this attack only needs to connect their attack rig to the fast charger for a few seconds, modifying the firmware to amplify voltages. After the victim connects their smartphone or laptop to the infected fast charger, a malicious code modifies the charger's firmware, and the fast charger will force a power overload that normally heats up, bends, melting, or even burns the connected device. The good and bad news behind this is that most of the BadPower vulnerabilities can be fixed by updating the device firmware, but 18 different chip vendors do not offer firmware update as an option. Reducing the risk of a BadPower attack includes hardening firmware to prevent unauthorized modifications, but also deploying overload protection

to charged devices***. The NTIC Cyber Center recommends that users deploy overload protection on mobile devices and updating firmware when possible to prevent unauthorized modifications.***

Data Leaks and Breaches

IT recruitment and staffing services agency, Collabera, has been compromised by Maze ransomware, resulting in the theft of employees' personal information. Information compromised in the breach includes employee names, physical addresses, Social Security numbers, dates of birth, employment benefit data, and passport and immigration visa details. The initial attack vector is currently unknown but Collabera has restored its systems via backup files. Affected employees were notified and were offered free credit monitoring services. ***The NTIC Cyber Center encourages those affected to consider placing a fraud alert or security freeze on their credit files with Equifax, Experian, or TransUnion. In addition, we advise activating the free credit and identity monitoring services offered to affected personnel before the deadline on October 31, 2020 and enabling multi-factor authentication (MFA) on all accounts that offer it.***

Cybersecurity researchers from WizCase discovered five e-learning platforms using misconfigured and unencrypted servers that left nearly one million user records accessible to anyone online. The five known companies affected by this vulnerability are Escola Digital, MyTopDog, Okoo, Square Panda and Playground Sessions. The data leaked from these servers contained personal information such as users' full names, email addresses, ID numbers, phone numbers, home addresses, dates of birth, and specific course and school information. ***The NTIC Cyber Center recommends e-learning users that have installed any of the listed applications immediately change their passwords to their accounts and any other accounts that use the same credentials. We always recommend using passwords that are unique to each account and enabling multifactor authentication on any account that offers it. Lastly, remain vigilant for any social engineering campaigns that may result from this data exposure.***

Upcoming Webinars

Closing the Critical Skills Gap for Modern and Effective Security Operations Centers (SOCs): Survey Results

Any successful security operations center (SOC) will combine skilled people, effective processes and efficient technology. Previous SANS surveys have shown that the skills of the people are the prime prerequisite to enable organizations to define critical SOC processes; create use cases, hypotheses and plans; architect effective security solutions; and efficiently deploy, operate and maintain security systems. From that skills base, sophisticated technology and tools can be used as a force multiplier. CISOs and SOC managers who can reduce or close their critical skills gaps have the highest probability of minimizing business impact from cyberattacks when budgets and staffing are constrained.

Webcast attendees will learn:

- Where hiring managers turn when sourcing potential new hires
- Which skill areas are most sought after
- What technologies employers wish new hires had hands-on experience using
- Which security technologies are perceived as enabling organizations to delay or mitigate the need for additional staff

To register for this free webinar on Thursday, July 30 at 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.

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. Perpetrators emotionally manipulate kind-hearted and generous individuals using sad stories and spoofed correspondence that appears legitimate. They target victims using email, social media, websites, voice messaging services, crowd funding platforms, and even in person. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Magento Adds 2FA to Protect against Card Skimming Attacks

Analytic Comment: The Adobe Security Operations team states that approximately 75 percent of all web skimming (also known as Magecart or e-skimming) attacks were a result of threat actors exploiting compromised administrator accounts to embed malicious scripts on Magento Commerce websites. Adobe has since added two-factor authentication (2FA) to the Magento platform to combat unauthorized logins for Magento.com accounts, Cloud Admin, and Magento Admin. In addition to configuring 2FA on their accounts, Magento administrators are also urged to upgrade to Magento 2.x before the Magento 1.x platform before it reaches its end-of-life (EoL) on June 2020. For more information about Magecart attacks including mitigation strategies, please see the NTIC Cyber Advisory titled Magecart: A Rapidly Growing Threat to Ecommerce Websites.

The Rise in Sextortion Online

Analytic Comment: Research from Michigan State University reveal that the lockdown has contributed to increase of sextortion crimes – crimes in which private images or videos are leveraged to extort money from victims. While there are various forms of sextortion with different motivation and methodologies, one of the more alarming details is that 46 percent of sextortion victims were minors. This underscores the importance for parents and legal guardians to maintain vigilance and monitor their children's online activity. For more information about these types of scams, please see our product titled Securing Our Communities: Sextortion Scams.

Patches and Updates

Adobe Releases Security Updates

Microsoft Releases Security Update for Edge

Mozilla Releases Security Update for Thunderbird

ICS-CERT Advisories

Treck TCP/IP Stack (Update E)

We welcome your feedback.

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

Receive this email from a friend or colleague and want to subscribe? Sign up here!

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-07-039

HSEC-1 | NTIC SIN No. 2.5, 5.4

July 30, 2020

National Capital Region Cyber Threat Spotlight

APT28/Fancy Bear Targets Multiple US Organizations

Between December 2018 and May 2020, Russia's state-sponsored hacking group APT28, also known as Fancy Bear, targeted multiple US organizations including state and federal government agencies, educational institutions, and the energy sector, according to a recent report from Wired. The group attempted to compromise victims' email servers, VPN servers, and Microsoft Office 365 accounts using spear-phishing campaigns, password-spraying attacks, and brute-force attacks. Once targeted mail servers had been successfully compromised, the hacking group would steal the contents of entire mailboxes. ***The NTIC Cyber Center recommends organizations maintain awareness of this and other advanced persistent threats (APTs) and employ a defense-in-depth approach to protecting data, systems, and networks. Continuously educating employees about social engineering methods such as spear-phishing, enforcing strong password policies, and enabling multifactor authentication (MFA) on all user accounts can help reduce the risk of account compromise. Having a comprehensive cyber incident response plan in place can help organizations quickly recover from a cyber attack. For more information, please download the NTIC Cyber Center's Guide for Cyber Incident Response Planning.***

Federal Partner Announcements

CISA Announces Third Annual National Cybersecurity Summit

CISA's Annual National Cybersecurity Summit will be held virtually as a series of webinars every Wednesday for four weeks beginning September 16 and ending October 7. The 3rd Annual National Cybersecurity Summit will bring together infrastructure stakeholders from around the world and provide a forum for meaningful conversations and collaboration on cybersecurity. Each series will have a different theme that focuses on CISA's mission to "Defend Today, Secure Tomorrow," with presentations from targeted leaders across government, academia, and industry.

This year's themes are:

- Sept 16: Key Cyber Insights
- Sept 23: Leading the Digital Transformation
- Sept 30: Diversity in Cybersecurity
- Oct 7: Defending our Democracy

This is a no-cost event but pre-registration is required. You can now register for the event here. For more information, visit www.cisa.gov/cybersummit2020.

CISA Releases Toolkit to Promote Public Safety Communications and Cyber Resiliency

The Cybersecurity and Infrastructure Security Agency (CISA) is charged with ensuring that the Nation's public safety and national security and emergency preparedness communities can seamlessly and securely communicate to keep America safe, secure, and resilient. Any interruption in communications can have a cascading effect, impacting the public safety agency's ability to deliver critical lifesaving services to the community. Therefore, public safety agencies should carefully plan, implement, and review communications capabilities for resiliency to maintain daily communications abilities and prepare in advance for emergency events.

Resiliency is the result of three key elements: route diversity, which promotes communications routing between two points over more than one physical path with no common points; redundancy, which ensures additional or duplicate communications assets share the load or provide back-up to the primary asset; and protective/restorative measures, which decrease the likelihood that a threat

will affect the network and enable rapid restoration if services are lost or congested. Public safety agencies should include each of these key elements in their communications resiliency plans.

In addition, assessments of public safety communications enable agencies to determine current capabilities, identify potential threats and vulnerabilities, and potential areas of improvement. These assessments ensure:

- Continuity of service in the event of an emergency
- Increased organizational control
- Prioritization of areas for network improvement
- Justification for network improvement funding requests
- Fulfillment of organizational diversity assessment requirements

To assist public safety agencies in navigating the wealth of information available regarding communications resiliency, CISA created the *Public Safety Communications and Cyber Resiliency Toolkit* to provide guidance and resources supporting the ability of communications networks to withstand damage and minimize the likelihood of a service outage. Through the use of an interactive graphic displaying components of the emergency communications ecosystem, Toolkit users can easily navigate through a number of topics and access applicable resources. The Toolkit is intended to identify and address emergent trends and issues, consolidate resources, educate stakeholders at all levels of government, and propose mitigations to enable resilient public safety communications.

For more information and additional guidance regarding communications resiliency, visit https://www.cisa.gov/safecom/technology.

Current and Emerging Cyber Threats

Fraudulent Photo-Editing Android Apps Deliver Unwanted Ads

Researchers from cybersecurity firm White Ops uncovered an ad-fraud scheme dubbed Chartreuse Blur consisting of 29 fraudulent photo-editing apps for Android that display out-of-context (OOC) ads and randomly open web browsers on compromised devices. OOC ads are displayed on the home screen when the compromised device is unlocked, plugged into a charger, or switches cellular networks. Upon installation, the app's icon disappears to make deletion difficult. These apps have been downloaded 3.5 million times from the Google Play Store. ***The NTIC Cyber Center recommends Android users thoroughly research apps before downloading them and only install trusted and vetted apps. 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.

Fake SharePoint Notifications Used to Steal Microsoft Office 365 Credentials

Researchers at the email security company Abnormal Security discovered a phishing campaign that uses fraudulent SharePoint alerts as a lure in a targeted cyber attack against corporate Microsoft Office 365 users to steal their credentials. The emails used in this campaign impersonate automated SharePoint notifications to trick users into clicking a malicious embedded link. Once clicked, victims are directed to a phishing page where they are prompted to input their Microsoft account credentials. The credentials are then sent to the threat actor's server to be sold or reused to further compromise a network. ***The NTIC Cyber Center recommends Microsoft Office 365 users remain vigilant for email phishing campaigns disguised as SharePoint notifications, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. If you believe you have been targeted by this campaign, notify your organization's IT security team immediately.***

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.

Garmin Targeted in WastedLocker Attack

Wearable device manufacturer Garmin reported experiencing an ongoing worldwide outage of some their online services due to a WastedLocker ransomware attack. Affected services include Garmin.com and Garmin Connect, as well as the company's call centers, preventing Garmin's employees from receiving calls and emails, and conducting online chats with customers. According to a photo shared with BleepingComputer, the file extension *.garminwasted* was appended to each encrypted file along with a ransom note named GARMINWASTED_INFO. It appears that the cyber threat group behind the WastedLocker attacks conducts targeted attacks as the ransomware is customized for each victim.

Lockscreen Ransomware Campaign

Researchers at Trustwave discovered a malicious email campaign that distributes a screen-locker ransomware variant via a malicious email campaign. This ransomware variant locks victims' screens rather than encrypting their data and then demands a ransom. Recipients are baited with emails containing a malicious embedded link that masquerade as an important Windows security update. Once clicked, the victim is redirected to a WordPress website masquerading as a Windows Support page. This page contains malware that causes the screen to display a fake Windows security warning suggesting victims need to renew their Windows license. The page then demands a payment in the form of Google Play Store cards, providing a form for victims to enter their name, email address, and Google Play card code. Fortunately, victims can remove the screen-locking malware and restore their systems by following the instructions provided in Trustwave's report.

Vulnerabilities

Security Flaw Discovered in DJI Drone Android Application

An Android application developed for the Chinese drone company Da Jiang Innovations (DJI) has a security flaw that would give threat actors the ability to use an auto-update mechanism that can bypass the Google Play Store and potentially install malicious applications to transmit sensitive personal information to DJI's servers. The application requests a wide range of permissions designed to obtain the user's personal data while it uses an anti-debug and encryption technique to counter security protocols. The application has over one million Android downloads via the Google Play Store. This flaw does not affect the iOS version of the app as it does not contain the same hidden update feature. This vulnerability was discovered during a security audit by an unnamed defense and public safety technology vendor who decided to investigate the DJI drone's privacy protocols. The application can seamlessly run in the background even after it is closed and it employs a Weibo SDK to install arbitrarily downloaded applications and trigger the feature that users use to live stream their drone video feed from Weibo. No evidence has been found to suggest that this vulnerability has been exploited to target any individuals with malicious intent. ***The NTIC Cyber Center recommends individuals and organizations refrain from using commercial drones manufactured in China and avoid installing any associated software to reduce the potential for data theft and cyber espionage efforts conducted by Chinese nation-state actors.***

Severe Dell PowerEdge Server Firmware Vulnerability

Researchers have released details about a newly patched high-severity path traversal vulnerability within the Dell PowerEdge servers' iDRAC technology that would give threat actors the ability to conduct remote attacks to take control of a targeted server. This path traversal vulnerability (CVE-

2020-5366) was discovered embedded within Dell EMC iDRAC9 versions prior to 4.20.20.20 and is rated a 7.1 on the severity scale. Dell has since released an update fixing the iDRAC firmware in early July. Threat actors can exploit this vulnerability if the iDRAC is connected to the internet, which Dell EMC does not recommend. ***The NTIC Cyber Center recommends network administrators who use Dell PowerEdge servers' iDRAC technology update to the latest firmware version immediately, configure the IP address range filtering and system lockdown mode options, and remove iDRAC from the internet as recommended by Dell EMC. For more information, please see Dell's support page here.***

Data Leaks and Breaches

A free lodging site known as CouchSurfing is investigating a data breach in which 17 million stolen user records were posted for sale on Telegram channels and hacker forums. Information compromised in the breach includes real names, user IDs, email addresses, and CouchSurfing account settings. The threat actor reportedly compromised CouchSurfing earlier this month in an unknown manner. Additionally, it is unknown whether or not passwords were affected in this breach. ***The NTIC Cyber Center recommends that Couchsurfing users change their credentials, monitor their accounts for any unauthorized or suspicious activity, and enable multifactor authentication on any account that offers it.***

A security breach affected online DNA matching service provider GEDmatch resulting in the exposure of DNA profiles of more than one million users whose profiles were, at the time, made available to law enforcement agencies. GEDmatch attributes the security breach to a sophisticated attack on one of their servers where the threat actor used an existing account to reset user permissions, making profiles visible to all users. This disruption lasted approximately three hours, leaving users who did not opt-in for law enforcement matching exposed. GEDmatch was breached twice in two days and claimed that no user data was downloaded or compromised. However,

Buzzfeed reports that users of genealogy and DNA testing company MyHeritage Ltd. were targeted in a phishing attack in which threat actors used email addresses obtained in the GEDmatch breach.. ***The NTIC Cyber Center recommends GEDmatch users immediately change the passwords to their accounts and any other accounts that use the same credentials, change all privacy settings back to the desired settings, and remain vigilant for any phishing campaigns that may result from this data exposure.***

BuzzFeed reported that the account information for hundreds of thousands of Instacart users is being sold on the dark web for approximately $2.00 per person. The information that is reportedly being sold contains users' names, email addresses, the last four digits of their credit card numbers, and the order histories of 278,531 Instacart accounts. Instacart denies any claim of a data breach stating "We are not aware of any data breach at this time. We take data protection and privacy very seriously." BuzzFeed researchers reached out to two supposed Instacart victims and confirmed their order date, transaction amount, and associated credit card numbers which matched the data contained in the breach. ***The NTIC Cyber Center recommends that all Instacart users immediately update their account passwords, refrain from reusing passwords across multiple accounts, and enable multifactor authentication where available, especially those associated with Instacart to prevent unauthorized access.***

Upcoming Webinars

Data Breach® Prevention. Response. Notification. TODAY

Three Things to Consider When Building a Secure Identity-Based Perimeter

The concept of "identity is the perimeter" is not new. However, COVID-19 has accelerated the transformation of workforce identity management, forcing organizations to navigate a new reality sooner than expected.

Whether or not they were prepared for it, more organizations are working remotely and utilizing SaaS tools. They are finding that the cloud is their new data center, any device can be considered a work device, and the internet is their new network. The physical workplace has disintegrated and led to a new perimeter: identity.

In this webinar, we will discuss three things to consider when securing this perimeter:

- Eliminate insecure passwords to substantially reduce the attack surface
- Implement continuous risk-based auth to adjust to new risk-based signals on the fly
- Procure a detailed view into who is coming and going in the new perimeter to simplify compliance and improve threat hunting capabilities

To register for this free webinar on Wednesday, August 12 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.

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. Although legitimate companies sometimes do conduct interviews using telecommunications software to save time and money or to interview candidates who are unable to meet in person, scammers appropriate this method to take advantage of ambitious jobseekers. They target victims using email, social media, professional networking websites, voice messaging services, and video chat platforms. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Federal Agencies Warn Foreign Hackers Are Targeting Critical Infrastructure

Analytic Comment: Foreign threat actors are attempting to target US critical infrastructure according to the National Security Agency (NSA) and the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Specifically, internet-enabled operational technology (OT) used in critical infrastructure are key components that, if compromised, can hinder services that provide water and gas to consumers. On OT systems, both the NSA and CISA have seen evidence of spear phishing and ransomware attempts. The nation-wide increase in remote work expands the attack surface that threat actors can exploit to conduct OT compromise.

US Claims Two Chinese Hackers Targeted Defense Companies, Dissidents, and Coronavirus Research

Analytic Comment: Two people were charged with stealing trade secrets and other valuable data from several companies including firms working on COVID-19 treatments, allegedly on behalf of China's Ministry of State Security. Charged by the US Justice Department, Li Xiaoyu and Dong Jiazh remain wanted by the FBI, facing indictments from 25 unnamed companies worldwide. The US Justice Department also observed the pair infiltrating software, defense, gaming, and biotech companies collecting proprietary data and attempting to extort money from companies for personal profit since 2009. Li and Dong also allegedly stole data from military satellite programs and military communications systems but will unlikely be arrested or face trial in the US.

Patches and Updates

Adobe Releases Security Updates for Magento

Cisco Releases Security Updates for ASA and FTD Software

Citrix Releases Security Updates for Workspace App for Windows

Google Releases Security Updates for Chrome

Mozilla Releases Security Updates for Multiple Products

ICS-CERT Advisories

Delta Industrial Automation DOPSoft (Update A)

HMS Industrial Networks eCatcher

Schneider Electric Triconex TriStation and Tricon Communication Module

Secomea GateManager

Softing Industrial Automation OPC

We welcome your feedback.

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

Receive this email from a friend or colleague and want to subscribe? Sign up here!

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.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-08-007

HSEC-1 | NTIC SIN No. 2.5, 5.4

August 6, 2020

National Capital Region Cyber Threat Spotlight

North Korean Phishing Campaign Targets US Defense Contractors

Between April and June 2020, McAfee researchers identified a phishing campaign dubbed "Operation North Star" masquerading as employment opportunities offered by "high-profile" defense contractors. Attributed to advanced persistent threat (APT) group Hidden Cobra, these emails contain a weaponized document that, if opened, will download an externally-hosted Word template embedded with malicious macros. This technique, called template injection, is used to bypass static document analysis employed by email security gateways to prevent end users from receiving malicious email attachments.

In this campaign, the macros download malicious dynamic-link library (DLL) files designed to establish a backdoor into the infected system and a connection with the attacker's command-and-control (C2) server. The attackers then use this backdoor to conduct cyber-espionage and steal data. ***The NTIC Cyber Center recommends network administrators review McAfee's threat analysis report Operation North Star - A Job Offer That's Too Good to Be True and block all associated indicators of compromise (IoCs). We also encourage all government employees and contractors to***

maintain awareness of this and other phishing campaigns and refrain from opening documents and clicking on links contained in unsolicited email and social media messages. If you believe you have been targeted by this or any other phishing campaign, notify your IT department immediately.

Federal Partner Announcements

Chinese Malicious Cyber Activity

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Defense (DoD) have identified a malware variant—referred as TAIDOOR—used by the Chinese government. In addition, the US Cyber Command has released the malware sample to the malware aggregation tool and repository, VirusTotal.

CISA encourages users and administrators to review Malware Analysis Report MAR-10292089-1.v1, US Cyber Command's VirusTotal page, and CISA's Chinese Malicious Cyber Activity page for more information.

FBI Reports Increase in Online Shopping Scams

The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (I3C) has released an alert on a recent increase in online shopping scams. The scams direct victims to fraudulent websites via ads on social media platforms and popular online search engines' shopping pages. Please review the FBI's IC3 Alert for indicators of fraud and tips to avoid being victimized.

Current and Emerging Cyber Threats

TrickBot Modified to Infect Linux Devices

A new TrickBot framework called Anchor has been developed for Linux and grants threat actors with backdoors that allows them secretly target Windows devices on the same network. TrickBot is a modular information-stealing Trojan and, in this variant, it comes with the ability to connect to TrickBot tools in older versions so that it may propagate on the network. The initial threat vector is currently unknown. Additionally, IoT devices that run Linux OS maybe a potential target for this version of TrickBot. ***The NTIC Cyber Center recommends network administrators review BleepingComputer's article here for an overview of the threat, indicators of compromise (IoCs), and a link to the malware sample.***

Doki Malware Targets Misconfigured Docker Cloud Instances Running on Linux

Cybersecurity researchers discovered a stealthy backdoor malware on misconfigured cloud-based docker servers running on Linux, dubbed Doki. This malware uses a unique connection to its command and control (C2) server by using a dynamic Domain Name System connecting its server in real-time. Threat actors initially search for exposed Docker instances that are publicly accessible and then start using their own cloud instances to compromise the target. Doki's stealthy abilities helped keep the malware undetected for over six months after a sample was submitted to the malware analysis engine, VirusTotal where only six antivirus engines mark this malware as malicious. ***The NTIC Cyber Center recommends administrators to close publicly accessible docket instances and scan for and proactively block the indicators of compromise (IoCs) associated with Doki*** here.

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.

Lockbit Ransomware Targets US SMBs

According to Interpol's Cybercrime Directorate, the threat actors behind LockBit ransomware are targeting American small-to-medium sized businesses (SMBs). First observed in September 2019,

LockBit is offered as a Ransomware-as-a-Service (RaaS), a service that allows a low-skilled third-party to create and manage the ransomware campaign. Once threat actors compromise a network, they use a publicly available penetration testing tool known as CrackMapExec to move laterally on the victim's network. Lockbit operators decrease their risk of detection due to how rapidly the ransomware spreads across a network. According to BleepingComputer, ransomware operators might join forces to elicit ransom payments. More information about this ransomware variant, including IoCs, is available in McAfee's report.

Vulnerabilities

GRUB2 Boot Loader

The GRUB2 boot loader is susceptible to buffer overflow attacks that allow threat actors to execute arbitrary code during the boot process. A boot loader is an application first run to boot and load the operating system. This attack is possible when local authenticated threat actors modify the GRUB2 configuration file that allows them to bypass signature verification. Since the malicious code runs before the operating system (OS), threat actors are able to modify the OS and control how it is loaded. Threat actors are able compromise systems even with Secure Boot enabled. ***The NTIC Cyber Center recommends administrators Update GRUB2 to the latest version when possible. Please see CERT Coordination Center Vulnerability Note VU#174059 for more information.***

wpDiscuz WordPress Plugin

WordPress has a maximum severity vulnerability with its wpDiscuz plugin that gives hackers the ability to take over hosting accounts on approximately 70,000 WordPress sites. The wpDiscuz plugin was designed to provide a real-time comment platform that will cache comments within a local database. The unpatched version of this plugin allows threat actors the opportunity to upload arbitrary files to the vulnerable WordPress hosting server, allowing threat actors to conduct remote code execution (RCE) and further infect the hosted account with malware. When exploited, this would completely give threat actors complete control over every site on the victims' server. ***The NTIC Cyber center recommends that WordPress wpDiscuz users update the plugin to the latest release as soon as possible and change all passwords associated with any WordPress accounts.***

Newsletter WordPress Plugin

A vulnerability identified in the WordPress plugin "Newsletter" could allow threat actors to potentially compromise websites and create rogue administrator accounts and backdoors. Threat actors can conduct these attacks when they leverage a reflected cross-site scripting (XSS) flaw and a

PHP Object Injection vulnerability. While the developer released a patch, at least 1500,000 WordPress sites may still be at risk of attack because of these vulnerabilities. ***The NTIC Cyber Center encourages administrators of WordPress websites that have the Newsletter plugin installed to immediately upgrade to the latest bug-free version, 6.8.3, and maintain regular website backups that are stored securely off the network.***

Data Leaks and Breaches

Multiple Startup Companies Disclose Data Breaches

Startup companies have started announcing their data breaches after a massive leak of stolen databases was published on a hacker forum earlier this month. BleepingComputer reported that the threat group ShinyHunters published the stolen databases of 18 websites for free, after profiting from the data in private sales. Researchers from BleepingComputer contacted several companies involved in this data breach revealing that emails, names, hashed passwords, addresses, phone numbers, and other information had been exposed and sold. ***The NTIC Cyber Center recommends that account users of any of the listed companies immediately change their associated passwords to reduce the risk of compromise.***

Havenly

A US-based interior design website known as Havenly disclosed a data breach in which 1.3 million user records were freely posted on a hacker forum. Information compromised in the breach includes full names, login names, email addresses, hashed passwords, phone numbers, zip codes, last four digits of credit cards and various usage data. Havenly has since distributed data breach notifications and performed mandatory password resets. Full credit card information was not exposed according to Havenly, and the initial threat vector is currently unknown. ***The NTIC Cyber Center recommends that Havenly users change their credentials, monitor their accounts for any unauthorized or suspicious activity, and enable multifactor authentication on any account that offers it.***

Upcoming Webinars

Cleaning Up Our Cyber Hygiene

Successful attacks almost always take advantage of conditions that could reasonably be described as poor cyber hygiene, including the failure to patch known vulnerabilities, poor configuration management, and poor management of administrative privilege. In this session, we'll dig a little deeper into the idea. We'll discuss the importance of cyber hygiene as a root cause issue for attacks and as a defensive strategy. We look at various attempts to define a specific set of practices to include, and how this might help establish a baseline for action. And suppose hygiene isn't enough, what then? Finally, we'll look at what might be done to turn cyber hygiene from a notion or a general exhortation to do better (cheer-leading) into a large-scale program of improvement.

To register for this free webinar on Friday, August 7 at 3:30 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 ***brushing scam*** is a deceitful technique that some e-commerce vendors use to boost their sales and

consumer ratings by creating fake orders and reviews. The US Department of Agriculture (USDA) recently issued a warning regarding a new and an ongoing brushing campaign in which unsolicited packages of seeds that appear to originate from China are being delivered to US citizens across the country. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Business ID Theft Soars Amid COVID Closures

Analytic Comment: Identity thieves who use businesses to establish unauthorized lines of credit have been extremely aggressive through the COVID-19 pandemic. Even with companies closing or waiting for the COVID-19 pandemic to end, threat actors involved in the organized identity theft rings still have a vast selection of targets from which to choose. Expert security researchers noticed that identity theft groups appear to target both active and inactive businesses by searching the companies' ownership records at the Secretary of State website that matches the associate state of incorporation. With that information, these threat actors are able identify the owners of the company, acquire their Social Security and tax ID numbers from the dark web or other online resources to fabricate official documents tied to the business and change the mailing address to an address that they control. After the fraudulent profiles are approved by Dun & Bradstreet, threat actors will start to apply for new lines of credit using the victim's business name.

Ransomware Feared as Possible Saboteur for November Election

Analytic Comment: Federal agencies believe targeted ransomware attacks could potentially incapacitate voting operations. Threat actors could target vote-reporting and calculation systems or place ransomware on networks that contain voter databases. An official from the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) stated that they are "seeing state and local entities targeted with ransomware on a near daily basis." Even failed ransomware attempts can disrupt elections as they can negatively impact voter confidence. This highlights the importance of implementing comprehensive and consistent IT security policies, redundancies, and cyber incident response plans to help government agencies tackle these challenges and more effectively secure the US election security posture.

Patches and Updates

Cisco Releases Security Updates for Multiple Products

ICS-CERT Advisories

Delta Industrial Automation CNCSoft ScreenEditor

Inductive Automation Ignition 8

Mitsubishi Electric Factory Automation Engineering Products

Mitsubishi Electric Factory Automation Products Path Traversal

Mitsubishi Electric Multiple Factory Automation Engineering Software Products

Philips DreamMapper

Treck TCP/IP Stack (Update F)

We welcome your feedback.

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

Receive this email from a friend or colleague and want to subscribe? Sign up here!

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

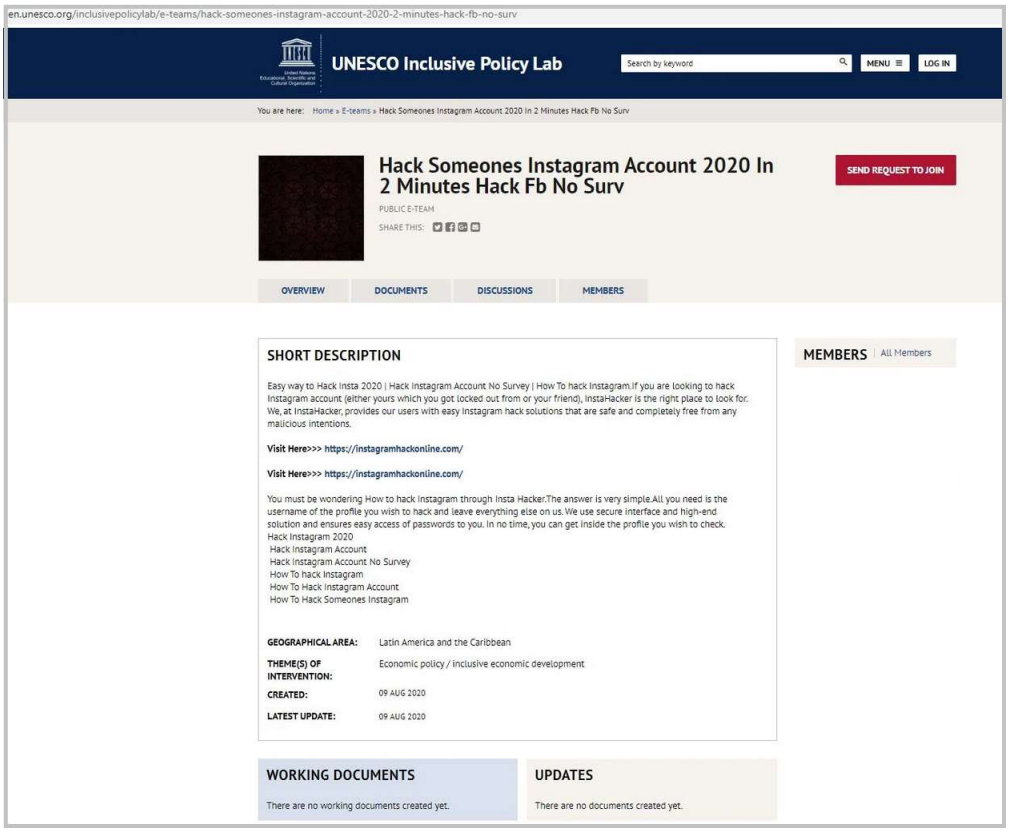
TLP:WHITE

Product No. 2020-08-019

HSEC-1 | NTIC SIN No. 2.5, 5.4

August 13, 2020

National Capital Region Cyber Threat Spotlight



Malware Distributors Target Government and University Websites

Security intelligence firm Cyble uncovered a hacking campaign in which threat actors exploit vulnerabilities in government and university websites to host articles that lead to malware infections and scams. These articles claim to provide links to hacking tools for various social media platforms and video streaming services. However, these links are malicious and ultimately infect victims with

malware, adware, or bait them into falling for online scams. Additionally, threat actors have used search engine optimization (SEO) techniques to manipulate search results and improve search rankings for these malicious webpages. ***The NTIC Cyber Center recommends website administrators regularly audit websites for unauthorized changes or access, ensure that all administrator accounts are secured with multifactor authentication, and ensure their platforms are updated with the latest versions to patch known vulnerabilities.***

Federal Partner Announcements

US Department of State Announces the Expansion of the Clean Network to Safeguard America's Assets

The Clean Network program is the Trump Administration's comprehensive approach to guarding our citizens' privacy and our companies' most sensitive information from aggressive intrusions by malign actors, such as the Chinese Communist Party (CCP). On August 5, 2020, the US Department of State issued a press statement announcing the launch of five new lines of effort to protect America's critical telecommunications and technology infrastructure.

These programs are rooted in internationally accepted digital trust standards and built upon the 5G Clean Path initiative, announced on April 29, 2020, to secure data traveling on 5G networks into US diplomatic facilities overseas and within the United States. For more information, please review the US Department of State's press statement.

Malicious Cyber Actor Spoofing SBA's COVID-19 Loan Relief Website via Phishing Emails

The Cybersecurity and Infrastructure Security Agency (CISA) is currently tracking an unknown malicious cyber actor who is spoofing the Small Business Administration (SBA) COVID-19 relief webpage via phishing emails. These emails include a malicious link to a fake page used for

malicious re-directs and credential stealing.

Small business owners and organizations at all levels should review the alert and apply the recommended mitigations to strengthen the security posture of their systems. We encourage you to share this alert with anyone who might be able to use it.

This alert can be found here and at cisa.gov/coronavirus.

Current and Emerging Cyber Threats

Fraudulent Zoom Notifications Target Microsoft Office 365 Credentials

Emails used in this campaign impersonate Zoom meeting notifications and are sent from both compromised accounts and newly registered domains to bypass various security filters. Once the links within these emails are clicked, victims are directed to a phishing page where they are asked to input their Microsoft Outlook or Office 365 credentials. This campaign features additional security evasion techniques as the HTML, JavaScript, and PHP code is typically encoded making them unreadable to individuals and other security filters. ***The NTIC Cyber Center recommends users remain vigilant for email phishing campaigns disguised as Zoom notifications, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. If you believe you have been targeted by this campaign, notify your organization's IT security team immediately.***

cPanel Users Targeted in Phishing Attack

Researchers discovered a phishing campaign masquerading as a security advisory targeting cPanel users with claims of security vulnerabilities within the web hosting management panel and a recommendation that all users install the latest updates. Threat actors behind this campaign crafted a sophisticated email that appears to have no grammar or spelling issues and uses a cpanel7831[.]com domain to appear as a legitimate advisory from cPanel. Designed to obtain users' credentials, recipient who click on the embedded link are brought to a fraudulent login page that threat actors use to steal and store the victimized cPanel users' credentials. ***The NTIC Cyber Center recommends cPanel users remain vigilant for phishing campaigns disguised as security advisories, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. If you believe you have been targeted by this campaign, change your cPanel password immediately and implement multifactor authentication, if available.***

Vulnerabilities

TeamViewer

TeamViewer, a remote access and troubleshooting application contains a vulnerability (CVE-2020-13699) that would allow remote unauthenticated threat actors to covertly connect to computers running the Windows operating system. Once connected, this could allow threat actors to execute arbitrary code or and steal password hashes. Users are compromised when they visit a website that contains a rogue iframe designed to launch the TeamViewer app on the targeted machine. This allows the threat actor's server to connect to via Server Message Block (SMB) protocol. A threat actor would be authenticated without passwords since the victim's machine is initiating the connection to the threat actor's system. TeamViewer has since released a patch. ***The NTIC Cyber Center recommends all users and administrators of vulnerable TeamViewer versions apply the available update as soon as possible. Additionally, we recommend all network administrators proactively block inbound and outbound traffic on SMB port 445 at the firewall to prevent unauthorized connections.***

Windows Print Spooler

Security researchers have found a vulnerability (CVE-2020-1337) in Windows print spooler that bypasses an old Windows patch and gives programs administrative privileges that could be used to execute malicious code. Windows print spooler uses SYSTEM privileges that gives any user the ability to modify and add SHD files into folders, a task that requires elevated privileges. While neither of the issues allows an adversary directly to compromise a host, they can serve in the second stage of an attack and lead to a full system compromise. A patch was released for this vulnerability on August 11, 2020. ***The NTIC Cyber Center recommends all users and administrators of vulnerable Microsoft Windows printing service versions apply the appropriate patch as soon as possible.***

Qualcomm Snapdragon

According to researchers at Check Point, smartphones running on a specific Qualcomm digital signal processor (DSP) chip contains several flaws that left nearly 50 percent of the world’s smartphones vulnerable to attacks. The vulnerabilities include the potential to gain access to photos, videos, call-recording, real-time microphone data, GPS and location data, and can also render a targeted smartphone unresponsive. These vulnerabilities allow malware and malicious code to remain hidden and become unremovable. Qualcomm released a patch for the six security flaws affecting the Snapdragon DSP chip, but mobile vendors still need to implement and deliver these

security patches to their users. ***The NTIC Cyber Center recommends that mobile users keep their software and operating systems up-to-date and decommission smartphones that are not in use or cannot be updated, as these vulnerabilities do not require user interaction to exploit.***

Data Leaks and Breaches

Online exam proctoring service ProctorU confirmed a data breach in which 444,000 user records were freely posted on a hacker forum. Information compromised in the breach includes full names, email addresses, hashed passwords, phone numbers, affiliation information and other data. Havenly has since distributed data breach notifications and performed mandatory password resets. Financial information was not exposed, according to ProctorU, and the initial attack vector is currently unknown. ***The NTIC Cyber Center recommends that ProctorU users change their credentials, monitor their accounts for any unauthorized or suspicious activity, and enable multifactor authentication on any account that offers it.***

The SANS cybersecurity training organization acknowledged suffering a data breach after a SANS employee fell victim to a phishing attack that allowed an unidentified threat actor to gain access to an email account. According to the announcement, SANS "identified a single phishing email as the vector of the attack." The threat actor set a forwarding rule and installed a malicious Microsoft Office 365 add-in on the compromised account, which forwarded 513 emails from the victim's account to an unauthorized external email account. This resulted in the breach of approximately 28,000 records containing personally identifiable information (PII). Affected data includes names, email addresses, work titles, company names, and addresses. Passwords and financial information were not affected by the breach. ***The NTIC Cyber Center recommends that SANS customers proactively change the password to their SANS account, along with any account that shared the same credentials to prevent any additional targeting. We also recommend remaining vigilant for phishing and vishing campaigns resulting from this data exposure.***

Upcoming Webinars

Data Breach Today
Prevention. Response. Notification.

Online Privacy, Security, and a Seamless Patient Experience

Your patients and members are today's consumers, and they expect seamless user experiences. But you can't meet their demands at the expense of security. You must remain a stalwart steward of protected health information (PHI) and personally identifiable information (PII). The distributed nature of healthcare delivery and R&D make this an especially difficult balancing act.

Join our webinar on August 19th to learn how Simeio Solutions, on the Ping Identity Platform, offered patients the privacy and security they needed in a real life healthcare portal.

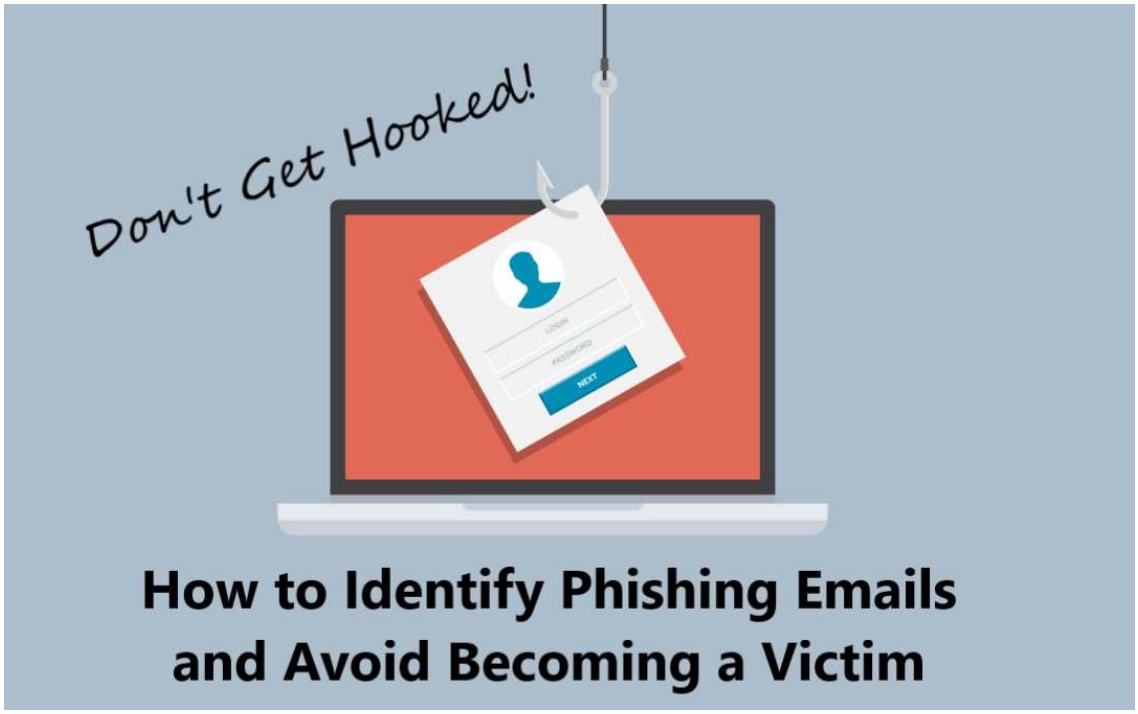
You will hear Baber Amin, West CTO at Ping Identity and Balraj Dhillon, Engagement Director at Simeio Solutions discuss:

- Common identity challenges to improving online patient experiences
- The need for privacy in online health portals and mobile applications
- Security requirements to protect PHI and PII

To register for this free webinar on Wednesday, August 19 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.



Phishing is a type of social engineering scheme in which an attacker tries to trick victims into revealing sensitive information such as their account login credentials (usernames and passwords), their banking or credit card information, or personally identifiable information (PII) such as dates of birth and Social Security numbers. The attackers then use this information to gain unauthorized access to email, social media, and financial accounts, steal victims' money and data, conduct financial fraud, or commit identity theft. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

The Cybersecurity Risks of Improper Employee Offboarding

Analytic Comment: With the Covid-19 pandemic forcing millions of layoffs in nearly every sector, cybersecurity researchers focus on six risks attached to offboarding employees improperly. Data loss, compliance violations, breaches of confidentiality, data breaches, ruined reputations, and wasted spend can result when employees are not thoroughly removed from all services or all confidential data is not destroyed or returned to the company before the employee leaves. Companies who are facing layoffs should always conduct proper exit interviews, stop email forwarding and file sharing, remove access to all applications and services, change any shared passwords and reassign suspended licenses to another employee to eliminate wasted spend.

Patches and Updates

Adobe Releases Security Updates

Apple Releases Security Updates for iCloud for Windows

Cisco Releases Security Updates for Multiple Products

Google Releases Security Updates for Chrome

Microsoft Releases August 2020 Security Updates

SAP Releases August 2020 Security Updates

ICS-CERT Advisories

Schneider Electric APC Easy UPS On-Line

Siemens Automation License Manager

Siemens Desigo CC

Siemens Opcenter Execution Core (Update A)

Siemens SCALANCE, RUGGEDCOM

Siemens SICAM A8000 RTUs

Siemens SIMATIC, SIMOTICS

Siemens UMC Stack (Update A)

Tridium Niagara

Yokogawa CENTUM

We welcome your feedback.

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

Receive this email from a friend or colleague and want to subscribe? Sign up here!

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-08-027

HSEC-1 | NTIC SIN No. 2.5, 5.4

August 20, 2020

National Capital Region Cyber Threat Spotlight

Emotet Targets US Businesses Using COVID-19 Themed Phishing Campaigns

Emotet malware threat actors have been exploiting the uncertainty surrounding the COVID-19 pandemic by targeting US businesses with COVID-19 themed phishing campaigns. Security researchers at Fate112 recovered a stolen email that had been being used in a phishing attack in which threat actors were pretending to be from the 'California Fire Mechanics' and were sending pandemic-related updates. Within the email is a malicious attachment titled 'EG-8777 Medical report COVID-19[.]doc' that claims to be created from an iOS device and requires the unsuspected victim to enable macros to view it properly. Once the malicious macros are enabled, Emotet will begin to download and install other malware such as Qbot or TrickBot, turning the victim's computer into a malware bot designed to send malicious email to other unsuspecting recipients. ***The NTIC Cyber Center recommends users remain vigilant for this and other 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.***

Federal Partner Announcements

Phishing Emails Used to Deploy KONNI Malware

The Cybersecurity and Infrastructure Security Agency (CISA) has observed cyber actors using emails containing a Microsoft Word document with a malicious Visual Basic Application (VBA) macro code to deploy KONNI malware. KONNI is a remote administration tool (RAT) used by malicious cyber actors to steal files, capture keystrokes, take screenshots, and execute arbitrary code on infected hosts.

For more information, including screenshots, downloadable indicators of compromise (IoCs), and mitigation recommendations please see CISA Alert AA20-227A.

North Korean Malicious Cyber Activity

CISA and the Federal Bureau of Investigation (FBI) have identified a malware variant—referred to as BLINDINGCAN—used by North Korean actors.

CISA encourages users and administrators to review Malware Analysis Report MAR-10295134-1.v1 and CISA's North Korean Malicious Cyber Activity page for more information.

Current and Emerging Cyber Threats

New Crypto-Mining Worm Steals AWS Credentials

Researchers at Cado Security uncovered a crypto-mining worm that steals Amazon Web Services (AWS) credentials, local credentials, and scans the internet for misconfigured Docker platforms. Believed to be the first worm to feature AWS functionality, the threat actors behind this are known as "TeamTNT" and specialize in targeting Docker and Kubernetes systems. While the initial infection vector is unspecified, some research suggest that it is attributed to improperly secured AWS settings. ***The NTIC Cyber Center recommends all cloud and container administrators properly configure and secure their accounts to reduce the risk of unauthorized access. We recommend network administrators proactively block the associated IoCs provided in Cado***

Security's report.

Drovorub Malware Targets Linux

A joint security alert from the FBI and NSA highlights a new strain of Linux malware, dubbed Drovorub, that can take control of targeted devices and is used steal files in cyber-espionage operations. The alert attributed the malware to the Russian advanced persistent threat group APT28, also known as Fancy Bear. Drovorub is viewed as a "swiss-army knife" in that it features a multi-component system that performs numerous malicious activities. It is recommended that organizations update any Linux system to a version running kernel version 3.7 or later to prevent Drovorub infections. While there are currently relatively few Linux threats, this will likely change in time as Linux is increasingly used in enterprise and cloud environments. ***The NTIC Cyber Center recommends all Linux administrators to update systems to the latest version as soon as possible.***

PurpleWave Data-Stealing Malware Discovered

Researchers have discovered PurpleWave, a new infostealer malware written in C++ to remain stealthy while it installs on a victim's device and can obtain confidential data and credentials. PurpleWave has the potential to steal passwords, cookies, payment card data, browser history, screen captures, system information, Telegram session files, Steam application data, cryptocurrency wallet data, and is capable of loading and executing additional malware. The creator of PurpleWave stealer advertises its malware on active Russian cybercrime forums so researchers at Zscaler consider PurpleWave as an ongoing threat, as the command and control (C2) servers associated with this campaign are still operational. ***The NTIC Cyber Center recommends network administrators reference and proactively block the associated indicators of compromise (IoCs) contained in the Zscaler report.***

Vulnerabilities

Thales Cinterion EHS8 M2M Modules

IBM researchers discovered a vulnerability (CVE-2020-15858) within the Thales Cinterion EHS8 product line that, if exploited, could allow remote threat actors to control devices or gain unauthorized access to the associated network. The affected product line is designed to secure machine-to-machine (M2M) communications over 3G and 4G networks and is used by over 30,000 companies, including those in the automotive, energy, telecom, and medical sectors. The vendor, Thales, confirmed that this vulnerability exists within several modules of the EHS8 product line, including BGS5, EHS5/6/8, PDS5/6/8, ELS61, ELS81, and the PLS62. ***The NTIC Cyber Center***

recommends all administrators of affected Thales Cinterion EHS8 modules review IBM's report and apply the available patch as soon as possible.

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.

Carnival Corporation Suffers Ransomware Attack

Cruise line company Carnival Corporation was compromised by a ransomware attack on August 15, 2020 that encrypted a portion of one of their brand's information technology systems, exposing the personal data of their guests and employees. It is currently unclear how many guests or employees are affected by this attack, but Carnival's preliminary assessment revealed that this incident will not materially affect its business operations or finances. Carnival has hired the industry's top security firms to recover from this attack and has since notified law enforcement of the incident.

Data Leaks and Breaches

350 Million Email Addresses Exposed on Unsecured AWS Server

The CyberNews research team discovered a breach that exposed seven gigabytes of unencrypted files that included 350 million email addresses. The breach is attributed to an unsecured publicly accessible Amazon Web Services (AWS) server owned by an unidentified party. The data was hosted in the United States for approximately 18 months and has since been removed as of June 10, 2020. ***The NTIC Cyber Center recommends email users remain vigilant for phishing attempts and encourages the use of lengthy, complex, and unique passwords for each account. We also urge users to enable multifactor authentication on any account that offers it to avoid falling victim to credential compromise.***

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

State-Backed Hacking, Cyber Deterrence, and the Need for International Norms
Analytic Comment: State-backed cyber threat actors are more frequently stealing money, sensitive personal and financial information, intellectual property, government secrets, and probing critical infrastructure. Globally accepted rules of engagement relating to cyber attacks have yet to be established during peacetime and attribution can be difficult. However, cyber threat intelligence sharing efforts between the public and private sectors have helped to improve attribution efforts and allowed the United States to work with allies to counter cyber threats associated with nation-state actors.

Patches and Updates

Google Releases Security Updates for Chrome

ICS-CERT Advisories

Schneider Electric APC Easy UPS On-Line

Siemens Automation License Manager

Siemens Desigo CC

Siemens Opcenter Execution Core (Update A)

Siemens SCALANCE, RUGGEDCOM

Siemens SICAM A8000 RTUs

Siemens SIMATIC, SIMOTICS

Siemens UMC Stack (Update A)

Tridium Niagara

Yokogawa CENTUM

We welcome your feedback.

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

Receive this email from a friend or colleague and want to subscribe? Sign up here!

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

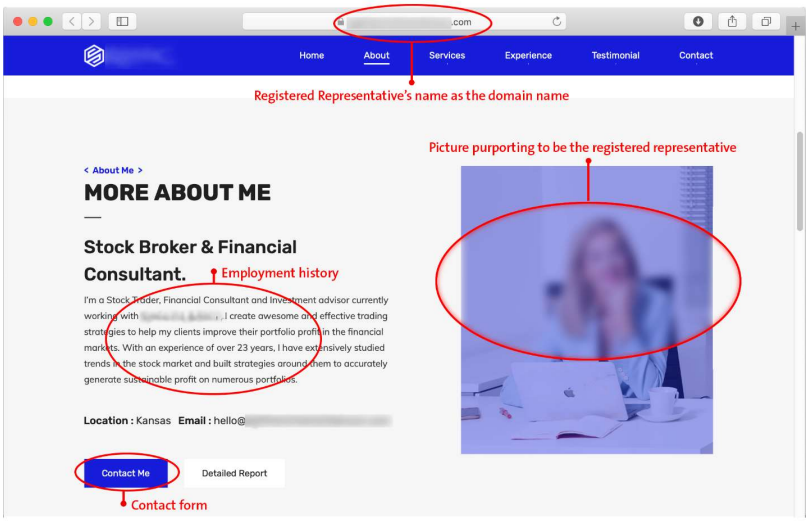
TLP:WHITE

Product No. 2020-08-037

HSEC-1 | NTIC SIN No. 2.5, 5.4

August 27, 2020

National Capital Region Cyber Threat Spotlight



(Image source: FINRA)

FINRA Warns of Phishing Websites Impersonating Registered Representatives

The US Financial Industry Regulatory Authority (FINRA) released a warning to its members that threat actors are using registered brokers' information to create possible phishing websites. These fraudulent websites will likely be used as phishing landing pages designed to steal the personal information of potential customers to commit financial fraud. The phishing websites in this campaign display legitimate broker information, including names, employment histories, and pictures, and provide a contact form for victims to enter their phone numbers and email addresses. Security researchers believe that the threat actors behind this campaign may attempt to use these associated domains in future email-based phishing campaigns. ***The NTIC Cyber Center***