NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-08-027

HSEC-1 | NTIC SIN No. 2.5, 5.4

August 20, 2020

National Capital Region Cyber Threat Spotlight

Emotet Targets US Businesses Using COVID-19 Themed Phishing Campaigns

Emotet malware threat actors have been exploiting the uncertainty surrounding the COVID-19 pandemic by targeting US businesses with COVID-19 themed phishing campaigns. Security researchers at Fate112 recovered a stolen email that had been being used in a phishing attack in which threat actors were pretending to be from the 'California Fire Mechanics' and were sending pandemic-related updates. Within the email is a malicious attachment titled 'EG-8777 Medical report COVID-19[.]doc' that claims to be created from an iOS device and requires the unsuspected victim to enable macros to view it properly. Once the malicious macros are enabled, Emotet will begin to download and install other malware such as Qbot or TrickBot, turning the victim's computer into a malware bot designed to send malicious email to other unsuspecting recipients. ***The NTIC Cyber Center recommends users remain vigilant for this and other Emotet email campaigns, avoid opening and unexpected emails, and refrain from clicking on links or opening attachments from unknown or untrusted sources. If you believe you have been infected with Emotet, notify your organization's IT security team immediately so they may contain and remediate the infection.***

Federal Partner Announcements

Phishing Emails Used to Deploy KONNI Malware

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

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

North Korean Malicious Cyber Activity

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

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

Current and Emerging Cyber Threats

New Crypto-Mining Worm Steals AWS Credentials

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

Security's report.

Drovorub Malware Targets Linux

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

PurpleWave Data-Stealing Malware Discovered

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

Vulnerabilities

Thales Cinterion EHS8 M2M Modules

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

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

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our website.

Carnival Corporation Suffers Ransomware Attack

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

Data Leaks and Breaches

350 Million Email Addresses Exposed on Unsecured AWS Server

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

Securing Our Communities

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

Rental scams are a type of social engineering scheme in which perpetrators advertise fake apartment, condominium, home, or vacation rental listings with the intent of defrauding those seeking to lease such properties. These scams frequently target students, prospective residents, and tourists interested in renting short-term or long-term stay properties listed on sites such as Craigslist, AirBnB, VRBO, and others. Rental scams are particularly prevalent during busy summer months when moving and vacation seasons peak and in markets where rental properties are in high demand. Click here to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

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

Patches and Updates

Google Releases Security Updates for Chrome

ICS-CERT Advisories

Schneider Electric APC Easy UPS On-Line

Siemens Automation License Manager

Siemens Desigo CC

Siemens Opcenter Execution Core (Update A)

Siemens SCALANCE, RUGGEDCOM

Siemens SICAM A8000 RTUs

Siemens SIMATIC, SIMOTICS

Siemens UMC Stack (Update A)

Tridium Niagara

Yokogawa CENTUM

We welcome your feedback.

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

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

TLP:WHITE

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.