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 though 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. Nefilim 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 extortion 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.*

![Neighbor number scam](image)

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)
OSIssoft 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.

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.