Cyber Threat Investigations & Expert Services (CTIX) FLASH Wrap-Up

March 2023

ankura | PROTECT, CREATE, RECOVER VALUE

CONTENTS

Executive Summary

The Ankura Cyber Threat Investigations and Expert Services (CTIX) FLASH Wrap-Up is a collection of high-level cyber intelligence summaries pertaining to current or emerging cyber events in March 2023, originally published in CTIX FLASH Updates throughout March. This publication includes malware threats, threat actor activity, and newly identified vulnerabilities impacting a wide range of industries and victims. The CTIX FLASH Update is a semi-weekly newsletter that provides a timely snapshot of cyber events, geared toward cyber professionals and end users with varying levels of technical knowledge. The events published in the FLASH typically occurred close in time to publication of the report.

To stay up to date on the latest cyber threat activity, sign up for our weekly newsletter: the Ankura CTIX FLASH Update.

MALWARE ACTIVITY

New "MQsTTang" Backdoor Identified and Attributed to Mustang Panda

Reported in the March 3rd, 2023, FLASH Update

- "MQsTTang", a new custom backdoor, has been discovered and attributed to the Chinese advanced persistence threat (APT) group Mustang Panda. Researchers observed this malware in an ongoing social engineering campaign that likely began in January 2023 and appears to be targeting government and political organizations in Europe, Asia, and Australia. Researchers noted that the malware "doesn't seem to be based on existing families or publicly available projects" and does not follow the group's usual tactics. The initial attack vector is believed to be through spearphishing. MQsTTang is being distributed through RAR archives, which contain single executables that are commonly named as phrases related to passports or diplomacy. MQsTTang uses the MQTT protocol for its command-and-control (C2) communication, which is not a technique typically used amongst publicly documented malware families. Researchers explained that the MQTT protocol is commonly used for communication between Internet of Things (IoT) devices and controllers, but a benefit to using it in malware is the protocol's ability to hide the malware's infrastructure behind a broker, ensuring that the victim machine does not communicate directly with the C2 server. This is executed through using the open-source QMQTT library, which depends on the Qt framework. A large portion of the framework is "statically linked in the malware" and used for malware development, which is another unusual tactic. Researchers are urged to closely monitor Mustang Panda's development as they delve into tactic, techniques, and procedures (TTPs) rarely observed in their arsenal. Additional technical details of MQsTTang and Mustang Panda as well as indicators of compromise (IOCs) can be viewed in the report linked below.

    - The Hacker News: MQsTTang Campaign Article
    - ESET: MQsTTang Campaign Report

ALPHV Extorting Healthcare Network with Clinical Images of Breast Cancer Patients

Reported in the March 7th, 2023, FLASH Update

- On February 20, 2023, Lehigh Valley Health Network (LVHN), a healthcare network based in Pennsylvania, disclosed that it had suffered a cyberattack by ALPHV. ALPHV (also known as BlackCat) is a Russia-linked ransomware group that typically targets healthcare and academic organizations and continues to be very active this year. LVNH noted that the attack involved "patient images for radiation oncology treatment and other sensitive information on a single physician practice in Lackawanna County" and that the network would not be paying the demanded ransom. In response to this payment denial, ALPHV has begun attempting to extort LVNH by publishing exfiltrated data and clinical images of breast cancer patients to their leak site, describing the images as nudity. Alongside this data, ALPHV stated, "Our blog is followed by a lot of world media, the case will be widely publicized and will cause significant damage to your business. Your time is running out. We are ready to unleash our full power on you!" Security researchers are outraged at this level of extortion and the threat group attempting to capitalize on the sensitivities surrounding cancer treatment. CTIX analysts will continue to monitor this ongoing situation and will provide updates as they become available.

    - The Record: Lehigh Valley Health Network Article
    - Lehigh Valley Live: LVHN Cyberattack Article

IceFire Ransomware Exploits File Sharing Software to Attack Linux-Powered Enterprise Networks

Reported in the March 10th, 2023, FLASH Update

- The IceFire ransomware, previously associated with the "ifire" file extension that targeted Windows servers, has been altered to a novel version that executes on Linux systems of enterprise networks. Media and entertainment companies in Turkey, Iran, Pakistan, and the United Arab Emirates have been the primary victims. IceFire exploits CVE-2022-47986, a deserialization vulnerability in the IBM Aspera Faspex file sharing software. The ransomware encrypts files and evades detection by deleting itself after executing; but most importantly, it allows certain paths that are critical for the functionality of the server to stay unencrypted, avoiding disruptions, damages, or shutdowns. Moving from Windows-based ransomware to targeting Linux networks is a tactic consistent with other prominent ransomware groups involved in big-game hunting (BGH), part of which focuses on targeting enterprises. This increasing use of ransomware groups using Linux encryptors likely correlates to the recent surge of enterprises transitioning to VMware ESXi virtual machines or similar Linux-managed infrastructure. CTIX analysts will continue to monitor this campaign and will provide updates as they become available.

    - The Hacker News: IceFire Article
    - Bleeping Computer: IceFire Article
    - Sentinel One: IceFire Report

New "GoBruteforcer" Malware Targets Web Servers in Brute-Force Attacks

Reported in the March 14th, 2023, FLASH Update

- "GoBruteforcer", a newly discovered Golang malware, has been observed being hosted on a legitimate website and targeting web servers specifically running Postgres, phpMyAdmin, MySQL, and FTP. Researchers detailed that the malware operators utilize a Classless Inter-Domain Routing (CIDR) block during their attack to scan the network and target all IP addresses found within the CIDR range. This method is used to target a wide array of hosts on various IP addresses as opposed to a single IP address. GoBruteforcer singles out Unix-like devices running specific architectures and attempts to obtain access through brute-force attacks using hard-coded credentials contained in the binary. The goal of this malware is to gather the devices into a botnet, which uses an internet relay chat (IRC) bot on the victim device for command-and-control (C2) communications. Researchers emphasized that GoBruteforcer is currently in active development, and it is likely that its tactics, techniques, and procedures (TTPs) will advance in the future. It is recommended that administrators ensure that their infrastructure, especially web servers in this instance, have strong passwords to combat against brute-force attacks. Additional technical details as well as indicators of compromise (IOCs) can be viewed in the report linked below.

    - The Hacker News: GoBruteforcer Article
    - Unit 42: GoBruteforcer Report

Actors Observed Abusing Adobe Acrobat Sign Service to Spread "Redline" Malware

Reported in the March 17th, 2023, FLASH Update

- Researchers have recently observed actors taking advantage of the legitimate e-signature service Adobe Acrobat Sign to distribute info-stealing malware. The campaign operators register for the service and send targeted emails containing documents hosted on Adobe's servers. The emails involve a real Adobe email address and legitimate Adobe URL to trick users into opening the shared documents and clicking a link contained in the documents' text. The link redirects users to a different website that prompts for a hard coded CAPTCHA to be entered. Once the CAPTCHA is completed, the users are prompted to download a malicious ZIP file that contains one (1) of two (2) possible "Redline" trojan variants, which have capabilities to exfiltrate passwords, cryptocurrency wallets, and more from a victim device. Researchers noted that the campaign operators "artificially increased the size of the Trojan to more than 400MB", which is suspected to be due to bypassing antivirus engines that behave differently for large files. Currently, it appears this technique is targeted to a specific victim, but there is a chance that it could be picked up by additional actors and see more widespread usage in the future. CTIX analysts recommend users to be cautious of all files they are emailed and ensure their legitimacy prior to interacting.

- ○ Bleeping Computer: Adobe Acrobat Sign Article
- ○ Avast: Adobe Acrobat Sign Report

General Bytes Discloses Security Incident and $1.5 Million Bitcoin Theft

Reported in the March 21st, 2023, FLASH Update

- General Bytes, a large cryptocurrency Automatic Teller Machine (ATM) manufacturer, disclosed on March 18, 2023, through Twitter that it suffered a "security incident" that resulted in the shutdown of various United States-based ATMs and the theft of approximately $1.5 million worth of bitcoin. General Bytes has approximately 15,000 ATMs located in over 149 countries around the globe, and a portion of the kiosks are "two-way", meaning that customers can exchange cash-for-crypto as well as crypto-for-cash. Karel Kyovsky, the founder of General Bytes, detailed in a statement released on March 19 that the security incident occurred from March 17 to March 18 and that the actor responsible "was able to upload his own java application remotely via the master service interface used by terminals to upload videos and run it using batm user privileges." This was made possible by exploiting a zero-day vulnerability tracked as BATM-4780. Kyovsky also detailed that the actor "scanned the Digital Ocean cloud hosting IP address space and identified running CAS services on ports 7741, including the General Bytes Cloud service and other GB ATM operators running their servers on Digital Ocean." After gaining initial access, the actors were able to access the database, read and decrypt API keys used to access funds in exchanges and hot wallets, send funds from hot wallets, exfiltrate usernames and password hashes, disable two-factor authentication, and access terminal event logs to scan for instances where customers scanned private keys at the ATMs. Technical mitigation details as well as indicators of compromise (IOCs) can be viewed in General Bytes' statement linked below.

  - ○ The Record: General Bytes Security Incident Article
  - ○ Bleeping Computer: General Bytes Security Incident Article
  - ○ General Bytes: Initial Tweet & Security Incident Statement

Information-Stealer "BlackGuard" Variant Observed with Advanced Capabilities

Reported in the March 24th, 2023, FLASH Update

- Researchers have identified a new variant of "BlackGuard", an information-stealing malware first discovered in March 2022 being sold as malware-as-a-service (MaaS) in Russian-speaking forums. BlackGuard is known for its attempts at exfiltrating "cookies and credentials stored in web browsers, cryptocurrency wallet browser extension data, desktop crypto wallet data, information from messaging and gaming apps., email clients, and FTP or VPN tools." The active malware is constantly evolving, and the new variant has updated, advanced features. The malware now has the ability to propagate through removable devices, such as USBs, and automatically infect new machines. The BlackGuard variant can also establish persistence between system reboots by adding itself under the "Run" registry key as well as copying malware files with random names to every folder within the C: drive. Researchers explained that this capability may be to increase the difficulty of removing the malware, but also noted that it could just be for annoyance. The malware can also download additional payloads from the command-and-control (C2) server and "execute them directly in the breached computer's memory using the 'process hallowing' method" in order to bypass antivirus detection. Another new feature is a crypto wallet clipper module that replaces crypto addresses copied to the Windows clipboard with the operator's address. Additionally, BlackGuard has broadened its target scope to include fifty-seven (57) crypto browser extensions and wallets to attempt to exfiltrate the data and crypto assets. Additional technical details and indicators of compromise (IOCs) can be viewed in the report linked below.

- Bleeping Computer: BlackGuard Stealer Article
- AT&T: BlackGuard Stealer Report

New Phishing Campaign Impersonating IRS to Distribute the "Emotet" Malware

Reported in the March 28th, 2023, FLASH Update

- Researchers have identified a new phishing campaign impersonating the Internal Revenue Service (IRS) to send fraudulent W-9 tax forms that contain the "Emotet" malware. Emotet is known to be historically distributed through malicious Microsoft Word and Excel documents in a variety of themed phishing campaigns, typically coinciding with holidays or business activities done at specific times of the year. However, the malware operators have recently begun to change their distribution method to Microsoft OneNote containing embedded scripts following the blocking of macros by default in Office documents. In this latest campaign, the malware operators are using an "IRS Tax Forms W-9" theme and specified that the sender of the phishing emails was an "inspector" from the IRS. Attached to the emails is a ZIP archive titled "W-9 form.zip" that contains a malicious Word document that is over 500 megabytes (MB) in size in order to bypass antivirus engines that behave differently for large files. Additional researchers observed another phishing campaign capitalizing on the tax season lure to impersonate business partners of the recipients. The operators of this campaign have been utilizing OneNote attachments that, once opened, pretend to be protected and prompt the victim into clicking a "view" button that results in the execution of VBScript code. Once launched, Emotet is downloaded and executed. Additional details of the latest Emotet phishing campaign can be viewed in the report linked below.
  - Bleeping Computer: IRS Phishing Campaign Article
  - Malwarebytes: IRS Phishing Campaign Report

3CX Confirms Embedded Malware in Desktop Applications, Impacting Thousands of Companies

Reported in the March 31st, 2023, FLASH Update

- 3CX, an enterprise communications software solutions manufacturer, has confirmed that various versions of its desktop application for Windows and macOS are affected by an active supply-chain attack, potentially impacting thousands of companies. 3CX has a client base of approximately 600,000 companies and the impacted versions currently include 18.12.407 and 18.12.416 for

Windows as well as 18.11.1213, 18.12.402, 18.12.407, and 18.12.416 for macOS. Nick Galea, 3CX's founder and chief executive, confirmed that the desktop application is embedded with malware and Pierre Jourdan, 3CX's chief information security officer, detailed that the attack "appears to have been a targeted attack from an Advanced Persistent Threat, perhaps even state sponsored, that ran a complex supply chain attack and picked who would be downloading the next stages of their malware." Various cybersecurity companies have published reports on the attack, and some researchers have noted code that "exactly matches" malware historically identified in attacks by the notorious North Korean threat actor Lazarus Group (while CrowdStrike specifically cites a sub-cluster known as Labyrinth Chollima). This situation has the potential for further damage, such as mass attacks, including widespread exfiltration of data. It should also be noted that any money generated from this ongoing supply-chain attack has the potential to be funding the North Korean government. 3CX users are urged to update their self-hosted and on-premises versions of the software to version 18.12.422 to mitigate the risk of exploitation. CTIX analysts will continue to monitor the repercussions of the 3CX compromise and report all updates as they become available. Additional technical information of this attack as well as indicators of compromise (IOCs) can be reviewed in the reports linked below.

- The Record: 3CX Supply-Chain Attack Initial Article & Updated Article
- The Hacker News: 3CX Supply-Chain Attack Article
- 3CX: Nick Galea's Statement & Pierre Jourdan's Statement
- Reports: SentinelOne, Sophos, & CrowdStrike

THREAT ACTOR ACTIVITY

Blackfly (APT41) Expands Toolset, Targets Asia

Reported in the March 3rd, 2023, FLASH Update

- Threat actors from the Blackfly organization have begun targeting entities throughout Asia in a new cyberespionage campaign. The group, commonly tracked as APT41, is a state-sponsored espionage group backed by the Chinese government. These actors have been conducting malicious activity since 2010, often times compromising assets to gain intelligence benefiting China's geopolitical policies. Earlier Blackfly attacks targeted the gaming industry but over time expanded to targeting a wide umbrella of entities throughout the telecommunications, manufacturing, medical, hospitality, natural resources, and food industries. Recently, the threat actors conducted attacks against Asian materials and composites entities, including two (2) subsidiaries of an Asian conglomerate believed to be in search of intellectual property to exfiltrate. Blackfly has incorporated a variety of malicious programs into their attacks since the latter half of 2022, including variants of the “Winnkit” backdoor, Mimikatz credential dumping, ForkPlayground memory dump, and a basket full of proxy configurations. Despite a significant setback in 2020 after multiple group members were arrested, Blackfly continues to operate with motivation for carrying out cyberespionage operations and is likely to do so in the coming future.

    ○ Symantec: Blackfly Article

Threat Actors Romance Android Users, Install Espionage Malware

Reported in the March 7th, 2023, FLASH Update

- Transparent Tribe actors have unveiled a new campaign targeting Android users throughout India and Pakistan. Historically, Transparent Tribe (APT36) is known for their continuous cyberespionage attacks against research, defense, and diplomatic organizations in Afghanistan and India for nearly a decade. This new campaign has set sights on Indian and Pakistani Android users who are involved with military or political operations in the region. Users are contacted on common messaging platforms and are lured via romance scams to download and install another messaging platform laced with malicious software. Transparent Tribe actors embedded malicious code into the applications (MeetsApp and MeetUp) to install the “CapraRAT” backdoor, one (1) of their more commonly used malwares in previous campaigns. Once installed, CapraRAT has the capabilities to exfiltrate sensitive information, make phone calls, record phone call audio, capture screenshots, and send SMS text messages. Communications from both malicious applications relay back to the same command-and-control (C2) server and contain the same digital certificates. Personal identifiable information (PII) of around 150 victims were obtained and analyzed by researchers due to weak security by the threat actors. CTIX continues to monitor threat actor activity worldwide and will provide additional updates accordingly.

    ○ WeLiveSecurity: Transparent Tribe Article

TA499 Targets North American and European Officials with New Phishing Techniques

Reported in the March 10th, 2023, FLASH Update

- A malicious email campaign has struck high-profile individuals throughout Europe and North America, primarily those who have given financial support to Ukraine and their allies. The threat actors responsible are with the Russia-aligned TA499 organization, otherwise referred to as Lexus or Vovan. Active since 2021, TA499 has focused on exploiting those against the Russian state, especially once the Ukraine/Russia conflict began last year. Targets of the group often include top-level officials and high-profile individuals from around the globe such as Mayors, CEOs, and celebrities. This new campaign homes in on North American and European users, masking email/phone communications from threat actors pretending to be political figures such as Ukrainian Prime Minister Denys Shmyhal. However, this campaign is slightly different than the typical phishing operation conducted by other threat groups. In this instance, threat actors will distribute phishing emails containing no malware, and instead ask to set up a phone/video conference call to discuss current Russia/Ukraine tensions. These conversations often include video conferencing where TA499 actors would physically impersonate Ukrainian officials through deepfake AI technology. The actors will then save the recordings and post them on YouTube/RUTUBE and use them for Russian propaganda. While no malicious software was deployed on victim systems, users were taken advantage of and defamed because of these threat actors. CTIX analysts continue to monitor threat actor activity worldwide and will provide additional updates accordingly.

  - Proofpoint: TA499 Article
  - Cyware: TA499 Article

UNC2970 Target Security Researchers of Western Tech Companies

Reported in the March 14th, 2023, FLASH Update

- North Korean threat actors operating on behalf of the UNC2970 threat group have been conducting malicious espionage activity against western media and technology corporations since June 2022. The group shows strong attribution back to the UNC577 threat group, which has conducted numerous malicious campaigns since their emergence in 2013. In this new campaign, UNC2970 actors utilize social platforms such as LinkedIn to pose as job recruiters and begin conversing with individuals, primarily security researchers. As the conversation persists, threat actors insist on shifting communications to WhatsApp where the malicious activities would begin. After some time, the threat actor will send the user a job description via a Microsoft Word document, which is laced with macro-malware and performs a remote-template injection. Once injected, the macro-code will begin downloading malicious payloads from actor-controlled command-and-control (C2) nodes, including the trojanized variant of TightVNC dubbed “LIDSHIFT”. This trojan will gather information from the user's system, such as the device name, product name, IP address, current process list, and will relay that information back to threat actor C2 servers. In addition to LIDSHIFT, UNC2970 actors have also been known to deploy additional malware such as “PLANKWALK”, “LIDSHOT”, “CLOUDBURST”, “TOUCHSHIFT”, “SIDESHOW”, “TOUCHKEY”, “TOUCHSHOT”, and “HOOKSHOT”. Detailed indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs), and malicious code are available for review in the below linked report.

  - Mandiant: UNC2970 Article

Threat Profile: Winter Vivern

Reported in the March 17th, 2023, FLASH Update

- Threat actors from the Russia-aligned Winter Vivern APT group have been conducting global cyberespionage campaigns against those who support and aid Ukraine. Winter Vivern, named after a command-and-control (C2) node URL string, was brought to light in early 2021 and has since been an underreported group. These actors attempt to stay out of the limelight as much as possible; however, this recent campaign has brought attention back to the group. Historically, the group has targeted numerous government organizations throughout India, Lithuania, Slovakia, and Vatican with espionage-related cyberattacks. Recent activity from Winter Vivern involved targeting the Ukraine & Italy Ministry of Foreign Affairs, Polish government agencies, and high-profile individuals throughout the Indian government. Tactics, techniques, and procedures (TTPs) of this campaign include Winter Vivern actors hosting clones of websites to disseminate their malicious payloads, hosting websites for credential phishing, and deploying masked Windows batch files to execute on a set schedule. One (1) malware variant observed during this campaign is "APERETIF", which is often hosted on vulnerable WordPress websites for malware distribution. Indicators of compromise (IOCs) uncovered in this recent Winter Vivern campaign can be referenced from the reports below. CTIX continues to monitor threat actor activity worldwide and will provide additional updates accordingly.

  - The Record: Winter Vivern Article
  - Sentinel One: Winter Vivern Report

SideCopy APT Actors Target Indian Government Agency

Reported in the March 21st, 2023, FLASH Update

- In their latest campaign, threat actors from the SideCopy APT group have been explicitly targeting users working for India's Defense Research and Development Organization (DRDO). The SideCopy APT group operates out of Pakistan and frequently targets entities throughout Southern Asia, including India and Afghan government entities. SideCopy was named as such due to their mirror-like infection chain of Sidewinder; a threat group operating in India. Additional reports also indicate some attribution to the Transparent Tribe (APT36) group who may be the parent organization of SideCopy. In this recent campaign, threat actors disseminate phishing campaigns to DRDO employees containing a URL to a supposed DRDO-related missile PowerPoint. However, upon visiting the link, users unknowingly download a malicious payload from the Action Rat malware family. The malware uses a variety of cloaking mechanisms such as changing the name of the file to avoid anti-virus detection. The malware itself establishes a connection to actor-controlled command-and-control (C2) servers where a bulk of user device data is uploaded. This data contains a variety of system information including device hostname, account username, operating system, and installed anti-virus applications. In addition to information gathering, the malware can remotely execute a list of commands to pull down additional payloads, gather additional file system documents, and obtain hardware information. CTIX analysts urge users to validate the integrity of email correspondence prior to visiting any embedded URL's or downloading any attachments to lessen the risk for threat actor compromise.

  - Cyble: SideCopy APT Article

North Korean Hackers Target German/South Korean Experts

Reported in the March 24th, 2023, FLASH Update

- Government agencies from Germany and South Korea issued a statement this week about a new campaign targeting experts of the Korean Peninsula. The group behind these attacks is a well-known North Korean threat organization tracked as Kimsuky, also known as Thallium or Konni Group. Active since 2012, this group initially focused on targeting assets from South Korea but has now shifted to include Russia, Europe, United States, and United Nations to their target list. Kimsuky consistently goes after intelligence from foreign policy and national security issues tied to the region, nuclear industry, and sanctions. These actors were also responsible for the 2014 Korean Nuclear Power Co. compromise alongside Operation Stolen Pencil, Operation Kabar Cobra, and Operation Smoke Screen, all which occurred between 2018 and 2019. The recent campaign unveiled that Kimsuky threat actors were spearphishing Korean experts by impersonating administrators. These email correspondences included a malicious payload where a Chromium-based extension was installed on the user's device unknowingly. Once the user opened their respective mail application, the malicious code would harvest the user's entire email inbox and upload it to actor-controlled command-and-control servers. CTIX continues to monitor threat actor activity globally and will provide additional updates accordingly.

  - The Record: Kimsuky Article

Threat Profile: Dark Power

Reported in the March 28th, 2023, FLASH Update

- A new ransomware group has made its presence known in the threat landscape by compromising ten (10) victims in a short period of time. The group calls themselves Dark Power and are believed to be operational since late January 2023, according to compiled data from their ransomware encryptor. Dark Power actors are following trends of several ransomware gangs by practicing double extortion, exfiltrating and encrypting the victim's data before later posting the exfiltrated data to their leak site if ransom demands are not met. Ransom demands uncovered to this point average $10,000, which is significantly lower than major players in the ransomware scene. Thus far, victims of Dark Power appear to operate in countries across the globe including Algeria, Egypt, France, Turkey, United States, and several others. So far, these actors have compromised at least ten (10) organizations encompassing several industries such as education, IT services, food production, healthcare, and manufacturing. An interesting tactic, technique, and procedure (TTP) of the group is that rather than utilizing text files to display ransom notes, Dark Power uses a PDF document in its place to show the ransom demand, qTox for negotiations, and onion address to the victim leak page. Overall, based on the variety of locations and industries Dark Power is targeting, they appear to compromise entities by opportunity rather than focusing on a direct country or industry, showing that the group is ready to make a name for themselves. Observed indicators of compromise (IOCs) can be viewed in the report linked below. CTIX continues to track threat actor activity worldwide and will provide additional updates accordingly.
  - Trellix: Dark Power Report

Threat Profile: APT43

Reported in the March 31st, 2023, FLASH Update

- Threat actors from the North Korean APT43 group have come into light after security researchers unveiled new shifts in targeting and operational changes. Active since 2018, APT43 operates in support of North Korean interests and has recently been targeting government entities, manufacturing, educational institutions, and business services throughout the United States, Japan, and South Korea. Previously motivated by cyberespionage, APT43 has begun shifting to more financially motivated attacks through several cryptocurrency laundering schemes. Additionally, APT43 actors lean on their sophisticated social engineering attacks as a primary point of compromise for their operations, more often utilizing fake online personas to gain trust and persuade users to download custom malicious payloads. Malware utilized by APT43 includes custom built in-house scripts alongside variants of “Pencildown”, “Venombite”, “Pendown”, and the “Hangman” backdoor. During some operations conducted around the COVID-19 pandemic, APT43 actors were rumored to have utilized custom malware from the Lazarus hacking group. APT43 continues to evolve as a threat organization and is becoming more of an asset to the Kimsuky family of actors. CTIX continues to monitor threat actor activity worldwide and will provide additional updates accordingly.

- ○ Mandiant: APT43 Article
- ○ CyWare: APT43 Article

VULNERABILITIES

Quantum Computing: Researchers Identify that CRYSTALS-Kyber, a Post-Quantum Algorithm, May Be Vulnerable to Exploitation

Reported in the March 3rd, 2023, FLASH Update

- A future quantum computing general-purpose algorithm standard selected by the U.S. National Institute of Standards and Technology (NIST) could be vulnerable to exploitation. Researchers from Sweden's KTH Royal Institute claim to have identified a security vulnerability impacting the quantum safe algorithm known as CRYSTALS-Kyber, which may be vulnerable to a side-channel attack. A side-channel attack is any attack based on extra information gathered because of the fundamental way a computer protocol or algorithm is implemented rather than flaws in the design of the protocol or algorithm itself. In the case of CRYSTALS-Kyber, the miniscule pieces of data that are leaked, as a byproduct of the way the algorithm functions, were collected and observed by researchers leveraging a neural network training method called recursive learning. In this side channel attack, the small data units leaked by the algorithm were analyzed for "small variations in power consumption or electromagnetic radiation to reconstruct what the machine is doing and find clues that would enable access." Successful exploitation could allow unauthenticated threat actors to access and exfiltrate privileged information. Notably, this attack didn't crack the algorithm itself and instead exploited a specific practical application implementation of the of the algorithm. Although this came as a surprise to the researchers, they did state that this finding is very beneficial since it is necessary to research these types of attacks prior to quantum computing becoming generally available to the public.

    - The Record: CRYSTALS-Kyber Vulnerability Article
    - KTH Royal Institute of Technology: CRYSTALS-Kyber Exploitation Report

PoC Published on Twitter for a Critical Microsoft Word Vulnerability Allowing for RCE

Reported in the March 7th, 2023, FLASH Update

- A proof-of-concept exploit has just been published for a critical vulnerability affecting Microsoft Word that could be exploited by threat actors to conduct remote code execution (RCE) attacks on vulnerable systems. The flaw, tracked as CVE-2023-21716, is a heap memory corruption vulnerability within Microsoft Word's RTF (Rich Text Format) parser and occurs when dealing with Microsoft Office’s “wwlib.dll”, a font table "(*\fonttbl*) containing an excessive number of fonts (*\f###*).” A remote attacker could exploit this flaw by creating a malicious ".RTF" file and delivering it to the victim through a phishing email or other social engineering tactic. This flaw does not require much user interaction to be exploited; simply previewing a malicious .RTF file using Microsoft Word could allow the threat actor to execute code with the permissions of the opening application. The low-level of user interaction coupled with the low complexity of the attack and a PoC exploit gives this flaw a CVSS score of 9.8/10. To prevent exploitation, Microsoft users should ensure that the latest updates are installed. If users cannot apply the patch, Microsoft has provided workarounds in their advisory, which include modifying the Windows Registry and enabling the Microsoft Office File Block policy, preventing any Office applications from automatically opening RTF documents unless the user approves the file origin. There is currently no evidence of active exploitation. CTIX analysts will continue to monitor this matter as well as other Microsoft critical vulnerabilities.

    - Microsoft: CVE-2023-21716 Advisory
    - Bleeping Computer: CVE-2023-21716 Article

Critical Fortinet Vulnerability Allows RCE and Can Lead to DoS

Reported in the March 10th, 2023, FLASH Update

- The cybersecurity solutions provider Fortinet has patched a critical vulnerability that could allow unauthenticated remote attackers to execute arbitrary code on vulnerable devices. The flaw, tracked as CVE-2023-25610, affects the administrative interface of their FortiOS and FortiProxy products, and is the result of a buffer underflow/underwrite/underrun. A buffer underflow occurs when a program attempts to read input data that's shorter than the allocated space, causing memory leaks and memory corruption. An unauthenticated threat actor could exploit this flaw by sending maliciously crafted requests to vulnerable instances of FortiOS and FortiProxy. Successful exploitation would allow threat actors to crash the service, pilfer sensitive information, conduct remote code execution (RCE), and cause denial-of-service (DoS) conditions to its GUI. Fortinet states in their security advisory that there is no evidence that this vulnerability is being actively targeted and exploited by attackers. CTIX analysts recommend that all administrators managing Fortinet devices ensure that they download and install the latest patch to prevent exploitation. If Fortinet products cannot be patched at this time, Fortinet has provided manual workarounds which include completely disabling the HTTP/HTTPS administrative interface, blocking it from the public internet, or whitelisting authorized IP addresses to prevent unauthenticated users from accessing the vulnerable instances.

    - Bleeping Computer: CVE-2023-25610 Article
    - The Hacker News: CVE-2023-25610 Article
    - Fortiguard: CVE-2023-25610 Advisory

CISA Adds Exploited Plex RCE Vulnerability Linked to LastPass Breach to the KEV

Reported in the March 14th, 2023, FLASH Update

- The Cybersecurity and Infrastructure Security Agency (CISA) has added an actively exploited critical remote code execution (RCE) vulnerability, potentially connected to the August 2022 LastPass breach, to its catalog of Known Exploited Vulnerabilities (KEV). The flaw, tracked as CVE-2020-5741, affects Plex Media Server, a central media hub where customers can access personal media on their own servers as well as stream free and on-demand movies and music. A threat actor that has previously gained access to a Plex Media Server administrator account could exploit Plex's Camera Upload feature to upload a maliciously crafted file to the Plex server, which then executes with no user interaction. The flaw has been patched by Plex, and the company urges their customers to upgrade to version 1.19.3 or newer to prevent exploitation. Although this vulnerability has not been definitively attributed to the LastPass breach, researchers believe that it is likely. LastPass was compromised after threat actors targeted a DevOps engineer’s home computer, and LastPass officials stated that the attacker exploited "a vulnerable third-party media software package, which enabled remote code execution capability and allowed the threat actor to implant keylogger malware”. Although LastPass has yet to confirm what vulnerability was exploited, they did admit that the exploited media software package was a Plex Media Server. The flaw's presence on the KEV mandates that all Federal Civilian Executive Branch (FCEB) agencies must patch this flaw no later than March 31, 2023, or face regulatory accountability. The LastPass compromise has been a novel and very dynamic situation, with new updates frequently being published. CTIX analysts will continue to monitor this matter as well as report on the latest critical vulnerabilities.

    - Bleeping Computer: CVE-2020-5741 Article
    - Plex: CVE-2020-5741 Advisory

- ○ ARS Technica: LastPass Employess Compromise Article

Over 100 Organizations Actively Exploited with Fortra GoAnywhere MFT Bug

Reported in the March 17th, 2023, FLASH Update

- A spokesperson for the cloud data management firm Rubrik, confirms that the company was compromised by malicious threat actors from the Clop ransomware group, exploiting a vulnerability in a third-party file transfer tool. The threat actors exploited a flaw in the GoAnywhere MFT managed file-transfer solution from Fortra, a critical vulnerability which has already led to the compromise of over 100 additional organizations. The flaw, tracked as CVE-2023-0669, is a pre-authentication command injection vulnerability from deserializing an arbitrary attacker-controlled object within GoAnywhere's License Response Servlet. A malicious attacker who has gained access to an administrator console could exploit this flaw to conduct remote code execution (RCE). The exfiltrated Rubrik data comes from a non-production IT testing environment containing internal sales information such as customer and partner names, business contacts, and a “limited number” of distributor orders. The third-party firm conducting Rubrik's post breach analysis stated that "there was no sensitive personal data such as Social Security numbers, financial account numbers, or payment card numbers exposed in the servers accessed." The data is slowly being posted on Clop's leak site, in an attempt to further extort ransom payment from Rubrik. The Cybersecurity and Infrastructure Security Agency (CISA) has added this vulnerability to their Known Exploited Vulnerabilities (KEV) catalog, meaning that regulated agencies must quickly patch the flaw or be held accountable. This vulnerability has since been patched, and CTIX analysts urge any organizations using GoAnywhere MFT to upgrade to version 7.1.2 to prevent exploitation. Attacks from Clop ransomware have been on the rise since the end of January, adding exfiltrated data to their leak site from several other organizations.
    - ○ The Record: CVE-2023-0669 Article
    - ○ Bleeping Computer: Clop Ransomware CVE-2023-0669 Article
    - ○ CISA: KEV

Acropalypse Flaw Affecting Google Pixel Devices Allows Redacted and Cropped Screenshots to Be Restored to the Original Image

Reported in the March 21st, 2023, FLASH Update

- Two (2) security researchers have published a proof-of-concept (PoC) exploit for a critical API design vulnerability affecting Google Pixel devices. The flaw exists in the Android 9 Pie Markup utility which allows users to crop, edit, and redact images and screenshots. In the PoC published on Twitter, the Markup's Pen tool is used to redact the card number from an image of a credit card, which is then exploited to partially recover the original image, clearly displaying the card number. A technical article from the 9to5Google website states that when an "image is cropped using Markup, it saves the edited version in the same file location as the original. However, it does not erase the original file before writing the new one. If the new file is smaller, the trailing portion of the original file is left behind, after the new file is supposed to have ended." The flaw, tracked as CVE-2023-21036, has been coined "Acropalypse", and successful exploitation could allow approximately 80% of an edited screenshot to be recovered. This poses a great threat to Pixel users who may use the Markup utility to protect sensitive information, as well as their own identity and the identity of others. Along with the PoC exploit, the researchers have offered a free demo utility which allows Pixel users to test the exploit on their own redacted and cropped images. The flaw was first reported to Google in January 2023, and on March 13, 2023, the vulnerability was patched. It should be noted that although the patch defends new image edits, it will not protect edited screenshots from the past five (5) years. One of the researchers stated that he wrote a script to scrape his own message history and found many images he'd sent over the years were vulnerable to exploitation. CTIX analysts recommend that all Google Pixel users should ensure that they are running the latest secure version of Android 9 to prevent exploitation of future images. There is currently no answer on providing a solution that patches images that have already been taken. CTIX will monitor this matter and provide relevant updates if a solution is identified.

- Security Affairs: Acropalypse Article
- 9to5Google: Acropalypse Article
- Google Issue Tracker: Acropalypse Technical Report

PoC Exploit Published on Github for Exploiting Critical Vulnerability in Veeam Backup & Replication Solution

Reported in the March 24th, 2023, FLASH Update

- A cross-platform proof-of-concept (PoC) exploit has been published on Github by researchers from Horizon3's Attack Team for a critical remote code execution (RCE) vulnerability affecting the digital security provider Veeam. Veeam Software is a US-based information technology company that develops backup, disaster recovery and modern data protection software for virtual, cloud-native, software-as-a-service (SaaS), Kubernetes and physical workloads. According to Veeam, its Veeam Backup & Replication (VBR) solution is very popular, leveraged by more than 450,000 customers across the world including "82% of Fortune 500 companies and 72% of Global 2,000." The flaw, tracked as CVE-2023-27532, exists in "Veeam.Backup.Service.exe", running on TCP port 9401 by default. It affects all VBR versions, and successful exploitation could allow unauthenticated threat actors to request encrypted credentials stored in the VeeamVBR configuration database. This would allow them to gain access to backup infrastructure hosts by exfiltrating the stolen credentials and gaining RCE with SYSTEM privileges. From there, the actors can move laterally across the network, drop malware, and exfiltrate sensitive data. This vulnerability was reported in February 2023, and was subsequently patched on March 7, 2023. CTIX analysts recommend that all VBR administrators ensure that they have updated their platform to prevent exploitation. Veeam also published a workaround for customers who cannot immediately patch their systems. If taking their servers offline would create too much of a negative impact to critical business processes, administrators can protect their vulnerable servers from this exploit by blocking all non-critical external connections to TCP port 9401 through their firewall.

    - Bleeping Computer: CVE-2023-27532 Article
    - Github: CVE-2023-27532 PoC Exploit
    - Veeam: CVE-2023-27532 Advisory

Critical Microsoft Outlook Zero-day Vulnerability Under Active Exploitation

Reported in the March 28th, 2023, FLASH Update

- Microsoft has published step-by-step guidance for detecting and blocking an actively exploited critical zero-day vulnerability affecting Microsoft Outlook. The guidance shows administrators how to identify indicators of compromise (IOC) to ascertain if they've already been compromised, as well as how to detect active attack attempts and defend their servers from the future exploitation of this flaw. The vulnerability, tracked as CVE-2023-23397, is an escalation of privilege flaw that allows privileged Net-NTLMv2 hashes to leak without any user interaction. The hashes can then be collected, weaponized, and redirected to perform NTLM-relay attacks by sending maliciously crafted emails to vulnerable Outlook instances. Successful exploitation allows the threat actor to manipulate the victim's session, allowing them to authenticate as the victim by "sending messages with extended MAPI properties containing UNC paths to attacker-controlled SMB shares." The pilfered credentials that the threat actors exfiltrate can be used for lateral movement, as well as changing vulnerable Outlook mailbox folder privileges, allowing the attackers to redirect sensitive emails from targeted accounts to their own command-and-control (C2) infrastructure. The exploitation of this flaw has been attributed by Microsoft to "a Russia-based threat actor," with other researchers believing it could be APT28 (STRONTIUM, Sednit, Sofacy, and Fancy Bear). CTIX analysts urge all Outlook and Exchange administrators to ensure that the guidance in the linked advisory is strictly followed to prevent their networks from being compromised.

  - Bleeping Computer: CVE-2023-23397 Article
  - GBHackers On Security: CVE-2023-23397 Article
  - Microsoft: CVE-2023-23397 Guidance

Critical Flaw in Microsoft Azure Could Allow Unauthenticated Remote Code Execution

Reported in the March 31st, 2023, FLASH Update

- Microsoft has patched a critical vulnerability in an Azure inspection tool that could be exploited by unauthenticated threat actors to conduct remote code execution (RCE). The flaw, tracked as CVE-2023-23383, exists in Azure Service Fabric Explorer (SFX) and has been dubbed "Super FabriXss", an homage to the "FabriXss" vulnerability patched in October 2022 by Microsoft. Azure SFX is a "distributed systems platform" that streamlines the ability to package, deploy, and manage microservices and containers, as well as assist with development and management of cloud applications. The vulnerability is a reflected cross-site scripting (XSS) flaw that gives unauthenticated attackers the ability to upload malicious scripts to trusted websites, compromising any unsuspecting victims who visit the site. The vulnerability received a CVSS score of 8.2/10, significantly higher than the original FabriXss flaw which had a CVSS of 6.2/10. This is due to the fact that the attacker can achieve full RCE without the prior need to authenticate as an administrative user. If successfully exploited, attackers would be able to launch follow-on attacks like dropping malware, as well as take complete control of affected systems. This vulnerability has been patched, and CTIX analysts urge users to ensure that they are running the most recent secure version of the platform.

  - The Record: CVE-2023-23383 Article
  - The Hacker News: CVE-2023-23383 Article
  - Microsoft: CVE-2023-23383 Advisory

HONORABLE MENTIONS

Euler Finance Falls Victim to a $197 Million Flash Loan Attack

Reported in the March 14th, 2023, FLASH Update

- An unidentified group of cybercriminals defrauded Euler Finance, a company specializing in cryptocurrency lending, of nearly $200 million. PeckShield, who specializes in detecting irregularities in blockchain asset transfers, was the first to flag the unusually massive transfer of crypto assets on Euler's crypto exchange platform, which utilizes a capital-efficient permissionless spending protocol. Lenders can make transactions without the presence of a trusted third-party, which the company noted allows users to earn greater interest on their assets while having a better ability to hedge the volatile crypto market. However, this may have assisted the hijackers who used what's known as a "flash loan attack" to pull off their heist. The attackers were able to manipulate Euler's smart contracts by targeting a vulnerability in their lending protocol, enabling them to borrow large sums of crypto assets without having to return them. Euler's specific logic flaw was in their donation and liquidation system where attackers manipulated the conversion rates to earn exaggerated profits when liquidizing their assets. The threat actor’s ETH wallet is being used to track the stolen assets; however, the criminals have reportedly begun washing their stolen funds via Tornado Cash, a sanctioned cryptocurrency mixer. CTIX analysts will continue to monitor this situation and provide additional updates as appropriate.

  ○ Gizmodo: Euler Finance Article
  ○ Bleeping Computer: Euler Finance Article

ChipMixer Platform Seized and Dismantled for Laundering Ransomware Payments

Reported in the March 17th, 2023, FLASH Update

- Adding to recent efforts to tackle international cybercrime, the US (FBI), Germany (BKA), and other European law enforcement agencies led a coordinated effort to seize four (4) servers belonging to ChipMixer along with $46.5 million in Bitcoin and seven (7) TB of data. ChipMixer has been a notorious player in the cryptocurrency mixing platform arena, having facilitated the laundering of up to $3.75 billion Bitcoin since beginning their operations in 2017. Cryptocurrency mixers offer a way for hackers, ransomware groups, and scammers to obfuscate financial tracks by commingling users’ crypto assets and funneling the pool of clean, untraceable money back out to the designated recipients. The ChipMixer platform has facilitated mixing $844 million worth of digital assets linked to illicit addresses with known criminal activity, a large majority of which has been traced back to stolen funds. ChipMixer is suspected to have aided prominent criminal groups such as North Korea’s Lazarus Group, APT28 (aka Fancy Bear or Strontium), LockBit, Zeppelin, SunCrpyt, Mamba, and Dharma. Beyond dismantling the clearnet and dark web websites connected to the platform, DOJ also charged Minh Quốc Nguyễn, the 49-year-old Vietnamese national, for money laundering and his association with creating and running the unlicensed crypto currency mixing service.

  ○ Bleeping Computer: ChipMixer Article
  ○ The Hacker News: ChipMixer Article
  ○ The Record: ChipMixer Article

Alleged BreachForums Owner Pompompurin Arrested on Cybercrime Charges

Reported in the March 21st, 2023, FLASH Update

- After the takedown of the RaidForums dark web hacker destination last year, BreachForums soon emerged in its place. The suspected administrator and owner of BreachForums, Pompompurin, is now in US Federal custody. During his arrest in connection to operating the hacking platform, 21-year-old Connor Brian Fitzpatrick reportedly admitted to being the owner of the BreachForums cybercrime conclave and claimed the alias "Pompompurin". FBI Special Agent John Longmire testified that "when I arrested the defendant on March 15, 2023, he stated to me in substance and in part that: a) his name was Conor Brian Fitzpatrick; b) he used the alias 'pompourin,' and c) he was the owner and administrator of 'BreachForums,' the data breach website referenced in the Complaint." BreachForums was known to be the largest data leak forum on the market, a digital haven for cybercriminals, hackers, and ransomware gangs looking to sell or buy the caches of data stolen during hacks and breaches. Just last week, the platform was used to post the sensitive personal data of US Congressional members and staff from the DC Health Link breach. A user who goes by the moniker "Baphomet" emerged claiming to be in the process of migrating the platform to new infrastructure. Baphomet also stated that he has enough access to protect BreachForums' infrastructure and users, has taken steps to restrict access from Pompompurin's account, and has been constantly monitoring logs to detect any signs of intrusive alterations. The actor named Baphomet is attempting to carry the torch that Pompompurin had once carried after the shutdown of their forebearer, RaidForums. It should be noted that on March 21, 2023, BreachForums was officially shut down, and can no longer be accessed. Baphomet posted a final message on the forum indicating the likely presence of Federal agents within the servers, and thus, the inability to operate in a safe manner.CTIX analysts will continue to monitor the situation and any migrating that occurs due to the shutdown.

    - Bleeping Computer: Pompompurin Article
    - The Record: Pompompurin Article
    - Krebs on Security: Pompompurin Article

New Malicious ChatGPT Chrome Extension Targets Facebook Accounts

Reported in the March 24th, 2023, FLASH Update

- Google has removed a malicious version of the ChatGPT Chrome browser extension from its Web Store that was stealing Facebook session cookies to take over accounts. The trojanized version of the legitimate ChatGPT extension, called "ChatGPT for Google", was originally uploaded to the Web Store on February 14, 2023, however the threat actor only started promoting it with Google Search advertisements on March 14, 2023. The extension had gained over 9,000 installations since March 14, 2023, and advertised the ability to improve search results when integrated. In actuality, the extension added code that covertly captured Facebook-related cookies and exfiltrated them to a remote server in an encrypted manner. The malware abuses the Chrome Extension API to acquire a list of the Facebook-related cookies before encrypting them using an AES key and attaching them to the X-Cached-Key HTTP header value. The stolen data is exfiltrated via a GET request to the attacker's server which can then be decrypted, ultimately hijacking the victim's Facebook sessions. Once the threat actor has the victim's cookies, they can proceed to take control of their Facebook accounts, change the passwords, profile names, and pictures, and even use it to disseminate misinformation or extremist propaganda. The extension is communicating with the same infrastructure used in a previous Chrome add-on campaign that had amassed 4,000 installations before Google removed it from the Chrome Store earlier this month. The latest extension was a backup for when the earlier version was reported and removed. However, it’s likely that the threat actor will have a backup plan via another “parked” extension waiting to be published, facilitating the next wave of infections. This exploitation trend underscores how cybercriminals are adapting their campaigns to capitalize on the popularity of ChatGPT to distribute malware and stage opportunistic attacks.

- ○ Bleeping Computer: Malicious ChatGPT Extention Article
- ○ The Hacker News: Malicious ChatGPT Extention Article

Norwegian Sailors Sound a Warning About Cyberattacks on the High Seas

Reported in the March 28th, 2023, FLASH Update

- Researchers with seafaring backgrounds are sounding the alarm about cyberattacks on ships and the catastrophic outcomes compromised floating computers present. While no official incidents have been reported, there have been many strange, unexplainable events occurring to ships recently. Cyberattacks on the supply chain and shipping industry have become common, as they're valuable targets for both financial and geopolitical purposes. Thus, ships themselves pose a significant risk, given that their inherent role in shipping and supply make them critical targets, with additional escalatory risks for those working in energy, oil, gas, agriculture and more. Some suspected attacks include jamming of ships' GPS causing unintentional entry into unauthorized waters, spoofing AIS (automated identification system) broadcasts of one ship's signal to the location of another ship, or potentially hacking the rudder on a ship to make it run aground. The scarcity of publicly acknowledged cyberattacks at sea doesn't necessarily point to the absences of cyberattacks but rather to the lack of official reporting in the shipping industry, where crew members handle these suspected cyberattacks the same as they would a typical maritime technical issue. Researchers at the Norwegian University of Science and Technology (NTNU) want to bring awareness to ship owners, their crews, and seafarers at large about the real-world implications that cyberattacks could have on ships while highlighting how a ship's Operational Technology (OT) and Information Technology (IT) are highly connected, meaning malware to the IT directly affects the OT. Maritime security and IT personnel should be prepared to handle the physical consequences that can arise from compromised IT and strengthen their ship's security to further deter hackers.
  - ○ The Record: Seafaring Cyberattacks Article

Experts Push to Slow Artificial Intelligence Research and Development

Reported in the March 31st, 2023, FLASH Update

- An open letter released by Future of Life institute has called on all artificial intelligence (AI) labs to immediately pause the training of powerful AI systems for at least six (6) months. The letter has been signed by experts in the field, influential researchers, leaders, and top executives, including Elon Musk and Steve Wozniak. It’s believed that the necessary planning, management, and care has not taken place in the development of AI, a powerful technology that not even the creators are fully able to understand, predict, or control. A reckless and naïve attitude has the potential to foster uncontrolled job automation, AI powered cyberattacks, and the relentless spread of disinformation and deepfakes. The letter addresses these growing concerns and potential risks that AI poses to human civilization, highlighting that the next few months of AI development will fundamentally dictate the course of history and our fate as a species. The objective of the letter isn’t intended to totally halt AI. Instead, researchers and developers should use this period of AI down-time to come together and formulate standardized safety protocols, build strict oversight, and heighten confidence to ensure that this emerging technological advancement can be used for the greater benefit and flourishment of human civilization rather than its demise.

- Bleeping Computer: AI Pause Article
- ESET: AI Pause Article
- Future of Life: AI Pause Letter