software is updated to the latest version. This highlights the importance of using lengthy, complex, and unique passwords for each account.

Pastebin Just Made It Easier for Hackers to Avoid Detection, Researchers Say

Analytic Comment: A policy change at text repository and sharing site Pastebin resulted in the disabling of its API that allowed users to scrape the site for information. Pastebin also removed its search bar, effectively eliminating the ability to search its platform for specific words, code, or terms. While the site is primarily used to share legitimate, non-malicious code, threat actors have increasingly abused the site to publish stolen data, conduct doxing campaigns, and host malicious code. Pastebin claims that it changed its policy to prevent third-parties from charging customers money to search their site.

Czech Cyber Officials Warn of Serious Threat to Health Care Sector

Analytic Comment: Cybersecurity authorities in the Czech Republic have issued a warning to the public about possible cyber attacks targeting health care facilities and IT systems coming in the next few days. They believe recent spear phishing campaigns are a "preparatory" phase of larger attacks to come. Last month, the Czech Republic's second largest hospital was hit with a cyber attack amidst COVID-19 testing. The US State Department's cyber diplomacy office highlighted the Czech Republic's advisory. This underscores the importance of having a cyber incident response plan in place prior to a cyber attack.

Patches and Updates

Apple Releases Security Update for Xcode

Cisco Releases Security Updates for Multiple Products

Google Releases Security Updates

Google Releases Security Updates for Chrome

Microsoft Releases Security Updates for Multiple Products

OpenSSL Releases Security Update

ICS-CERT Advisories

Inductive Automation Ignition

We welcome your feedback.

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

TLP:WHITE

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

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on *Subscribe to Receive Our Products* at the top of the page, and enter your information.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

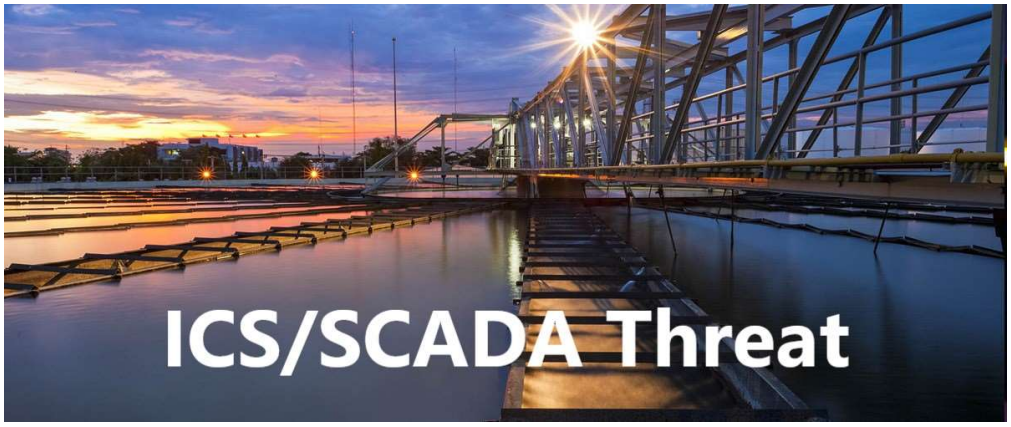
TLP:WHITE

Product No. 2020-04-039

HSEC-1 | NTIC SIN No. 2.5, 5.4

April 30, 2020

National Capital Region Cyber Threat Spotlight



Water Sector Facilities Targeted in Cyber Attacks

Israel's National Cyber Directorate recently issued an alert to water sector organizations following cyber attacks that were conducted against supervisory control and data acquisition (SCADA) systems at wastewater treatment plants, pumping stations, and sewage facilities. Although this specific threat may not have directly impacted the United States, protecting our nation's critical infrastructure sectors from such threats is imperative to protecting the Homeland, especially during this unprecedented time. As stay-at-home orders have been enacted all across the country, our citizens rely upon our critical infrastructure to maintain access to clean, running water, electricity and gas, and internet services. As we have witnessed all too often, cyber threats have no boundaries and those that impact one country can easily impact many more in the blink of an eye.

The NTIC Cyber Center recommends all organizations within critical infrastructure sectors adopt a proactive and robust approach to protecting their systems from this and other cyber threats and employ a comprehensive cyber incident response plan to swiftly handle successful attacks and

minimize disruption to their services and operations. We encourage all administrators of ICS/SCADA systems within the water sector and other critical infrastructure sectors to change passwords of internet-accessible control systems, using credentials that are lengthy, complex, and unique to each system. Additionally, implement, enable, and enforce the use of multi-factor authentication solutions and Virtual Private Networks (VPNs), and employ IP address whitelisting for internet-connected critical systems and components. Regularly scan and audit networks for unauthorized or unintended internet exposure and ensure that all software is patched and up-to-date with the latest versions. For a free, downloadable guide on cyber incident response planning and other resources, please visit our website here.

Federal Partner Announcement

FCC Takes Action to Protect American Consumers from One-Ring Scams

On April 28, 2020, the Federal Communications Commission issued a Notice of Proposed Rulemaking aimed at better protecting Americans from one-ring scam calls. One-ring scam calls occur when a call placed to a consumer's phone rings just once, using international toll-generating numbers that charge large fees per minute when consumers call back. The FCC's proposal is the latest step to address this problem; it follows a consumer alert the agency issued in May 2019 and implements one section of the recently passed Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act). For more information on these types of nuisance calls, please see the NTIC Cyber Center blog post titled Securing Our Communities: One Ring Scam Calls.

CISA Releases Microsoft Office 365 Security Recommendations

Since October 2018, the Cybersecurity and Infrastructure Security Agency (CISA) has conducted several engagements with customers who have migrated to cloud-based collaboration solutions like Microsoft Office 365 (O65). In recent weeks, organizations have been forced to change their collaboration methods to support a full “work from home” workforce.

O365 provides cloud-based email capabilities, as well as chat and video capabilities using Microsoft Teams. While the abrupt shift to work-from-home may necessitate rapid deployment of cloud collaboration services, such as O365, hasty deployment can lead to oversights in security configurations and undermine a sound O365-specific security strategy.

CISA continues to see instances where entities are not implementing best security practices in regard to their O365 implementation, resulting in increased vulnerability to adversary attacks. To review CISA's Microsoft Office 365 security recommendations, please see Alert AA20-120A.

Current and Emerging Cyber Threats

Asnarök Trojan Targets Physical and Virtual Firewalls

SophosLabs and Sophos internal security teams have been investigating a previously unknown SQL injection vulnerability that was exploited in a coordinated attack on some Sophos firewall products, leaving Sophos and its customers vulnerable to remote code execution. Threat actors discovered a zero-day SQL vulnerability and injected a command code that downloaded a Linux shell script from a remote server. In turn, this triggered a series of SQL commands that dropped additional files on the device to advance the attack. Once this vulnerability is exploited, the threat actor will use the scripts to collect the public IP address of the device, retrieve the firewall license key, query the SQL for user account information, steal the admin password hash from the RAM, query for VPN users and policies, compress the collected data using the tar compression tool, encrypt the tar file using OpenSSL, delete all evidence files, and exfiltrate the data. ***The NTIC Cyber Center recommends network administrators block the associated Sophos indicators of compromise (IoCs) listed in their report and make sure all devices are up-to-date with the latest patches. Users and administrators of affected products are encouraged to enable the automatic installation of hotfixes. Instructions on how to do so are available here.***

Revive Ad Server Exploited to Serve Malware

Revive ad server, an open-source online advertising platform, was compromised and exploited to deliver malware to unsuspecting victims. When websites use third-party and dynamic advertising services to support their websites using ad revenue, they lack complete control of which ads are

displayed on their sites and can become vulnerable to these types of attacks. Visitors to their websites who do not use ad-blocking software can then become infected by ads containing malicious code. In this particular case, visitors of sites using Revive to deliver ads were redirected to malicious sites promoting fraudulent Adobe Flash updates. These updates contained an adware bundle that has a history of delivering ransomware, data-stealing Trojans, unauthorized browser extensions, and other malware. ***The NTIC Cyber Center recommends using reputable ad-blocking software or browser extensions, only downloading applications or enabling pop-ups from trusted and vetted sources, and running reputable and up-to-date antivirus software.***

Phishing Campaign Uses Fake Customer Complaints to Target Victims

A new phishing campaign uses fraudulent customer complaints to trick corporate employees into downloading backdoors onto their employer's systems and network. Threat actors masquerading as corporate lawyers send emails to recipients regarding a supposed customer complaint and threatens to debit their financial accounts for the amount of the fine. Included in the body of the email is a Google Docs link that redirects those who click on it to a website hosting a malicious PDF document. If opened, this document downloads a Trojan, dubbed Bazaloader, that creates a backdoor into the victim's system, allowing for further network compromise. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns disguised as customer complaint 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 believe you have been infected by Bazaloader, contact your organization's IT department immediately.***

Phishing Campaign Spoofs Skype to Steal Account Credentials

Cybersecurity firm Cofense recently detected a phishing campaign that spoofs the video calling platform Skype to trick users into clicking a malicious link and divulging their login credentials to the attackers. This attack uses a sophisticated email that closely resembles a legitimate Skype notification. However, the emails contain a malicious link that, if clicked, delivers victims to a phishing page that attempts to collect their email login credentials. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns disguised as Skype 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 fallen victim to this or any other credential-stealing scheme, notify your organization's IT team and quickly change your login credentials to any affected 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.

Microsoft Provides Ransomware Prevention Guidance

Microsoft just released guidance for healthcare and critical service providers on how to reduce the risk of a ransomware infection. The risks outlined in the guidance include not applying software patches and updates in a timely manner, using outdated and unsupported platforms and hardware, misconfigurations in servers and software, and allowing remote desktop connections without mutifactor authentication, among others. Network administrators should also be aware that cyber threat actors may maintain unauthorized access to systems and network for long periods of time before executing ransomware or other malware infections.

Shade Ransomware Operators Release All Decryption Keys for Victims

The threat actors behind Shade Ransomware, also known as Troldesh or Encoder.858,. have ceased operations, released the decryption keys and instructions on how to use them, and apologized for their actions. The threat actors claimed to have stopped distributing the ransomware at the end of 2019 and created a GitHub repository that include over 750,000 decryption keys, instructions on how to use them, and a link to their decryption program. While the decryption keys have been confirmed to be valid, researchers report that they are not very user-friendly; however, cybersecurity firms are currently working to incorporate these keys into publicly-available decryption tools. The link to the associated GitHub repository is included in BleepingComputer's article here.

Sodinokibi Ransomware Targets SeaChange Video Platform

SeaChange, a video delivery software solutions firm, has allegedly fallen victim to a Sodinkobi ransomware attack in which the threat actors behind the campaign have begun slowly publishing images of files and documents stolen during the attack. Data stolen reportedly includes bank statements, insurance certificates, driver's licenses, and a cover letter for a proposal for a Pentagon video-on-demand service. Sodinokibi operaters, the US Department of Defense, and SeaChange have yet to provide any additional information regarding the ongoing ransomware attack. This

incident highlights the increasing efforts of ransomware campaigns to coerce victims into paying the ransom.

Sodinokibi Ransomware Targets CivicSmart Smart Parking Meter Firm

CivicSmart, a company that sells "smart" parking meters as well as technology used by various parking enforcement authorities, was targeted in a Sodinokibi ransomware attack in March. The attackers threatened to publicly release as much as 159 GB of stolen data from the company that included employee records, vendor contracts, bank statements, and credit card numbers if CivicSmart did not pay the ransom. Researchers suggest the ransom may have been paid, based upon the removal of the stolen data from the attacker's website, but paying the ransom does not guarantee that the attacker will not use, sell, or release the data in the future.

Vulnerabilities

iOS Vulnerability Allows Access to Apple Mail Application

Researchers at ZenOps recently discovered an iOS Apple Mail application vulnerability that, if abused, could be used to gain access a victim's email account, allowing threat actors to leak, alter, or delete emails. Threat actors can do this when they send emails past a specific threshold to alter a device's memory. Victim compromise can occur in various ways, depending on the iOS version. In iOS 12, users have to click on an email for the compromise to occur but, in iOS 13, no user action is required. It is believed that that threat actors have already leveraged this vulnerability against iOS users within several Fortune 500 companies and other high-profile individuals. Apple has issued a patch in the beta version of iOS 13.4.5. ***The NTIC Cyber Center recommends iOS users to patch to the latest version whenever possible.***

WordPress Plugin "Real-Time Find and Replace"

A vulnerability identified in the WordPress plugin "Real-Time Find and Replace" could allow threat actors to inject malicious code into their sites and create rogue administrator accounts. Threat actors use cross-site request forgery (CSRF) to facilitate a stored cross-site scripting (Stored XSS) attack on older plugin versions. While the developer released a patch quickly, over 70,000 WordPress sites may still be at risk of attack as a result of this vulnerability. ***The NTIC Cyber Center encourages administrators of WordPress websites that have the Real-Time Find and Replace plugin installed to immediately upgrade to the latest bug-free version, 4.0.2, and maintain regular website backups that are stored securely off the network.***

IBM Data Risk Manager Zero-Day Vulnerabilities Discovered

A security researcher published four zero-day vulnerabilities discovered within the IBM Data Risk Manager, an enterprise security appliance, after attempting to disclose them to the company. IBM reportedly refused to accept the researcher's vulnerability report and classified it as "out of scope" for their vulnerability disclosure program. The report included authentication bypass, command injection, insecure default password, and arbitrary file download vulnerabilities. After the public disclosure, IBM responded by publishing a security advisory that addresses three of the four vulnerabilities. ***The NTIC Cyber Center encourages administrators of affected IBM security appliances review IBM's support document, upgrade to the latest version, and reset the default userID and password as soon as possible.***

Data Leaks and Breaches

A researcher discovered a breach of data associated with 2.5 million credit card transactions belonging to mobile payment solutions provider, PAAY. While the database did not include cardholder name or card verification values, it did expose credit card numbers, expiration dates, and amounts spent from transactions dating back to September 1, 2019. The breach is attributed to an improperly secured database that was not password-protected. The database is said to have been exposed for up to three weeks before it was taken offline. ***The NTIC Cyber Center recommends PAAY users monitor associated payment accounts and report any suspicious and unauthorized activity to their financial institutions.***

EXECUPHARM
A Parexel® Company

ExecuPharm, an outsourcing company that serves the pharmaceutical industry, was the victim of a CLOP ransomware attack in March 2020 that resulted in the compromise of sensitive corporate and employee information including Social Security numbers, financial information, drivers licenses, passport numbers, and other data. This breach is the latest in a series of cyber attacks in which ransomware operators threaten and subsequently publish data belonging to victims who refuse to pay the ransom. ***The NTIC Cyber Center encourages those affected to place a fraud alert or***

security freeze on their credit file with Equifax, Experian, or TransUnion. In addition, we advise activating the free credit monitoring and identity protection services offered by ExecuPharm to affected individuals.

Ambry Genetics, a California-based genetic testing laboratory, reported a data breach that may have exposed the medical information of almost 233,000 individuals. The incident occurred between January 22 and 24, 2020 and is considered the second-largest data breach affecting healthcare records so far this year. Compromised data includes customer names, medical information, and Social Security numbers. ***The NTIC Cyber Center encourages those affected to place a fraud alert or security freeze on their credit file with Equifax, Experian, or TransUnion.***

Upcoming Webinars

Staying Secure and Compliant in a Work from Home Environment

It is a lot for IT teams to handle a remote workforce. Keeping up with security issues, maintaining data compliance, and minimizing data loss are some of the challenges IT teams are facing today.

In this webinar, we will cover how IT and security teams can empower end-users working remotely by increasing their ability to collaborate while also ensuring data security and compliance.

What we will cover:

- Staying compliant when employees work remotely
- How to eliminate shadow IT in terms of data sharing
- Ways you can make sure the authentication process for accessing company data is still under IT control

To register for this free webinar on Tuesday, May 5 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.

Fleeceware apps are mobile device applications that charge users high subscription fees after the app's free trial period ends. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Would You Have Fallen for This Phone Scam?

Analytic Comment: As security protocols dictating access to financial accounts improve, attackers are employing increasing sophisticated tactics to trick banking customers into divulging sensitive information that would allow unauthorized access into their accounts. In recent KrebsOnSecurity reports, readers shared stories of how profit-motivated cyber criminals were able to fool otherwise tech-savvy individuals into providing sensitive information such as security words, allowing them to gain access and make changes to their accounts. It is interesting to note that the two stories shared by readers also employed phone number spoofing in their schemes, which underscores the importance of never providing any sensitive personal or financial information during a phone call that you did not initiate. When in doubt, hang up on the caller and place a call to the financial institution's phone number directly for account-related questions and concerns.

Scammers Targeting Jobless Trying to Work from Home, Law Enforcement Says

Analytic Comment: As is the case with any crisis or disaster, nefarious actors often look for ways to exploit the situation and prey on society's most vulnerable individuals. Knowing that many people are currently out of work due to the pandemic, scammers are using logos and branding of popular companies to promote fraudulent job postings designed to steal money from individuals who may already be struggling financially. Before responding to any job offer online, thoroughly research the organization prior to sending any personal or financial information. Additionally, never agree to deposit any checks sent by the organization that are not specifically designated as a salary payment. Never agree to deposit a check into a personal account and then immediately transfer a portion of the money back to the organization and never deposit a check to your personal account to make purchases from third-party vendors on behalf of any organization.

Recycling Credentials in Four Easy Steps

Analytic Comment: This report from cybersecurity company Intsights provides a step-by-step process to explain how cyber threat actors collect and use stolen login credentials to compromise accounts. Credential stuffing attacks are commonly employed to target and compromise a large number of victims and accounts quickly and data breaches often provide these hackers with the information they need to conduct these attacks. This report highlights the risks of only requiring passwords for authentication and using the same login credentials across multiple accounts. For more information on this type of attack, please see our report titled Credential Stuffing Attacks - A Growing Yet Easily Mitigated Threat.

Patches and Updates

Adobe Releases Security Updates for Multiple Products

Google Releases Security Updates for Chrome

Juniper Releases Security Updates for Junos OS

Samba Releases Security Updates

VMware Releases Security Updates for ESXi

ICS-CERT Advisories

Sierra Wireless AirLink ALEOS (Update B)

We welcome your feedback.

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

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

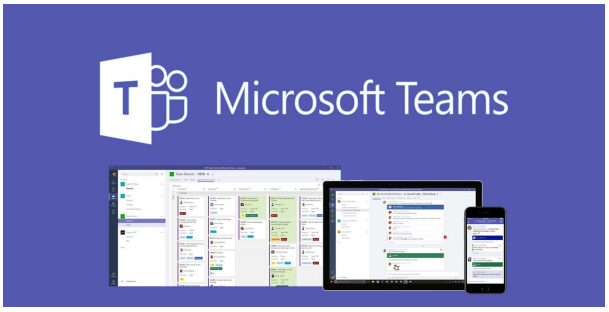
TLP:WHITE

Product No. 2020-05-008

HSEC-1 | NTIC SIN No. 2.5, 5.4

May 7, 2020

National Capital Region Cyber Threat Spotlight



Phishing Campaign Targeting Office365 Credentials Uses Fake Teams Alert

Security researchers recently discovered a sophisticated phishing campaign attempting to collect Office 365 credentials from unsuspecting victims by spoofing automated Microsoft Teams notifications. Cyber threat actors behind this campaign clone Microsoft Teams alert to craft convincing emails. These emails contain a link that, if clicked, will eventually deliver victims to a phishing page designed to look like the Microsoft Office 365 login page. If visitors to the page enter their login credentials, the attackers will collect them and use them to compromise their accounts. To bypass email security gateways, the link contained in the emails redirects victims through several websites before delivering them to the phishing landing page. ***The NTIC Cyber Center encourages all users of Microsoft Office products maintain awareness of this and other phishing threats and log into their Microsoft Teams account directly through the application, rather than via a link provided in a notification email. If you use Microsoft Teams within a work environment and you believe you have fallen victim to this or any other Microsoft Office phishing scheme, notify your organization's IT department immediately so that they may force a password reset and prevent further account compromise.***

Remote Workers Targeted with Fake Zoom Downloader

Trend Micro researchers have discovered a malware distribution campaign that attempts to trick remote workers into downloading a malicious Zoom installation file containing the RevCode WebMonitor Remote Access Trojan (RAT). If installed, the RAT will allow the threat actors behind the campaign to remotely access and control the victim's machine, steal sensitive data and login credentials, log keystrokes, and modify system processes. Because the malware is bundled with a legitimate Zoom installation file, victims may not immediately know they have been compromised. ***The NTIC Cyber Center recommends Zoom users only download Zoom installation files from Zoom's official download center. We encourage network administrators to proactively block the associated indicators of compromise (IoCs) provided in the Trend Micro report. If you believe you have downloaded a malicious Zoom installation file or have become infected with the RevCode WebMonitor RAT or any other malware, notify your organization's IT team immediately.***

Current and Emerging Cyber Threats

Malvertising Campaign Targets 900,000 WordPress-Powered Websites

WordPress security company Defiant observed a drastic increase in attacks attempting to exploit cross-site scripting (XSS) vulnerabilities within WordPress-powered websites beginning April 28, 2020. According to the company's threat intelligence team, the attacks are originating from a single cyber threat actor who attempts to inject malicious JavaScript code designed to redirect website visitors to malicious websites. The threat actor also exploits active administrator sessions to insert backdoors into vulnerable WordPress themes' headers. Targeted plugins include Easy2Map, Blog Designer, WP GDPR Compliance, Total Donations, and Newspaper. ***The NTIC Cyber Center recommends all WordPress website administrators update plugins to the latest versions and remove outdated plugins that are no longer supported or available in the WordPress repository. We also recommend enabling multifactor authentication on all WordPress administrator accounts.***

Vulnerable WordPress Plugins Leveraged to Deliver Adwind RAT

Researchers at Zscaler ThreatLabZ discovered that threat actors are leveraging compromised WordPress websites to distribute the Adwind remote access Trojan (RAT). This is easily done

through the exploitation of WordPress plugin vulnerabilities, allowing threat actors to gain access to the administrative panel of the WordPress Content Management System (CMS). Once access is secured, the threat actors upload malicious payloads to the website server to be delivered to unsuspecting website visitors. In this particular case, the threat actors used malicious Java archive (JAR) files to conceal and deliver the Adwind RAT. This RAT's capabilities include collecting system information, keystrokes, login credentials, and web form data. It can also record video and sound and take screenshots on infected systems. ***The NTIC Cyber Center recommends WordPress website administrators to keep all systems up to date with the latest patches, avoid downloading plugins or running JAR files from unknown or untrusted sources, enable two-factor authentication on website administrator accounts, and properly vet all plugins and themes prior to and after installation.***

Several Websites Leak Emails to Advertisers and Analytics Companies

Researchers published a report on April 29, 2020 that multiple websites have been leaking its users email addresses to third-party advertising and analytics companies. When a third-party loads its JavaScript code on a website, it can pass information about the visitor's location, type of device, browser fingerprints, cookies, and URL query strings or parameters through request headers that are transmitted to the third-party's domain. Creating a new account on a website or unsubscribing to a newsletter can send personal information to third-party companies and some argue that these should be classified as data breaches based on current regulations and laws in many countries. ***The NTIC Cyber Center recommends users maintain awareness of this and similar threats, be aware of phishing and spam campaigns that can result from these data leaks, and use a reputable ad-blocker to prevent JavaScript from loading in the browser.***

Fraudulent Antivirus Software Expiration Scheme Discovered

Scammers are distributing fraudulent antivirus software expiration warnings to recipients to profit from software license renewal commissions. These scammers are rogue security software affiliates that ignore company guidelines to sell software subscriptions under false pretenses. In this case, scammers send fraudulent expiration alerts via emails that contain a link to purchase a renewal. Once clicked, the affiliate will leverage a tracking cookie to earn credit on sales via the purchase page. ***The NTIC Cyber Center recommends users verify expiration dates of antivirus software before renewing their subscriptions and only use the official antivirus software company's website to download any updates. As always, we recommend never clicking on links or opening attachments in emails that originate from unknown or unexpected sources.***

Pirated Movie Files Used to Deliver Malware

The Microsoft Security Intelligence team issued a warning about malicious Visual Basic Scripts (VBScripts) used in a recently discovered cryptocurrency-mining campaign, targeting people who download pirated movies. This campaign turns movie piracy sites into tools that can deliver malware to the users of the site through fraudulent movie torrents. Threat actors camouflage its malicious zip file with titles of trending blockbuster movies or offer promises of pre-release copies of movies or television shows. ***As downloading and sharing pirated movies, music, and software is illegal, the NTIC recommends only using legal platforms to download and stream media to prevent these types of malware infections.***

Mobile Ad Delivery Platform Abused to Push Data-Stealing Malware

Threat actors are exploiting an Android advertisement distribution platform known as StartApp to deliver data-stealing malware to victims. To conduct this activity, the threat actors inject malicious ads into software development kits (SDKs) meant for distributing legitimate ads. When applications use third-party and dynamic advertising services to support their apps using ad revenue, they lack complete control of which ads are displayed on their app and can become vulnerable to these types of attacks. App users who do not vet applications before installation can then become infected by ads containing malicious code. ***The NTIC Cyber Center recommends that users only download applications from trusted and vetted sources, keep device operating systems up to date, and backup data on mobile devices regularly. In addition, before installing any app, exercise caution and research both the app itself and the developer. Once an app is installed, monitor the app's requests for permission authorizations and data activity.***

EventBot Android Malware Bypasses 2FA

Researchers at Cybereason Nocturnus have been investigating a new Android banking trojan, dubbed "EventBot," that bypasses two-factor authentication (2FA) and steals financial information from Android users. This campaign downloads a malicious application that targets users of over 200 different financial institutions while EventBot runs in the background of the device, acting as a keylogger. EventBot requests permission to launch as soon as the device boots, to read and receive SMS messages, to receive notifications about other installed applications, and access any content displayed on the device screen. This campaign is in its early stages of development, but is already considered to be a major threat due to its sophistication. ***The NTIC Cyber Center recommends Android users avoid downloading apps from third-party marketplaces and carefully scrutinize all user reviews prior to installation, even when downloading apps from the official Google Play store.***

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 Has Worm-Like Properties and Spreads Quickly

A new ransomware dubbed Lockbit performs ARP requests and exploits open SMB ports to spread across a network in a worm-like manner and lock hundreds of devices and in just a few hours. 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. In one incident, Lockbit was able to encrypt approximately 25 servers and 225 workstations within three hours. While threat actors who spend an extended amount of time on a compromised have an increased chance of being detected, Lockbit operators decrease their risk of detection due to how rapidly the ransomware spreads across a network. It appears that, in one LockBit incident, the attacker brute-forced an administrator account via an outdated and vulnerable VPN service to gain access to the targeted network. More information about this ransomware variant, including IoCs, is available in McAfee's report.

Vulnerabilities

SaltStack Salt

Researchers from F-Secure disclosed two high-severity vulnerabilities that can allow threat actors to conduct remote code execution on SaltStack Salt, an open-source management framework for cloud environments. The first vulnerability, CVE-2020-11651, allows remote user access without authentication. The second vulnerability, CVE-2020-11652, allows arbitrary directory access. Upon vulnerability disclosure, SaltStack Salt developers have since released a patch to remediate the vulnerabilities. ***As there have already been reports of cyber threat actors exploiting these vulnerabilities, the NTIC Cyber Center highly recommends all administrators of SaltStack Salt update to the latest versions 2019.2.4 and 3000.2 as soon as possible.***

Upcoming Webinars

Data Breach Today
Prevention. Response. Notification.

Social Engineering Campaigns Target You: Don't Be a Victim, Be Prepared

People are the weakest link in your security posture.

Naturally, people are trusting. That trust can be abused- allowing for the wrong links to be clicked, malware to be installed and sensitive data to be leaked. With today's changing landscape including accommodating the remote worker, IoT everywhere and using a cloud first approach to services, your users are bound to experience the threat of social engineering, especially with today's landscape where cybercriminals are exploiting COVID-19.

Join us to learn about the real threat to your people including:

- How to use open source tools to simulate various forms of social engineering attacks using a penetration testing framework
- Learn industry best practices for reducing the risk of social engineering
- And learning the steps you can take to improve your people, process and technology

To register for this free webinar on Tuesday, May 13 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.

Counterfeit goods are fraudulent products that are similar or nearly identical to their legitimate counterparts and are typically sold for financial gain. While the sale of counterfeit goods is not a new practice, advances in technology and the popularity of e-commerce platforms have led to an increase in the prevalence of counterfeit goods distribution. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Local Governments Asked to Protect Small Businesses from Cyber Threats

Analytic Comment: Small businesses have been requesting aid from state governments to assist with cybersecurity needs to secure their financial systems and remote workers who are at home during the COVID-19 pandemic. With cyber threat actors creating campaigns daily targeting coronavirus relief funds and online payments, some businesses have been forced to move all operations offline to keep their data secure. California's state and local agencies have been assisting each other in producing weekly reports detailing global, national, and state-based threats with cybersecurity tips and pushing that information to trusted organizations. The Cyber Readiness Institute has stated that "gathering cybersecurity information in one place is the most helpful thing local governments and their partners could do," and that "by placing private-sector technology leaders alongside state governors to dispense basic cyber hygiene, business owners should be able to find all the cybersecurity information they need in one place." This model has shown to be effective and is encouraged in all states.

Hacker Bribed "Roblox" Insider to Access User Data

Analytic Comment: Roblox, a popular online game among children with over 100 million active users, was breached when a hacker bribed a Roblox employee for access to the backend customer support panel. Within the support panel, the hacker is able to view users' email addresses, change

passwords, ban users and modify multifactor authentication settings. While Roblox spokesperson stated that a very small number of customers were impacted and individually notified, this incident underscores the importance of implementing organizational policies and audits to reduce the risk that insider threats can pose.

Patches and Updates

Cisco Releases Security Updates for IOS XE SD-WAN Solution Software

Google Releases Security Updates for Chrome

Mozilla Releases Security Updates for Firefox and Firefox ESR

SaltStack Patches Critical Vulnerabilities in Salt

Unpatched Oracle WebLogic Servers Vulnerable to CVE-2020-2883

ICS-CERT Advisories

Fazecast jSerialComm

LCDS LAquis SCADA

SAE IT-systems FW-50 Remote Telemetry Unit (RTU)

We welcome your feedback.

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

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-05-017

HSEC-1 | NTIC SIN No. 2.5, 5.4

May 14, 2020

National Capital Region Cyber Threat Spotlight

Nigerian-Based BEC Campaign Targets Government Health and Medical Agencies

Researchers within Palo Alto's Unit 42 intelligence group have been tracking a Nigerian-based business email compromise (BEC) campaign targeting a variety of government agencies at the local, state, and national level. Dubbed SilverTerrier, this campaign has been active since January 30, 2020, using COVID-19 lures to target victims working for medical or healthcare-focused government agencies within the US and across the globe. The phishing emails used in this campaign attempt to infect systems with Agent Tesla and NanoCore remote access Trojans (RATs), LokiBot and Formbook information-stealing malware, and PowerShell scripts to deliver additional malware to victims. The emails are designed to look as thought they have originated from a legitimate person or department within the targeted organization or a familiar third-party, often using the word "Invoice" in the subject line to prompt recipients to open the emails and malicious attachments. BEC scams are commonly used to divert legitimate funds to criminal-owned financial accounts, but can also be used to deliver malware and compromise email accounts within an organization. ***The***

NTIC Cyber Center recommends employees of all US government organizations maintain awareness of BEC scams, refrain from opening attachments or clicking on links within unexpected emails, and verify financial transaction procedures with multiple parties within your organization before submitting any payment requests received via email or over the phone. If you believe you have been impacted by this or any other BEC campaign, notify your organization's IT department immediately. To learn more about this type of attack, please see our blog post titled [Securing Our Communities: BEC Scams]().

Federal Partner Announcement

North Korean Malicious Cyber Activity

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Defense (DoD) have identified three malware variants—COPPERHEDGE, TAINTEDSCRIBE, and PEBBLEDASH—used by the North Korean government. In addition, US Cyber Command has released the three malware samples to the malware aggregation tool and repository, VirusTotal. The US Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA.

CISA encourages users and administrators to review the Malware Analysis Reports for each malware variant listed above, US Cyber Command's VirusTotal page, and CISA's North Korean Malicious Cyber Activity page for more information.

Top 10 Routinely Exploited Vulnerabilities

CISA, the Federal Bureau of Investigation (FBI), and the broader US Government are providing this technical guidance to advise IT security professionals at public and private sector organizations to place an increased priority on patching the most commonly known vulnerabilities exploited by sophisticated foreign cyber actors.

This alert provides details on vulnerabilities routinely exploited by foreign cyber actors—primarily Common Vulnerabilities and Exposures (CVEs)—to help organizations reduce the risk of these foreign threats.

Foreign cyber actors continue to exploit publicly known—and often dated—software vulnerabilities against broad target sets, including public and private sector organizations. Exploitation of these

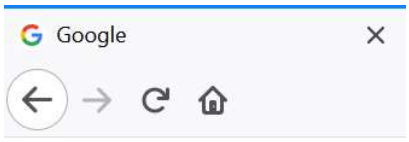
vulnerabilities often requires fewer resources as compared with zero-day exploits for which no patches are available.

The public and private sectors could degrade some foreign cyber threats to US interests through an increased effort to patch their systems and implement programs to keep system patching up to date. A concerted campaign to patch these vulnerabilities would introduce friction into foreign adversaries' operational tradecraft and force them to develop or acquire exploits that are more costly and less widely effective. A concerted patching campaign would also bolster network security by focusing scarce defensive resources on the observed activities of foreign adversaries. For more information, along with indicators of compromise, a list of vulnerabilities, and mitigation recommendations, please see CISA Alert AA20-133A.

Current and Emerging Cyber Threats

Magecart Group Leverages Favicons to Steal Payment Card Data

Malwarebytes researchers recently discovered a Magecart campaign that leverages favicons to load a malicious JavaScript data-skimmer into ecommerce websites and collect visitors' personal and payment card data. Favicons are the small branding logos or icons usually displayed within the title or address bar of web browsers when someone visits a website.



(The multi-colored "G" is an example of a favicon.)

In this campaign, the Magecart group created a fraudulent favicon hosting service to serve the malicious icons, and then promoted free downloads to website administrators who wanted to embed a favicon on their sites. Once embedded, the malicious favicon collects any data that is entered on the site, including names, addresses, phone numbers, email addresses, and payment card information. ***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. We also recommend website administrators exercise extreme caution before embedding any elements provided or hosted by third-parties into their websites.***

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

Phishing Campaign Targets Cisco WebEx Users

An email phishing campaign that clones the graphics and formatting design of a Cisco WebEx automated Secure Socket Layer (SSL) certificate error has been targeting and attempting to steal account credentials from WebEx users. These threat actors persuade recipients of the phishing email to act urgently by sending a fraudulent email claiming the user has been blocked from the platform due to SSL certificate errors, prompting them to log into WebEx and verify their account. The login link embedded in the emails redirects victims to a phishing landing page designed to collect WebEx login credentials for use in future attacks. Users of other video conferencing platforms have also been targeted in similar phishing campaigns. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns disguised as video conference email 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 believe you have been targeted by this campaign notify your organization's IT security team immediately.***

New Chinese Botnet Malware Kaiji Targets Linux Servers and IoT Devices

Researchers at security firm Intezer discovered a Chinese-based botnet malware, dubbed "Kaiji," targeting Linux-based servers and internet-of-things (IoT) devices. Kaiji is unique in that it is written from scratch in the Golang programming language and it exclusively conducts Secure Shell (SSH) brute-force attacks to target the root user account on devices. Root access is essential for Kaiji as it needs custom network packets from privileged root user accounts to conduct distributed denial-of-service (DDoS) attacks. When the SSH connection is made, a bash script is executed to prepare the environment for Kaiji. ***The NTIC Cyber Center recommends network administrators disable unneeded SSH connections, use lengthy, complex, and unique administrator credentials, and regularly monitor devices for unauthorized user accounts and access. Additionally, we also recommend administrators review Intezer's report and proactively block any associated Indicators of Compromise (IoCs).***

FINRA Alerts Members to Widespread Phishing Campaign

The US Financial Industry Regulatory Authority (FINRA) alerted members of an ongoing phishing campaign targeting Microsoft Office and SharePoint user credentials. This phishing campaign uses the domain address broker-finra[.]org to spoof email correspondence from FINRA's vice presidents to lure users into opening a malicious PDF attachment. The PDF file contains a link that, if clicked,

redirects victims to a phishing page designed to collect victims' Microsoft Office and SharePoint login credentials. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns disguised as FINRA email 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 believe you have been targeted by this campaign notify your organization's IT security team immediately.***

Corporate MDM Server Exploited to Deliver Cerberus Trojan

A threat actor compromised a "multinational conglomerate" with the Cerberus Trojan, infecting more than 75 percent of their Android devices. Cerberus is a banking Trojan that collects private data such as credentials, keystrokes, contacts, and SMS messages and exfiltrates it to a command-and-control (C2) server. Additionally, Cerberus can maintain persistence by leveraging administrator privileges to prevent uninstallation attempts and disabling Google Play Protect, halting the detection and removal of the malware. The initial attack vector is attributed to target's mobile device management (MDM) server, in which the threat actors were able to breach and abuse its remote installation app features to further distribute malware onto numerous Android devices. ***The NTIC Cyber Center recommends network administrators to properly configure security settings when using asset management services. Users who believe their devices have been infected with Cerberus Trojan should notify their organization's IT security team immediately. We recommend network administrators review Check Point's report and proactively block the associated IoCs.***

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.

VCrypt Variant Locks Files Using 7-ZIP

A new ransomware variant known as VCrypt leverages the legitimate 7-ZIP command-line program to generate password-protected data archives. Once VCrypt compromises a machine, it deletes files found in various Windows data folders and creates new "encrypted" files named after the folders,

appending the *.vxcrypt* extension to the name. It then launches the Internet Explorer browser to display a ransom note named *help.html* that includes instructions on how to recover the locked files. Researchers determined that this variant does not actually encrypt files, but rather acts as a data-wiping malware. VCrypt primarily targets French users and the attack vector is currently unknown. Bleeping Computer provides associated IoCs here.

Toll Group Impacted by Nefilim Ransomware Attack

Transportation and Logistics service provider Toll Group reported that on May 5, its network was compromised by Nefilim ransomware, making it the second successful ransomware attack that Toll Group has experienced in three months. The company noticed unusual activities on a few of their servers prompting them to shut down their network to investigate and remove any threats. Neflim is a relatively new variant distributed by a Ransomware-as-a-Service (RaaS) operation in which less-skilled hackers can use their service to launch ransomware attacks against targeted organizations. Fortunately, there is no evidence to suggest that any data had been extracted from the Toll Group network, but the company did have to disable their MyToll shipping portal customer site for the time being.

Taiwan Oil Refinery Targeted in Ransomware Attack

Cyber attacks recently targeted two of Taiwan's natural resource companies, the state-owned petroleum, gasoline, and natural gas company CPC Corporation and Formosa Petrochemical Corporation (FPCC), one day apart. On May 4, 2020, CPC's cybersecurity experts reported a ransomware attack that caused outages on their network that left gas stations unable to access the digital platform it needed to accept customers VIP cards or electronic payment apps. That attack on CPC put FPCC's staff on high alert on May 5, 2020, leading to the discovery of "irregularities" on FPCC's corporate network where malware was quickly located and removed. The malware variants and attack vector are currently unknown.

Maze Ransomware Operators Claim to Attack US Egg Supplier

The threat actors behind MAZE ransomware claimed to have compromised egg supplier and producer, Sparboe Companies. The threat actors shared a ZIP file named "part1" containing 17 folders that include data such as current and former employee information, nest-run inventory, expense reports, injury reports, dock schedules, and other data. Sparboe Companies has neither confirmed or denied the alleged MAZE ransomware attack and has yet to publish an official response. Sparboe Companies is one of several companies in which MAZE threat actors have claimed to have targeted.

Sodinokibi/REvil Now Encrypts Open Files

Sodinokibi ransomware, also known as REvil, has received an upgrade that allows it to encrypt files that are already open and locked by another process. Various applications such as databases and mail servers lock files that are open through them, to prevent file corruption or multiple processes writing to a file simultaneously. Generally, ransomware is unable to affect or encrypt files that are locked in these processes; however, Sodinokibi can now automatically disable this function and impact files that a user has open through another application.

Vulnerabilities

Citrix ShareFile

Citrix has fixed three vulnerabilities for its collaboration and file sharing platform, ShareFile. If exploited, these vulnerabilities allow unauthorized parties to access private data. While the exact details of the flaws have not been disclosed, the vulnerabilities affect ShareFile storage zones Controller 5.9.0, 5.8.0, 5.7.0, 5.6.0, and 5.5.0. Customers with Citrix-managed storage zones do not need to take any action, although Customer self-managed storage zones are encouraged to take mitigating steps to protect themselves against exploitation. ***The NTIC Cyber Center recommends Citrix ShareFile users with self-managed storage zone themselves should immediately sign-in and utilize the latest mitigation tool.***

Data Leaks and Breaches

Dating app MobiFriends experienced a data breach in January 2019, exposing the personal details of over 3.6 million registered users on several online forums. The stolen data did not contain private messages, images, or adult content, but information such as email addresses, mobile numbers, birth dates, genders, usernames, passwords, and website activities were compromised. Risk Based Security (RBS) noticed the data leak online then verified the validity of the data against the MobiFriends website. Details about how the application was hacked and the threat actors behind this campaign are currently unknown. ***The NTIC Cyber Center recommends users of the***

MobiFriends dating app remain vigilant for phishing emails exploiting this data breach, especially sextortion campaigns, and immediately change their passwords to their MobiFriends account and any other accounts that use the same credentials. We always recommend using passwords that are unique to each account.

ChatBooks, a photo print service for social media, disclosed a data breach that resulted in the exposure of personal information for approximate 15 million user records. The perpetrators listed the data for sale on the dark web as part of a series of breaches in which 11 companies were compromised, exposing over 73 million user records in total. Information exposed in the data breach includes names, e-mail addresses, hashed and salted password, phone numbers, FacebookIDs, and merchant tokens. Chatbooks does not currently believe that payment data was compromised. ***The NTIC Cyber Center recommends Chatbooks users remain vigilant for an increase in phishing attempts perpetrated through email, social media, telephone, text messages, or other avenues as a result of this data exposure. We also encourage using lengthy, complex, and unique passwords for each account and enabling multifactor authentication on any account that offers it to avoid falling victim to credential compromise.***

Upcoming Webinars

Enabling Consistent Multi-Cloud Security, Forensics, and Incident Response

Today's threat landscape is continually evolving, and it becomes evident that new tools are needed to identify and remediate these attacks effectively. Historically, organizations have standardized on infrastructure, which helps enable consistency for addressing security challenges. Due to the migration to the cloud, the data center has now become the most inconsistent infrastructure environment that many organizations operate. Every new cloud requires a complete rethinking of

how to implement security controls. To effectively defend against and respond to threats, we need to drive consistency. This session will cover how to enable effective threat defense and response across the hybrid cloud.

To register for this free webinar on Friday, May 15 at 10:30 AM EDT, click here

---

Securing Our Communities

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

A ***neighbor number scam***, also called ***neighbor spoofing*** or ***caller ID spoofing***, is a technique that scammers use to deliberately falsify telephone caller ID information to conceal their identifying information. Masquerading as a neighbor or otherwise legitimate local caller, scammers prey on those who answer these calls in any number of ways. Becoming familiar with neighbor number scam calls can help prevent you from falling victim to financial fraud and identity theft. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Remote Workers Failing on Password Security During #COVID19 Crisis
Analytic Comment: Several international studies reveal multiple telework security gaffes. One study revealed 17 percent of employees shared their work credentials with family members. While 70 percent of businesses are using multi-factor authentication (MFA) and virtual private networks (VPNs) to improve security, 54 percent of teleworkers are reported to have no plans to update work credentials despite having the means to update them. Since the pandemic has led to a dramatic increase in teleworking, it is imperative that companies to reconsider their security policies to ensure a proper security posture.

Hackers Turned Virginia Government Websites into Elaborate eBooks Scam Pages

Analytic Comment: Vulnerable websites and website servers, especially those associated with government agencies, are attractive targets for hackers seeking to host malicious content and craft convincing scams. If a top level domain (TLD) such as .gov is abused and used in a phishing campaign, it could easily trick victims into thinking the associated website is legitimate. All website administrators, but especially those who work for government agencies, are encouraged to regularly audit their website servers for unauthorized activity and ensure that they are up-to-date with the latest security patches.

Patches and Updates

Adobe Releases Security Updates

Microsoft Releases May 2020 Security Updates

ICS-CERT Advisories

3S-Smart Software Solutions GmbH CODESYS V3 Library Manager (Update A)

Advantech WebAccess Node

Eaton Intelligent Power Manager

Interpeak IPnet TCP/IP Stack (Update D)

OSIsoft PI System

Siemens KTK, SIDOOR, SIMATIC, and SINAMICS (Update A)

Siemens RUGGEDCOM, SCALANCE, SIMATIC, SINEMA (Update A)

Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC (Update C)

Siemens SINAMICS (Update C)

Siemens SIPROTEC 5 and DIGSI 5 (Update C)

We welcome your feedback.

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

TLP:WHITE

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

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on *Subscribe to Receive Our Products* at the top of the page, and enter your information.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-05-025

HSEC-1 | NTIC SIN No. 2.5, 5.4

May 21, 2020

National Capital Region Cyber Threat Spotlight

Romance Scammer Impersonates Top US Military Officials

On May 12, a cyber threat actor used the social media platform Facebook to impersonate the current commander of US Transportation Command and a Gmail account to masquerade as the head of the US Army Cyber Command to lure a victim into what is commonly known as a "romance scam." A romance scam, also known as a sweetheart scam or confidence fraud, is a social engineering scheme in which a perpetrator masquerades as a potential love interest, concealing his or her true intentions to elicit money or material possessions from unsuspecting victims looking for love online. These scammers, who work either alone or in an organized crime ring, create detailed fraudulent profiles on dating websites, apps, and social media platforms using images stolen from legitimate profiles or elsewhere on the Internet.

Although this victim recognized that this was a scam before it resulted in any financial loss, many people fall victim to romance scams each year. In 2019, the Federal Trade Commission (FTC) declared that romance scams resulted in more consumer financial loss than in any other scam and stated that the median reported loss to romance scams is approximately seven times higher than that

of other fraud schemes. Romance scams typically target emotionally vulnerable people and exploit them for profit, but they can also be used to conduct sophisticated cyber-espionage campaigns to obtain confidential or classified information from targets.

To learn more about identify and protect yourself from romance scams, please read our blog post titled Securing Our Communities: Romance Scams.

Federal Partner Announcement

CISA Releases Resources for Schools Using Video Conferencing Platforms

CISA released two documents on securing video conferencing for schools: **(TLP:WHITE) Cybersecurity Recommendations for K-12 Schools Using Video Conferencing Tools and Online Platforms** and **(TLP:WHITE) CISA Cybersecurity Tip Sheet for Schools Using Video Conferencing.** They can be found at: https://www.cisa.gov/publication/secure-video-conferencing-schools.

The first document is for school district and campus IT administrators and staff charged with securing their IT networks, as well as end users such as teachers to help them think through cybersecurity issues. The second document includes non-technical tips to keep users and students safe.

We kindly request any questions or feedback related to this document be reported to CISA at CISAservicedesk@cisa.dhs.gov or 888-282-0870.

ICE HSI Promotes Online Safety for Kids through Virtual Presentations

US Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Child Exploitation Investigations Unit (CEIU) is now offering virtual presentations for school systems and

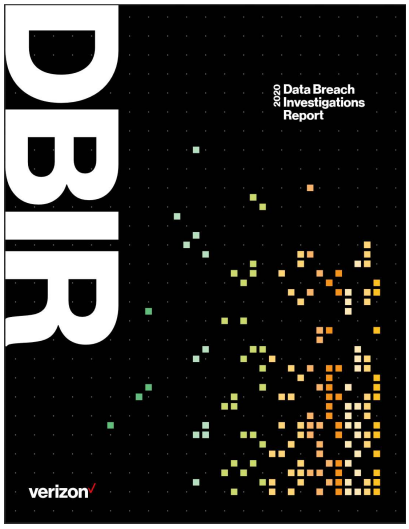
youth organizations nationwide through the Project iGuardian program. Through online seminars, parents, teachers and students will have the opportunity to learn more about the dangers of online environments, how to stay safe online and how to report abuse and suspicious activity – particularly while kids are using online learning tools during the COVID-19 pandemic.

"A laptop, a phone, or other internet-connected device could lead children into a world where they may be at risk. This is especially true with apps providing messaging, photo, or video sharing capabilities; in chat rooms; and on gaming platforms," said Erin Burke, section chief for Cyber Crimes Center CEIU and Victim Identification Program. "It is imperative that parents and other trusted adults have conversations with children and provide oversight to ensure they aren't exposed to environments where they could potentially be vulnerable to predators."
Organizations interested in taking part in the virtual presentations can submit requests to iGuardian@ice.dhs.gov. Requests should include the following information:

- Contact information including organization, name, phone number, and email
- Requested date/time
- Preferred online platform
- Type of audience:
    1. Parent, guardian or educator
    2. Children (Kindergarten – 5th grade)
    3. Youth (6th-8th grade)
    4. Youth (9th-12th grade)

Project iGuardian is an outreach effort to share information focused on keeping children and teens safe from online predators through education and awareness. The project helps children, teens, and parents be smarter about online safety and avert online sexual predators by providing safety tips a number to call, and a website with links to more information and resources.
In fiscal year 2019, the number of children HSI rescued and/or identified from instances of child exploitation grew to 1,069, compared to 859 the year prior. This fiscal year, as of March 2020, HSI has initiated more than 2,700 cases and have made more than 1,400 criminal arrests related to the exploitation of children. Since 2013, HSI has rescued and/or identified over 6,500 child victims, thanks in part to initiatives like Project iGuardian.
To report suspicious activity or instances of child sexual exploitation, contact your local law enforcement agency. Tips can be submitted online at ice.gov/tipline, by phone at 866-DHS-2-ICE or by contacting your local HSI office. Reports can also be filed with the National Center for Missing & Exploited Children (NCMEC) at 1-800-THE-LOST or online at cybertipline.org.

Industry Report



Verizon Releases 2020 Data Breach Investigations Report

Verizon's 2020 Data Breach Investigations Report (DBIR) highlights trends and commonalities found within 3,950 data breaches analyzed throughout the course of last year. In their summary of findings, 45 percent of these incidents involved active hacking techniques such as brute force or vulnerability exploitation to gain entry into networks, 70 percent of breaches were conducted by external threat actors, 72 percent of victims were large businesses, and 86 percent of data breach incidents were financially motivated. Additionally, 37 percent of breaches involved stolen credentials, either to gain access to networks or to collect them from victims. ***The NTIC Cyber Center recommends all network administrators review Verizon's 2020 DBIR to learn about the most prevalent attacks and tactics used to infiltrate networks, compromise systems, and conduct data theft.***

Current and Emerging Cyber Threats

Fake Zoom "Missed Meeting" Emails Steal Login Credentials

Researchers at Abnormal Security have uncovered a phishing campaign in which threat actors are masquerading as Zoom to steal Microsoft Office 365 credentials. Threat actors are crafting fraudulent Zoom email notifications alerting recipients of a missed meeting. The email prompts users to click a link to get more details and a recording of the meeting. Once clicked, recipients are forwarded to a fraudulent landing page used to harvest entered credentials. ***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.

Magecart Continues to Threaten Vulnerable Ecommerce Sites

A security researcher discovered 1,236 domains that were infected with payment card skimmers resulting from Magecart's continued attacks on insecure ecommerce websites. This investigation was performed using free online tools to track malicious java scripts and changes to the skimmer's domain. The researcher determined that online businesses within the United States represented the largest number of Magecart infections. However, not all of the infected websites loaded its data to the credit card skimmer as the skimmer's domain may have been unreachable or disabled. ***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. We also recommend website administrators exercise extreme caution before embedding any elements provided or hosted by third parties into their websites.***

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.

YouTube Account Recovery Phishing Campaign Discovered

An account recovery phishing campaign that is being used to steal credentials from Youtube content creators was discovered on a compromised WordPress website. The compromised website contained two pages designed to harvest usernames, passwords, and recovery numbers that could later be used to gain unauthorized access to accounts through the account recovery process. Even though it is currently unknown what lure was used to attract victims to the phishing page, researchers observed that HTML code on the phishing page was sending data to a third-party URL while redirecting victims to the YouTube's Creator Awards website. ***The NTIC Cyber Center recommends users remain vigilant for phishing emails, avoid opening unexpected emails, and refrain from clicking on links or opening attachments from unknown or untrusted sources. Additionally, before entering any login credentials or sensitive information into a website, verify the URL to ensure it is legitimate. If you receive an email that you suspect may be malicious or you believe you have entered your organization login credentials into a phishing website, notify your IT security team immediately.***

Ramsay Malware Designed to Infect Air-Gapped Systems

ESET researchers discovered that Ramsay malware can pilfer data from air-gapped systems, which are systems or networks that are isolated from the rest of an organization's network and are not accessible via public internet. ESET was able to uncover three different Ramsay malware variants that were able to scan a compromised system and collect Word, PDF and ZIP documents and store them in a hidden folder for exfiltration at a later date. In some variants, Ramsay can spread in a network environment through portable executable files via removable drives and network shares. While it is uncertain how the stolen data is being exfiltrated and who is behind this operation, Ramsay does contain shared elements with Retro malware from the DarkHotel hacker group believed to be affiliated with the South Korean government. ***The NTIC Cyber Center encourages network administrators to remain vigilant for Ramsay malware and exercise caution when using removable drives and network shares on air-gapped systems.***

Hoaxcalls and Mirai Botnets Target Symantec Secure Gateway 5.0.2.8

Researchers from Palo Alto Networks' Unit 42 discovered new Hoaxcalls and Mirai botnet campaigns targeting Symantec Secure Web Gateway 5.0.2.8, a product that reached its end-of-life (EOL) in 2015 and end-of-support-life (EOSL) in 2019. Threat actors are leveraging a post-authentication remote code execution on the 5.0.2.8 version to compromise devices, allowing them to proxy network traffic, download updates, prevent reboots, conduct DoS attacks, and maintain persistence. Symantec Web Gateway 5.2.8. is no longer exploitable with this vulnerability and there is currently no indication that any other version is vulnerable. Symantec states that Secure Web Gateway solutions, including ProxySG and Web Security Services, are unaffected. ***The NTIC Cyber Center encourages network administrators to remain vigilant for Hoaxcalls and Mirai botnet campaigns and proactively block the indicators of compromise (IoCs) associated with these botnets here. We also strongly recommend replacing any products that have reached their EOL or EOSL to newer, supported versions.***

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.

Ako Ransomware Demands Two Payments: One to Decrypt Files and One to Delete Stolen Data

The threat actors behind the Ako ransomware campaign are now demanding two ransom payments: one payment to decrypt files and another to delete stolen files. Stolen data can be used for leverage as the threat actors will likely threaten to publicly release it if victims do not remit both payments. These threat actors have already published stolen data after one of their victims payed $350,000 to decrypt their files but did not send the additional payment demanded for file deletion. While corresponding with members of the cybersecurity website BleepingComputer, the threat actors behind Ako ransomware campaigns claimed that that they use this double-extortion tactic on select victims that vary depending on the size of the victim organization and the type of data stolen. ***The NTIC Cyber Center assesses with high confidence that this tactic will be adopted by additional ransomware campaigns as threat actors seek to maximize profits and coerce victims into submitting multiple payments.***

Magellan Health Victimized in Ransomware Attack

On May 12, 2020, Magellan Health, Inc. filed a breach notification notice stating that the company had been victimized in a ransomware attack. Although the ransomware variant that impacted the company has not been made public, Magellan Health did state that the attack conducted using a phishing email that impersonated one of the company's clients. Additionally, the company announced that the attackers behind the ransomware campaign did exfiltrate data from a corporate server that included sensitive information such as names, addresses, employee ID numbers, Social Security numbers, and, in some cases, usernames and passwords. This incident highlights the ongoing threat of ransomware and data breaches conducted against large organizations, especially those within the healthcare sector.

Sodinokibi/REvil Targets Entertainment Law Firm, Steals 756 GB of Data

According to researchers at Emsisoft, entertainment law firm Grubman Shire Meiselas & Sacks was victimized in a ransomware attack that has exposed several A-list celebrities' data and personal information. An unknown threat group using the ransomware strain named Sodinokibi/REvil allegedly stole 756 GB of data from the entertainment law firm. The group threatened to release the data in nine installments if the ransom demands are not met. A small amount of data has already been published on a data leak website to lend credibility to their threat. In a follow-up report, the threat group claimed to have damaging information on President Trump and reportedly found a buyer for that data. They now are threatening to auction off stolen data associated with the pop singer, Madonna. Incidents such as these highlight the importance of treating ransomware infections as data breach incidents as threat actors who have gained access to a network can and often do steal

data.

ProLock Victimizes ATM Provider Diebold Nixdorf

On April 25, 2020, the largest automatic teller machine (ATM) provider in the United States, Diebold Nixdorf, suffered a ransomware attack on its corporate network that temporarily disrupted services. Diebold's security team disconnected its corporate network to investigate some abnormalities, where it was determined that a ProLock ransomware had breached their corporate network. Fortunately, Diebold revealed that the ransomware had been found and contained and did not affect ATMs, customer networks, or the general public.

Vulnerabilities

Unpatched Site Kit WordPress Plugin Vulnerable to Exploitation

Researchers at cybersecurity firm Wordfence, discovered a vulnerability in Site Kit, an official Google WordPress plugin, that could be used to gain administrator access to the Google Search Console within targeted websites. Threat actors can leverage the Google Search Console to inject malicious code, manipulate search engine results, remove pages from Google search results, modify sitemaps, and view sensitive performance data. The vulnerability is attributed to two flaws that allow subscriber-level users to escalate privileges and become Google Search Console owners on affected sites. While a patch is currently available, there are still over 100,000 unpatched sites that are vulnerable to exploitation. ***The NTIC Cyber Center recommends WordPress website administrators who installed the Site Kit 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 is also recommended.***

Upcoming Webinars

Data Breach®
Prevention. Response. Notification. TODAY

How to Avoid the Security Dangers with Working from Home (WFH)

The new normal for many office workers is working from home (WFH), and they are finding many new challenges and dangers which comes with this. This is because 90+% cyber security attacks

begin with email, and users are more at risk than ever of attack due to not having an IT department nearby or have the correct end-point protection and polices in place.

In this webinar, cyber security advisor and 8x awarded Microsoft MVP (Exchange/Office 365) J. Peter Bruzzese will discuss valid concerns and ways to mitigate those concerns.

Watch to learn about:

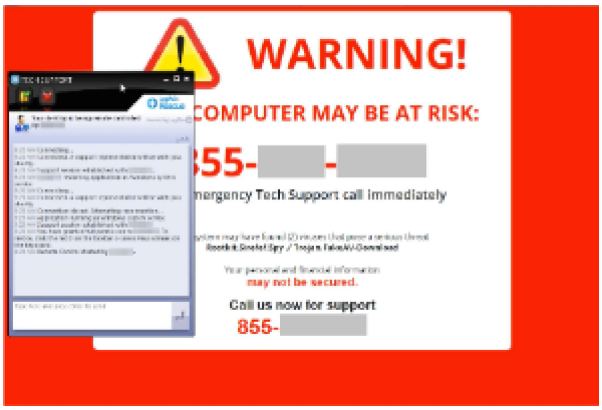
- Understanding the risks of not securing your home network
- How much protection do you really have from working from home
- How layered solutions can help protect you while working from home

To register for this free webinar on Wednesday, May 27 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.



Have you ever received an unsolicited phone call or email from someone offering to help fix a computer problem? How about a pop-up or error message indicating your device was infected and urging you to contact a support person who could help? If so, you were a target of a ***tech support scam***. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Why All Employees Need Cybersecurity Training
Analytic Comment: The COVID-19 pandemic has forced cybersecurity researchers to examine

employees' general awareness of cybersecurity responsibilities in order to close a serious security gap. A survey released earlier this year from Egress revealed that 64 percent of its respondents did not know that that all employees have a responsibility for keeping data safe, 65 percent of UK respondents have had no extra cyber attack training, and 52 percent of employees work using unsecured personal mobile devices. With most people working from home, it is important that companies provide frequent trainings on good password hygiene, how to detect and avoid phishing emails, and how to securely access sensitive data. Without these trainings, companies increase their risk of becoming victimized by successful cyber attacks.

Washington, DC Adds Security Requirements in New Data Breach Notification Law
Analytic Comment: Washington, DC recently expanded its data breach notification law (DC Act 23-268) to include additional categories of personal information covered by the law. The law initially covered victims' first names and last names in combination with a sensitive identifying number (Social Security number, driver's license or DC identification card number, or payment card number), or any codes that would allow access to an individual's financial account. The additional categories include victims' first names and last names with medical data, genetic data, health insurance data, and biometric data, or any listed data type that would allow a threat actor to commit identity theft without a name. The new law also requires businesses collecting DC residents' data to implement "reasonable security safeguards" and will allow lawsuits when an entity fails to meet these standards.

Patches and Updates

Adobe Releases Security Updates

Google Releases Security Updates for Chrome

ISC Releases Security Advisory for BIND

Microsoft Releases Security Advisory for Windows DNS Servers

VMware Releases Security Update for Cloud Director

ICS-CERT Advisories

3S-Smart Software Solutions GmbH CODESYS V3 (Update A)

Emerson OpenEnterprise

Emerson WirelessHART Gateway

Opto 22 SoftPAC Project

Rockwell Automation EDS Subsystem

We welcome your feedback.

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

TLP:WHITE

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

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on *Subscribe to Receive Our Products* at the top of the page, and enter your information.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-05-032

HSEC-1 | NTIC SIN No. 2.5, 5.4

May 28, 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 $350 and the fund will be inform of a (Cashier Check).

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 Local Organization,

Promotes Money Mule/Reshipping Scheme

The NTIC Cyber Center recently received a report of a phishing campaign targeting an organization within DC, promoting a possible "money mule" or "reshipping" scheme to potential job-seekers looking for work-at-home opportunities. The subject line of the email contains verbiage suggesting recipients can earn $350 weekly and the body of the email contains an invitation to accept part-time work that can be done from home, along with an embedded malicious link. The link 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 poor-quality stock photo.

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

CISA, DOE, and UK's NCSC Issue Guidance on Protecting Industrial Control Systems

The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Energy (DOE), and the UK's National Cyber Security Centre (NCSC) have released Cybersecurity Best Practices for Industrial Control Systems, an infographic providing recommended cybersecurity practices for industrial control systems (ICS). The two-page infographic summarizes common ICS risk considerations, short- and long-term cybersecurity event impacts, best practices to defend ICS processes, and highlights NCSC's product on Secure Design Principles and Operational Technology.

CISA, DOE, and NCSC encourage users to review Cybersecurity Best Practices for Industrial Control Systems. For more in-depth information, visit CISA's ICS Recommended Practices webpage and DOE's Cybersecurity Capability Maturity Model (C2M2) Program webpage. For information on CISA Assessments, visit https://www.cisa.gov/cyber-resource-hub.

Current and Emerging Cyber Threats

Blue Mockingbird Targets Enterprise Systems with Cryptocurrency-Mining Malware

Blue Mockingbird, a threat group active since 2019, is targeting enterprise systems in a cryptocurrency-mining campaign. The group targets public-facing enterprise servers running ASP.NET applications that use the Telerik framework for the user interface component, exploiting CVE-2019-18935 to install a web shell. Once the server is compromised, Blue Mockingbird uses a privilege escalation tool to gain administrator access and modify settings to maintain persistence on the machine. The group then installs the cryptocurrency-mining software XMRRig to mine for Monero, a type of cryptocurrency popular for its privacy and security features. If the server is connected to an internal network, Blue Mockingbird will attempt to move laterally through the network using remote desktop protocol (RDP) or server message block (SMB) ports. ***The NTIC Cyber Center recommends all network administrators regularly audit networks for vulnerable and unsecured servers and devices and ensure that all running software is patched with the latest version. We also recommend proactively blocking the associated indicators of compromise (IoCs) available in Red Canary's report.***

Phishing Campaign Spoofs US Supreme Court Correspondence

An ongoing email phishing campaign disguised as a US Supreme Court subpoena has been discovered targeting Office 365 credentials of unsuspecting recipients. According to researchers at Armorblox, this sophisticated scheme impersonating US Supreme Court correspondence is designed to trigger urgency and fear in busy employees who may not have the time to review every email in detail before clicking on the links. The link used in this campaign redirects users to a fully functioning CAPTCHA page where the victim is prompted to verify that they are not a bot to add legitimacy to the campaign. Next, victims are directed to a phishing page designed to look like the official Microsoft login page to capture credentials and use them for secondary attacks against employees, customers, or third-party vendors, or to exfiltrate confidential data. Researchers have noticed an increase in credential phishing attacks against small and medium-sized businesses that allow the attackers to potentially compromise larger affiliated companies. ***The NTIC Cyber Center recommends users remain vigilant for email phishing campaigns disguised as a correspondence from the US Supreme Court, 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 your Office 365 login credentials have been compromised in this or any other phishing scheme, notify your organization's IT team immediately.***

Phishing Campaign Exploits Symantec's Click-Time URL Protection

Researchers at Armorblox discovered a phishing campaign targeting Office 365 and Adobe Online credentials. These phishing emails masquerade as official correspondence and contain a malicious link claiming to lead to an externally-hosted file. Once clicked, the link will redirect to multiple URLs before loading a fraudulent landing page designed to steal account credentials. These emails can bypass Office 365 security controls as they do not display conventional detectable phishing patterns and leverage Symantec's Click-Time URL Protection tool to rewrite URLs. ***The NTIC Cyber Center recommends users remain vigilant for malicious email campaigns exploiting Symantec's Click-Time URL Protection, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources.***

New Cryptocurrency-Mining Botnet Discovered

Palo Alto Unit 42 researchers discovered a new botnet campaign that delivers Perl Shellbot to mine cryptocurrency on compromised devices and avoids detection by using a specially crafted rootkit. The threat actors known as "Los Zetas" spread Perl Shellbot by distributing malicious shell scripts to devices that are already compromised and can send instructions via an Internet Relay Chat-based command-and-control (C2) server once victims execute the downloaded scripts. Additionally, a shared library and a custom rootkit are leveraged to keep crypto-mining operations hidden. ***The NTIC Cyber Center recommends users remain vigilant for malspam, avoid opening unexpected emails, and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. Additionally, we recommend network administrators keep all systems and software up-to-date with the latest security patches and to proactively block the IoCs provided in Unit 42's post.***

Android Malware Mandrake Went Undetected for Years

Security researchers at Bitdefender discovered Android malware, dubbed Mandrake, that has remained undetected for four years. Mandrake allows threat actors to gain complete control of an Android device and record screen activity, exfiltrate data, block calls and SMS messages, adjust the volume, pilfer credentials, transfer money, and blackmail victims. Threat actors initially deliver the malware via fraudulent apps hosted on the Google Play Store. Once downloaded, the apps act like a dropper designed to stealthily deliver additional malware onto an infected device. It believed that the threat actors behind Mandrake are financially motivated. ***The NTIC Cyber Center recommends Android users to thoroughly research apps before downloading and to 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.

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.

Snake Ransomware Publishes Patient Data

The threat actors behind the Snake ransomware campaign that targeted Fresenius Medical Care has published stolen data belonging to the healthcare organization's patients that included medical data and personally identifiable information. The stolen data was posted on an unnamed website and is considered to be a small portion of a larger leak. Information exposed in the data breach includes patients' names, dates of birth, genders, mailing addresses, phone numbers, test results, allergy data, and physicians treatment observations. Cybersecurity company Dragos states that Snake ransomware has uncommon functions that allow it stop processes associated with industrial control system (ICS) operations.

NetWalker Shifts Focus to Large Enterprise Networks

Security researchers recently discovered that the group behind NetWalker, a Ransomware-as-a-Service campaign, has begun limiting its service to hackers that have guaranteed access to large enterprise networks, offering these new potential customers 80 percent of the profit generated through successful ransomware attacks. This shift in tactics suggests that the NetWalker ransomware group is choosing "quality over quantity" when it comes to leasing its services, preferring to attract customers who can deliver guaranteed results with direct access to networks, rather than relying on those distributing phishing emails that can easily be blocked, filtered, or ignored. This also may suggest that ransomware operators are finding it increasingly difficult to successfully infect a network as organizations work to improve security protocols to prevent such attacks. Additionally, researchers at Trend Micro observed that NetWalker ransomware employs a fileless approach to infection by executing a malicious PowerShell script directly in memory,

eliminating the need for saving the ransomware binary to the hard drive. This infection vector helps the malware evade detection by security software and maintain persistence on the compromised system. For more information on how NetWalker infects a system, including IoCs, please see Trend Micro's report.

Vulnerabilities

DNS Vulnerability NXNSAttack

Cybersecurity researchers have a new vulnerability dubbed NXNSAttack that allows threat actors to conduct large-scale distributed denial-of-service (DDoS) attacks to takedown targeted websites. Threat actors leverage the vulnerability to alter the DNS delegation process, forcing DNS resolvers to generate more DNS queries to targeted authoritative servers, which could lead to a botnet-scale disruption to online services. Since the disclosure of NXNSAttack, multiple companies within the internet infrastructure domain have released patches to remediate the vulnerability. ***The NTIC Cyber Center recommends network administrators who self-managed DNS severs to update their DNS resolver software to the latest version.***

Data Breaches

An undisclosed number of Paycheck Protection Program (PPP) applicants under Bank of America (BoA) has had their data exposed in a potential data leak. BoA accidently exposed the data during a test submission to the US Small Business Administration system. Information exposed includes business addresses, tax identification numbers, Social Security numbers, phone numbers, email addresses, and citizenship statuses. BoA states that the information was exposed for a limited amount of time to some authorized vendors and has no reason to believe that the data has been misused. While the number of affected applicants remain undisclosed, BoA has offered affected customers free identity theft protection services. ***The NTIC Cyber Center recommends affected BoA customers enroll in offered identity theft protection services, routinely monitor their account statements, and immediately notify their financial institutions of any unauthorized or suspicious activity.***

Home Chef, a meal delivery service headquartered in Chicago, IL, recently confirmed a major breach potentially affecting the personal information millions of the company's customers. Compromised data includes email addresses, encrypted passwords, mailing addresses, the last four digits of payment cards, and other associated information. ***The NTIC Cyber Center recommends Home Chef users change their account passwords, enable two-factor authentication on any account that offers it, avoid reusing passwords across multiple platforms, and remain vigilant for phishing campaigns resulting from this or other data breaches.***

Wishbone, an image-sharing app for iOS and Android, was compromised exposing 40 million user records. The database containing the user records was leaked for free on a hacker forum. Information exposed includes usernames, email addresses, date of births, hashed passwords, mobile numbers, Facebook and Twitter access tokens, gender, profile images, and other metadata. It is currently unknown how the data was stolen. ***The NTIC Cyber Center recommends Wishbone users change their account passwords, enable two-factor authentication on any account that offers it, avoid reusing passwords across multiple platforms, and remain vigilant for phishing campaigns resulting from this or other data breaches.***

Upcoming Webinars

Data Breach Today®
Prevention. Response. Notification. TODAY

Zero Trust: Fast Forwarding into Working without Boundaries

With the impact of COVID-19 driving many organizations to rapidly evolve how they support remote work, IT organizations are under tremendous pressure to ensure they're managing risk effectively. Many on-premises apps are being accessed remotely for the first time, more employees

are using personal devices for work, and the policies used to secure access and route network traffic are seeing entirely new trends in telemetry.

Come join Dr. Chase Cunningham, Principal Analyst of Security and Risk at Forrester, and Alex Weinert, Director of Identity Security at Microsoft, to learn how a Zero Trust security approach secures remote access to applications with dynamic access policies, protects all the devices accessing your network, and empowers employees with simpler, more productive experiences.

To register for this free webinar on Friday, May 29 at 10:30 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.

Virtual kidnapping is a type of phone scam in which the perpetrator uses online reconnaissance and social engineering tactics to research their victims and convince them that their loved ones have been kidnapped. The perpetrator then demands a ransom payment for their safe return. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Nearly One Fifth of Law Firms Show Signs of Compromise

Analytic Comment: Based on the results of a recently conducted audit, cybersecurity firm BlueVoyant determined that 100 percent of law firms were targeted in cyber attacks during the first

quarter of 2020, suggesting that these entities are a high-value target for financially-motivated cyber threat actors. As a result, cybersecurity experts are suggesting that the legal sector should be included as one of the critical infrastructure sectors as defined by the US Department of Homeland Security, since a successful cyber attack could disrupt legal proceedings and financially devastate law firms.

Growing Threat of Destructive Attacks is One of the Top Risks Organizations Face

Analytic Comment: A recent poll conducted by Deloitte revealed that 65 percent of C-level executives within organizations view destructive cyber attacks as one of the top risks within their organizations. Ransomware attacks and data-wiping malware infections can severely debilitate and delay operations, if not completely destroy an organization's ability to continue altogether. Poor cyber hygiene among staff and insufficient asset management protocols can drastically increase the risk that an organization will fall victim to such an attack. Therefore, organizational leaders are encouraged to prioritize and regularly review cybersecurity efforts and implement procedures designed to reduce this risk.

Patches and Updates

Apple Releases Security Update for Xcode

Apple Releases Security Updates

Cisco Releases Security Updates

Drupal Releases Security Updates

Microsoft Releases Security Update for Edge

ICS-CERT Advisories

Johnson Controls Software House C-CURE 9000 and American Dynamics victor VMS

Schneider Electric EcoStruxure Operator Terminal Expert

We welcome your feedback.

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

TLP:WHITE

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

Receive this email from a friend or colleague and want to subscribe? Visit www.ncrintel.org, click on ***Subscribe*** *to Receive Our Products* at the top of the page, and enter your information.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

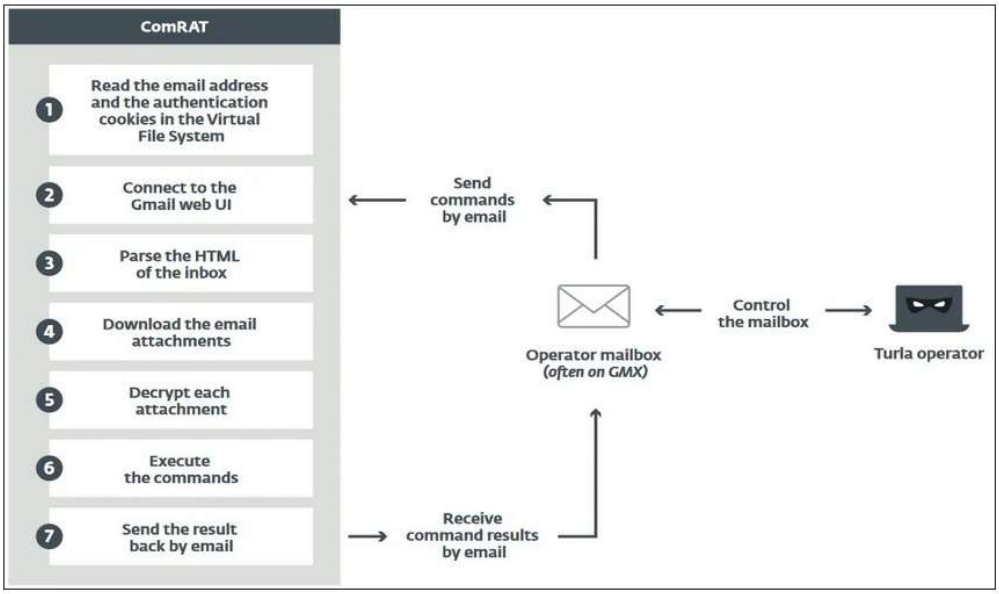
TLP:WHITE

Product No. 2020-06-006

HSEC-1 | NTIC SIN No. 2.5, 5.4

June 4, 2020

National Capital Region Cyber Threat Spotlight



Russian Cyber-Espionage Group Uses ComRAT to Target Government Organizations

Cybersecurity firm ESET recently discovered ComRAT, a new variant of malware that Turla, a state-sponsored Russian hacking group, is using to bypass network security controls and conduct cyber-espionage campaigns. ComRAT is a remote access Trojan (RAT) developed in C++ that uses the Gmail web interface to avoid detection, receive commands from attackers, and steal data from infected systems. Researchers believe that ComRAT is exclusively used by Turla to steal confidential and sensitive data from government organizations. ComRAT is installed using a PowerShell script and maintains persistence using scheduled tasks. It remains hidden by modifying the registry, encrypting and injecting processes into the system's default browser, and using ports 80 and 443 to communicate with its Gmail-based command-and-control (C2) server. ***The NTIC Cyber***

Center recommends all network administrators proactively block the associated indicators of compromise (IoCs) available in ESET's report.

Federal Partner Announcement

Hurricane-Related Scams

June 1 marks the official start of the 2020 Atlantic hurricane season. The Cybersecurity and Infrastructure Security Agency (CISA) warns users to remain on alert for malicious cyber activity targeting potential disaster victims and charitable donors following a hurricane. Fraudulent emails—often containing malicious links or attachments—are common after major natural disasters. Exercise caution in handling emails with hurricane-related subject lines, attachments, or hyperlinks. In addition, be wary of social media pleas, texts, or door-to-door solicitations relating to severe weather events.
To avoid becoming victims of malicious activity, users and administrators should review the following resources and take preventative measures.

- Staying Alert to Disaster-related Scams
- Before Giving to a Charity
- Staying Safe on Social Networking Sites
- Avoiding Social Engineering and Phishing Attacks
- Using Caution with Email Attachments

If you believe you have been a victim of cybercrime, file a complaint with the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) at www.ic3.gov.

Current and Emerging Cyber Threats

Steganography Used in Attacks against the Industrial Sector

According to cybersecurity researchers, cyber threat actors are targeting industrial sector employee credentials using malicious PowerShell scripts hidden within images. This technique is called steganography and, in this particular campaign, the threat actors use image hosting services to bypass network security detection. This campaign begins with a phishing email containing a Microsoft Office document embedded with a malicious macro designed to decrypt and execute a

PowerShell script. This script then downloads an image hosted on either Imgur or Imgbox that contains another PowerShell script payload. The second script then begins the process of collecting and exfiltrating Windows access credentials. ***The NTIC Cyber Center recommends users remain vigilant for email phishing campaigns by 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 network administrators monitor for events indicating that a Microsoft Office application launched PowerShell, restrict programs from gaining SeDebugPrivilege privileges, keep endpoint antivirus software up-to-date, and limit the use of administrator accounts.***

Valek Malware Targets Microsoft Exchange Servers

Researchers at Cybereason discovered that the malware loader known Valak has been upgraded with information-stealing capabilities targeting Microsoft Exchange servers. Valak is distributed via phishing emails that contain Microsoft Word documents embedded with a malicious macro. Once enabled, the malicious macro delivers Valek, which attempts to maintain persistence on the machine and steal sensitive data including usernames, passwords, domain passwords, and certificates. Valak has multiple variants, some of which are associated with more than 50 C2 servers. ***The NTIC Cyber Center recommends users remain vigilant for malicious email 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. We recommend all network administrators proactively block associated IoCs available in Cybereason's report.***

Octupus Scanner Malware Infects NetBeans Repositories

Security researchers discovered a new malware variant, dubbed Octopus Scanner, that leverages the GitHub web-based hosting platform to infect NetBeans repositories used in many open-source software projects. This malware identifies NetBeans project files and embeds malicious payloads in JAR binaries, project files, and dependencies to spread to downstream development systems. Once infected, the malware will begin enumerating all projects in the NetBeans directories, copying the malicious payload cache.dat to nbproject/cache.dat, and modifying the nbproject/build-impl.xml file to make sure the malicious payload is executed every time a new NetBeans project is built. At least 26 different open-source code repositories were found to be infected with information-stealing malware directly linked to this campaign that left backdoors for threat actors in all of the NetBeans project builds. ***The NTIC Cyber Center recommends all developers using NetBeans regularly audit and analyze code for errors, vulnerabilities, and unauthorized backdoors.***

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.

PonyFinal

Threat data from Microsoft Security Intelligence reveals that PonyFinal ransomware is deployed in human-operated ransomware attacks, in which threat actors use custom techniques based on prior research of targeted systems. Human-operated ransomware attack campaigns rely on active measures for their initial attack vector rather than tricking victims into clicking on executable files. In this case, threat actors likely exploited unpatched flaws, vulnerable internet-facing servers, or used brute-force attacks against a target's systems management server. Once the target system is compromised, threat actors may remain dormant, waiting for the opportune time to deploy PonyFinal, which may range from a week to multiple months. In order to mitigate human-operated ransomware, experts advise to keep systems up-to-date, audit assets for vulnerabilities and misconfigurations, adopt the principle of least privilege, and avoid using domain-wide, administrator-level service accounts.

Ragnar Locker Leverages VMs to Avoid Detection

Researchers at Sophos discovered that Ragnar Locker ransomware leverages virtual machines (VMs) to bypass security software and encrypt target machines. VMs are a simulated emulation of an operating system environment primarily used for research and development. In this instance, the threat actors leverage a Windows XP VM to run the ransomware and encrypt files on the host system. Since security software on the host machine does not typically monitor activity in the VM, the malicious activity can go undetected. The initial infection vector is currently undetermined and there is currently no publicly available decryption tool.

Ransomware Attacks Increased 40 Percent, Ransom Demands Skyrocket

Ransom demands for ransomware attacks have increased 14 times in one year due to its dominance in the cyber threat community and the increased capabilities of its operators. The cybersecurity company Group-IB reported a 40 percent increase in ransomware attacks from 2018 to 2019,

driving the ransom demands from $6,000 to $84,000. Even though intrusion techniques have not changed much since 2019, there are more than a dozen ransomware operators in the ransomware-as-a-service (RaaS) community targeting high-profile entities across the globe using Remote Desktop Protocol (RDP) exploitation to gain access to vulnerable servers.

Vulnerabilities

PageLayer WordPress Plugin

Researchers at Wordfence discovered two vulnerabilities in a plugin known as PageLayer that could be used to erase contents or compromise Wordpress sites running outdated versions of the plugin. The first vulnerability allows users with subscriber-level permissions to maliciously modify posts. The second vulnerability allows threat actors to forge requests as the site administrator to modify plugin settings that could lead to a malicious JavaScript injection. An updated version of PageLayer is available. ***The NTIC Cyber Center recommends WordPress website administrators who installed the PageLayer 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 is also recommended.***

Data Breaches

US transportation provider Amtrak recently disclosed a data breach in which customer data was compromised. Unknown threat actors were able to obtain Amtrak Guest Reward usernames and passwords and access customer data. Compromised data includes account details and unspecified personal information. Financial data, credit card data, and Social Security numbers were unaffected, according to Amtrak. While it unknown how the threat actors initially obtained Amtrak Guest Reward credentials, it is likely that they leveraged reused credentials stolen in another breach. Amtrak has initiated a password reset on affected accounts ceasing unauthorized access and is offering fraud monitoring services to compromised accounts. ***The NTIC Cyber Center recommends affected Amtrak customers change the passwords to their accounts and enroll in the free fraud monitoring program offered by the company. We also encourage the use of lengthy, complex, and***

unique passwords for each account and enabling multifactor authentication on any account that offers it to avoid falling victim to credential compromise.

Upcoming Webinars

Data Breach TODAY®
Prevention. Response. Notification.

How to Protect Employees by Running Deep SSL Inspection for Encrypted Traffic

In 2020, most new cyber attacks will come through encrypted traffic.

Currently companies, incl. midsize companies have perimeter-based security appliances. But with data and applications moving into the cloud, and the majority of employees in the network accessing corporate data and applications remotely, the question is how can UTMs protect them?

And on top of everything, internet traffic is almost 100% encrypted, adding more pain to injury - as cyber attacks will also come through this almost 100% encrypted traffic.

But legacy NGFWs don't have deep SSL inspection even for perimeter-based network security. So what can be done to protect your employees?

Join our webinar to learn and discuss:

- How midsize companies can deploy elastic network security solutions with limited resources
- How you can protect offsite/remote workers
- How you can run deep SSL inspection for encrypted traffic

To register for this free webinar on Wednesday, June 10 at 10:00 AM EDT, click here

---

Securing Our Communities

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

Business Email Compromise (BEC) – also known as a ***CEO scam*** or ***whaling*** – is a type of phishing scheme in which the perpetrator conducts online reconnaissance against a target organization and then uses various social engineering techniques to try and convince employees within that organization to divulge sensitive personal or financial information. This scheme is successful when the perpetrators can elicit an emotional response from their targets that overrides logic and any security procedures the organization already has in place. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Computer Science Student Discovers Privacy Flaws in Security and Doorbell Cameras

Analytic Comment: A researcher uncovered systemic design flaws in internet-connected security and doorbell cameras that allow unauthorized users to access video feeds. In the case where a device has shared accounts, a revoked account may still retain access to the video feeds. The option for removing active user accounts do not function as intended in many of these devices. These flaws jeopardize privacy in cases where two parties no longer reside at the same residence, such as in a divorce or in a roommate situation. Device manufacturers have placed more emphasis on convenience rather than security as complicated device authentication and access control schemes may cause customers to abandon their products. This underscores the importance of understanding and maintaining authentication and access control for purchased devices.

Patches and Updates

Apple Releases Security Updates

Cisco Releases Security Updates for CML and VIRL-PE

Cisco Releases Security Updates for NX-OS Software

Mozilla Releases Security Updates for Firefox and Firefox ESR

VMware Releases Security Updates for Multiple Products

ICS-CERT Advisories

ABB Central Licensing System

ABB Multiple System 800xA Products

ABB System 800xA

ABB System 800xA Base

GE Grid Solutions Reason RT Clocks

Inductive Automation Ignition (Update A)

Johnson Controls Kantech EntraPass

SWARCO CPU LS4000

We welcome your feedback.

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

TLP:WHITE

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

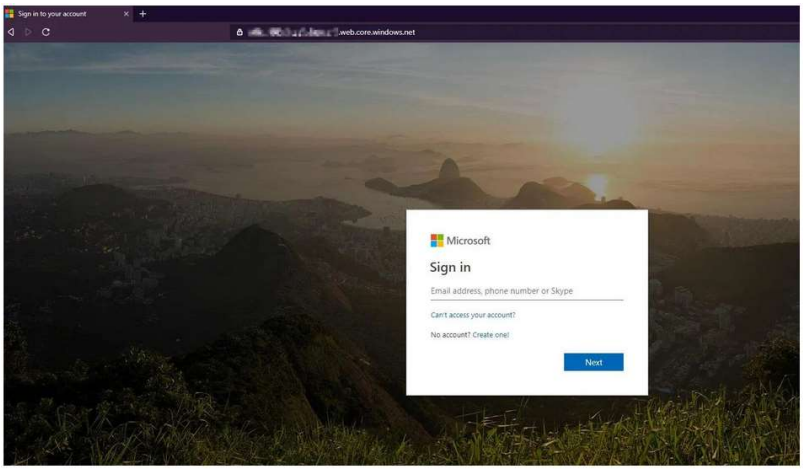
TLP:WHITE

Product No. 2020-06-017

HSEC-1 | NTIC SIN No. 2.5, 5.4

June 11, 2020

National Capital Region Cyber Threat Spotlight



Remote Workers Targeted in Office 365 Phishing Campaign Masquerading as VPN Configuration Update Requests

Security experts discovered that a new email phishing campaign is using a fraudulent virtual private network (VPN) configuration update request to target Office 365 customers and steal their login credentials. According to the email security company Abnormal Security, these phishing emails were sent to approximately 15,000 inboxes in an effort to target and exploit remote workers. The threat actors behind the campaign craft the originating email address to match the domain names of targets' organizations and attach a malicious VPN configuration message in the body of the email. This message contains a link that takes victims to a phishing page that spoofs the official Microsoft Office 365 login page. This campaign could have a high rate of success in tricking unsuspecting victims since many recipients will click through and log into their Office 365 accounts to avoid losing remote access to company servers and resources. ***The NTIC Cyber Center recommends users remain vigilant for email phishing campaigns pretending to be VPN configuration updates,***

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.

Federal Partner Announcement

Unpatched Microsoft Systems Vulnerable to CVE-2020-0796

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of publicly available and functional proof-of-concept (PoC) code that exploits CVE-2020-0796 in unpatched systems. Although Microsoft disclosed and provided updates for this vulnerability in March 2020, malicious cyber actors are targeting unpatched systems with the new PoC, according to recent open-source reports. CISA strongly recommends using a firewall to block SMB ports from the internet and to apply patches to critical- and high-severity vulnerabilities as soon as possible.

CISA also encourages users and administrators to review the following resources and apply the necessary updates or workarounds.

- Microsoft Security Guidance for CVE-2020-0796
- Microsoft Advisory ADV200005
- CERT Coordination Center's Vulnerability Note VU#872016

CISA Releases New Cyber Essentials Toolkit

As a follow-up to the November 2019 release of Cyber Essentials, the Cybersecurity and Infrastructure Security Agency (CISA) released the first in a series of six Cyber Essentials Toolkits. This is a starting point for small businesses and government agencies to understand and address cybersecurity risk as they do other risks. CISA's toolkits will provide greater detail, insight and resources on each of the Cyber Essentials' six "Essential Elements" of a Culture of Cyber Readiness. Today's launch highlights the first "Essential Element: Yourself, The Leader" and will be followed each month by a new toolkit to correspond with each of the six "Essential Elements." Toolkit 1 focuses on the role of leadership in forging a culture of cyber readiness in their organization with an emphasis on strategy and investment.

"We thank all of our partners in government and the private sector who played an essential role in the development of CISA's Cyber Essentials Toolkit," said CISA Director Christopher Krebs. "We hope this toolkit, and the ones we are developing, fills gaps and provides executives the tools they

need to raise the cybersecurity baseline of their teams and the organizations they lead."

Developed in collaboration with small businesses and state and local governments, Cyber Essentials aims to equip smaller organizations that historically have not been a part of the national dialogue on cybersecurity with basic steps and resources to improve their cybersecurity. Cyber Essentials includes two parts – guiding principles for leaders to develop a culture of security, and specific actions for leaders and their IT professionals to put that culture into action.
Each of the six Cyber Essentials includes a list of actionable items anyone can take to reduce cyber risks. These are:

- Drive cybersecurity strategy, investment, and culture;
- Develop heightened level of security awareness and vigilance;
- Protect critical assets and applications;
- Ensure only those who belong on your digital workplace have access;
- Make backups and avoid loss of info critical to operations; and
- Limit damage and restore normal operations quickly.

To learn more about the Cyber Essentials Toolkits, visit https://www.cisa.gov/cyber-essentials.

Current and Emerging Cyber Threats

Fraudulent Zoom Installation Files Deliver Devil Shadow Botnet Malware

Threat actors are leveraging fraudulent Zoom installation files to infect victims with malware. Once compromised, threat actors may remotely run processes or install the Devil Shadow botnet that is capable of downloading keyloggers, taking screenshots, and accessing webcams on infected systems. These installers originate from unofficial application marketplaces and websites that are unaffiliated with the company, Zoom. Researchers suspect that threat actors will likely attempt to distribute additional fraudulent teleconferencing apps as well. ***The NTIC Cyber Center recommends users remain vigilant for fraudulent teleconferencing applications and only download applications from trusted and official sources. If you believe your system has been compromised by this or any other campaign, notify your organization's IT security team immediately.***

Phishing Campaign Targets PBX Users

Security firm IronScales has detected an email-based phishing attack targeting companies that use private branch eXchange (PBX) telephone systems. This attack uses custom subject lines that often

include a company name or the recipient's name and spoof voicemail notification emails while appearing to originate from a PBX integration. Researchers have stated that almost 100,000 email inboxes worldwide have received these phishing emails and the threat actors behind the campaign are likely trying to obtain login credentials that would provide access to various services, personally identifiable information (PII), or business data. ***The NTIC Cyber Center recommends implementing effective email security controls and conducting regular security training for employees to help reduce risk and harden networks against email-based threats.***

Brute-Force Malware Targets Various Web Platforms

Popular web platforms are being targeted in an aggressive brute-force malware campaign designed to compromise various systems used for managing content, databases, and file transfers, as well as backup files and administrator login paths. Researchers that discovered the malware noticed that it targets cPanel and installs a free Alternate Lite WordPress theme replacing a "cutomizer.php" script with a file upload script that allows getting files via POST request or URL. Once all files are ready, the malware contacts a command and control (C2) server to receive a list of targets and login credentials. Threat actors use this data to analyze targets' personal identifiers, generating a word list that will be used in brute-force attacks while using multiple devices to bypass the web platforms' security protocols. ***The NTIC Cyber Center recommends using lengthy, complex, and unique credentials, and regularly monitoring web platforms for unauthorized user accounts and access.***

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.

Maze Ransomware Targets US Nuclear Missile Contractor

Multiple open source reports indicate that Westech International, a US military contractor providing support for the US Minuteman III intercontinental ballistic missile program, was recently victimized in a Maze ransomware attack. According to a Sky News report, the Maze ransomware operators gained access to Westech International's network, exfiltrated data, and then deployed their encryption scheme across the network. To pressure the company into paying the ransom, the Maze

operators began to leak some of the stolen data online, including company emails, payroll information, and other sensitive employee data. Westech International has hired a computer forensic firm to investigate the incident and currently, the attack vector, remediation process, and whether or not classified information was stolen is unknown. This incident underscores the importance of employing a defense-in-depth strategy to cybersecurity, ensuring that networks and sensitive data are properly secured using a variety of controls and methods, to reduce the risk of becoming victimized in a cyber attack.

Zorab Ransomware Campaign Double-Encrypts Files

Threat actors are using fraudulent decryption tools to distribute additional ransomware to systems previously compromised by ransomware, resulting in the double-encryption of files. In this case, threat actors are distributing fraudulent decryption tools claiming to be for the STOP Djvu ransomware variant, but instead encrypts the victim's already encrypted data with Zorab ransomware. Zorab appends .ZRB to affected file names and drops a ransom note with the file name *--DECRYPT--ZORAB.txt.ZRB* on infected systems. It is recommended that ransomware victims only use free ransomware decryption tools provided by NoMoreRansom.org if they are unable to restore their data from backups. For more information, including associated indicators of compromise (IoCs), please review BleepingComputer's article.

eCh0raix Ransomware Targets QNAP NAS Devices

The threat actors behind the eCh0raix ransomware variant have launched a campaign targeting QNAP network attached storage (NAS) devices. Threat actors compromise QNAP devices via vulnerabilities or by brute-forcing device passwords. Once compromised, threat actors inject malicious code or perform remote code execution and drop a ransom note with the file name *README_FOR_DECRYPT.txt* on affected devices. There is currently no free decryption tool available; however, users who have enabled QNAP's Snapshot backup service can recover their files. More information about eCh0raix ransomware is available on Bleeping Computer's website. Administrators of QNAP NAS devices are encouraged to review this security advisory and apply the appropriate firmware updates to patch against these vulnerabilities as soon as possible.

Avvadon Ransomware Lures Victims into Opening a Malicious Photo

A newly discovered ransomware variant, Avaddon, is being delivered via a massive phishing campaign targeting victims across the globe. The phishing campaign attempts to lure recipients into opening an attached ZIP file by suggesting that the file contains a photo of the recipient or the sender. In reality, however, the file contains a JavaScript file masquerading as a JPG image file that, if opened, launches a PowerShell and Bitsadmin command, triggering the download and execution

of the ransomware. Avaddon appends .avdn to the names of encrypted files and drops a ransom note named *[id]-readme.html* into each affected folder. The ransom note contains instructions on how to pay the ransom and a countdown timer that threatens to double the extortion fee if the payment is not sent within a specified period of time. Security researchers who examined a sample of the executable determined that it is unlikely that a free decryption tool could be created for this variant.

Vulnerabilities

VMware Cloud Director

Researchers at Citadelo discovered a code injection vulnerability in VMware Cloud Director versions 10.1.0 and older that allows threat actors to compromise and control private cloud infrastructures. Authenticated threat actors can leverage the HTML and Flex user interfaces or API calls to push malicious traffic to the system, which could lead to a full takeover of the cloud infrastructure. In affected versions of VMware Cloud Director, threat actors can compromise and control systems without revealing their identities. The vulnerability has since been patched. ***The NTIC Cyber Center recommends administrators of VMware Cloud Director to update to the latest version as soon as possible.***

Data Breaches and Leaks

Threat actors are publicly sharing a database containing over 26 million unique LiveJournal user accounts on several hacker forums. Compromised data includes email addresses, usernames, profile URLs, and plain text passwords. While LiveJournal has not confirmed the legitimacy of the database or an associated breach, cybersecurity website BleepingComputer stated that credentials from the LiveJournal database were reused in another attack. ***The NTIC Cyber Center recommends LiveJournal users change the passwords to their accounts and delete accounts that are no longer used or needed. We also encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication on any account that offers it to avoid falling victim to credential compromise.***

CyberNews discovered a breach of student loan information belonging to a collective of student loan debt relief providers known as the Student Advocates Group (SAG). Information exposed includes names, addresses, dates of birth, phone numbers, Social Security numbers, tax ID numbers, credit card numbers, banking data, PIN numbers, occupation information, and contact information sourced from 25,000 PDFs and more than 55,000 call recordings. The breach is attributed to improperly secured Amazon Web Services (AWS) S3 buckets, leaving them publicly exposed for anyone to access. The AWS buckets have since been secured. ***The NTIC Cyber Center recommends SAG 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 SAG customers monitor associated payment accounts and report any suspicious and unauthorized activity to their financial institutions. Those affected may want to consider placing a fraud alert or security freeze on their credit file with Equifax, Experian, or TransUnion.***

Upcoming Webinars

Data Breach®
Prevention. Response. Notification. TODAY

Hackers Have First-Move Advantage - How Can We Rapidly Equip Cyber Ready Humans to Respond?

An attacker's first-move advantage clearly comes down to their rapid innovations, meaning security teams always have to operate reactively. Like forest fires, cyber-attacks are devastating and unpredictable; and like firemen, defenders can only race to the scene. But by the time they arrive, the damage is usually done.

All cyber-skilled individuals, good and bad, have the same qualities: they learn fast, they persevere, and they dare to tread boundaries. But most of all, they want to innovate.

The problem when upskilling the good guys has always been this: how do we keep them at the cutting edge of cybersecurity while staying legal? We want defenders to innovate as rapidly as the criminals.

Register for this upcoming live webinar and learn:

- How human readiness can be mapped to the risks that organizations face;
- The advantages of skills content that incorporates real threat intelligence, real tools and real techniques;

- The importance of a "security-first" approach to upskilling teams across many roles, including, IT, DevOps, project management and more.

To register for this free webinar on Tuesday, June 16 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.

Celebrity scams **–** also known as ***imposter scams***, ***impersonation scams***, and ***fan scams*** **–** are a type of social engineering scheme in which the perpetrator masquerades as a celebrity or popular social media personality, concealing his or her true intentions to elicit money or personal information or to trick the victim into clicking on malicious links. These scammers create convincing yet fraudulent profiles on social media platforms using images of famous personalities to attract likes, clicks, and retweets from unsuspecting fans. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

Chinese and Iranian Hackers Targeted Biden and Trump Campaigns, Google Says
Analytic Comment: The head of Google's Threat Analysis Group stated that state-backed hackers are actively targeting US politicians. Chinese hackers have targeted Joe Biden's campaign staffers and Iranian hackers have targeted Donald Trump's campaign staffers. While these hacking attempts have been unsuccessful so far, the threat of foreign influence and espionage affecting the presidential election remains a risk and it is imperative that politicians, staffers, and associates

maintain awareness of these and other cyber threats.

Researchers Say OmniBallot Online Voting Platform Is Vulnerable to Manipulation

Analytic Comment: The online voting platform, OmniBallot, is vulnerable to hacking according to researchers from the University of Michigan and the Massachusetts Institute of Technology. Threat actors, including insider threats, could install malware onto the voting device to manipulate votes. While OmniBallot has been used before in select states and in limited circumstances, 2020 will be the first year that the platform will feature an online ballot return option. This underscores the importance of proper security standards, audits, physical receipts, and government collaboration as cyber threat actors attempt to undermine the US election process.

Patches and Updates

Adobe Releases Security Updates

Cisco Releases Security Updates for Multiple Products

Google Releases Security Updates for Chrome

Microsoft Releases June 2020 Security Updates

VMware Releases Security Update for Horizon Client for Windows

---

ICS-CERT Advisories

Advantech WebAccess Node

Mitsubishi Electric MELSEC iQ-R series

OSIsoft PI System (Update A)

Philips PageWriter TC10, TC20, TC30, TC50, and TC70 Cardiographs (Update A)

Siemens Industrial Products (Update G)

Siemens LOGO!

Siemens SIMATIC, SIMOCODE, SINAMICS, SITOP, and TIM (Update H)

Siemens SIMATIC, SINAMICS

Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK

Siemens SINUMERIK

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

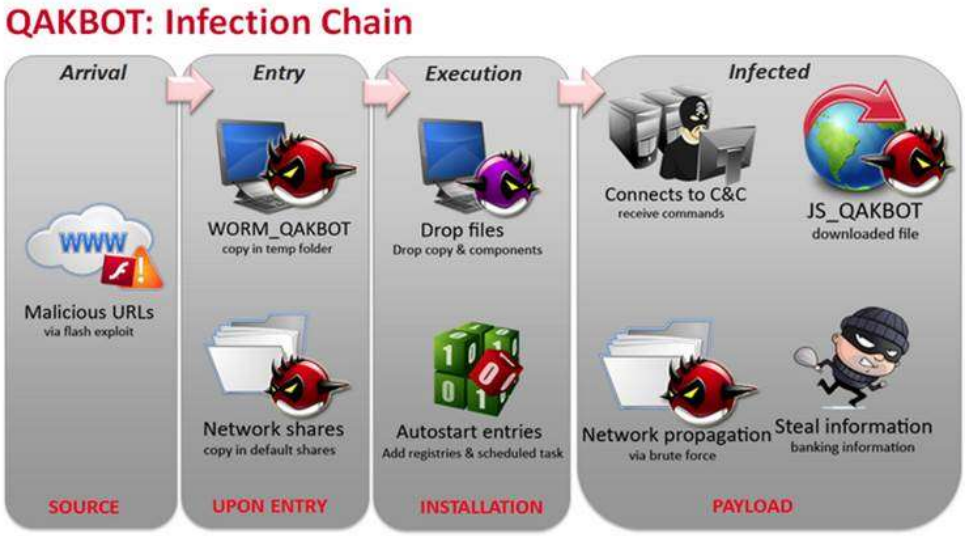
TLP:WHITE

Product No. 2020-06-027

HSEC-1 | NTIC SIN No. 2.5, 5.4

June 18, 2020

National Capital Region Cyber Threat Spotlight



Qbot/Qakbot Campaign Targets US Bank Customers

Researchers at F5 Labs have observed attacks leveraging Qbot malware to pilfer credentials associated with approximately 46 different US financial institutions. Qbot, also known as QakBot, Quakbot and Pinkslipbot, is a banking Trojan used to steal victims' financial data and can log keystrokes, steal cookies, create backdoors, and inject additional malware onto an infected system. Threat actors are typically spreading Qbot using browser hijacks or web redirections. Newer versions of Qbot have been upgraded to resist forensic examination and evade detection as they employ anti-virtual machine techniques and hide their malicious code from scanners and signature-based tools. Once compromised, Qbot will spy on the victim's web browsing habits and will pilfer credentials from specific financial services when accessed. Qbot maintains persistence by embedding itself into the *%APPDATA%* folder and generating a new registry value so that it can execute when the system reboots. ***The NTIC Cyber Center recommends users keep software and***

operating systems up-to-date and 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 the Qbot Trojan, notify your organization's IT security team immediately.

Federal Partner Announcement

Increased Use of Mobile Banking Apps Could Lead to Exploitation

As the public increases its use of mobile banking apps, partially due to increased time at home, the FBI anticipates cyber actors will exploit these platforms.

Americans are increasingly using their mobile devices to conduct banking activities such as cashing checks and transferring funds. US financial technology providers estimate more than 75 percent of Americans used mobile banking in some form in 2019.

Studies of US financial data indicate a 50 percent surge in mobile banking since the beginning of 2020. Additionally, studies indicate 36 percent of Americans plan to use mobile tools to conduct banking activities, and 20 percent plan to visit branch locations less often. With city, state, and local governments urging or mandating social distancing, Americans have become more willing to use mobile banking as an alternative to physically visiting branch locations. The FBI expects cyber actors to attempt to exploit new mobile banking customers using a variety of techniques, including app-based banking Trojans and fake banking apps.

To read more about this threat, along with recommendations to protect yourself and your organization, please review the FBI's Public Service Announcement here.

CISA Releases Disinformation Toolkit

As the nation and the world continues to fight against COVID-19, the Cybersecurity and Infrastructure Security Agency (CISA) continues to work on products and resources intended to help improve resilience and minimize related risk associated with the pandemic.

Yesterday, CISA released a Disinformation Toolkit to help state, local, tribal and territorial (SLTTs) officials bring awareness to misinformation, disinformation, and conspiracy theories related to COVID-19. The Toolkit includes talking points, frequently asked questions, and flyers, and provides simple steps individuals can take to combat false or misleading information related to the pandemic.

We encourage you to share this publication with state and local government officials who might be able to use it.

For authoritative information and resources on COVID-19, visit the CDC's website and CISA.gov/coronavirus.

Current and Emerging Cyber Threats

Phishing Campaign Exploits Black Lives Matter Movement to Deliver Trickbot

Researchers have uncovered a phishing campaign that delivers Trickbot malware embedded in emails masquerading as Black Lives Matter (BLM) voting correspondence. Trickbot is a modular information-stealing Trojan and, in this campaign, threat actors send emails requesting that recipients vote anonymously about BLM with 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 Trickbot onto the victim's system. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns disguised as BLM 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.***

MageCart Payment Skimmer Discovered on Greenworks Tools Website

RapidSpike researchers discovered a MageCart script, also known as a payment card skimmer, on Greenworks hardware tools website, targeting site visitors' payment data. Threat actors compromised the site with malicious code that enables the theft of card data (number, CVV, expiration date), account credentials (usernames and passwords) and personal information (phone