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

April 2023

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 April 2023, originally published in CTIX FLASH Updates throughout April. 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

TMX Finance Discloses Data Breach Impacting 4.8 million Individuals

Reported in the April 4th, 2023, FLASH Update

- TMX Finance (TMX), along with a portion of its subsidiaries, collectively disclosed a data breach following a cyberattack that was discovered on February 13, 2023, after suspicious activity was observed. TMX's impacted subsidiaries consist of TitleMax (a leading car title loan company in the United States), TitleBucks (a company specializing in car title-secured loans or pawns as well as in-store or online personal loans), and InstaLoan (a fast-approval personal loan service). An investigation into this activity concluded that an unauthorized third-party gained access to TMX systems on December 10, 2022, and data of approximately 4.8 million individuals was exfiltrated between February 3 and February 14, 2023. The company's data breach notice explains that the exfiltrated data includes names, dates of birth, passport numbers, driver's license numbers, federal/state identification card numbers, tax identification numbers, Social Security numbers (SSNs), financial account information, and additional data such as phone numbers, email addresses, and physical addresses. The actor responsible for the cyberattack and data breach of TMX has yet to claim responsibility, and TMX has not publicly attributed the attack to a specific threat group as of April 4, 2023. CTIX will continue to monitor the TMX Finance data breach and provide updates when available.
    - ○ The Record: TMX Finance Data Breach Article
    - ○ Office of the Maine Attorney General: TMX Finance Data Breach Notification Listing

Researchers Observe "Rorschach", One of the Fastest Ransomware Strains to Date

Reported in the April 7th, 2023, FLASH Update

- Researchers have recently observed a previously unnamed ransomware dubbed "Rorschach" that they emphasize to be "one of the fastest ransomware observed, by the speed of encryption." In the observed instance, researchers noted that Rorschach was deployed "using DLL side-loading of a Cortex XDR Dump Service Tool, a signed commercial security product," which is a loading method that is not typically utilized by ransomware operations and uses three (3) files during execution. The main payload is injected into "notepad.exe" and then runs processes in SUSPEND mode while providing falsified arguments. This technique is conducted to make analysis more difficult as well as deleting shadow volumes and backups by using legitimate Windows tools, clearing specific Windows event logs, disabling the Windows firewall, and attempting to stop a number of predefined services. Researchers explained that Rorschach has interesting capabilities that are not commonly seen in ransomware, such as making direct calls using the "syscall" instruction in order to evade defense mechanisms. Rorschach also employs a "highly effective and fast hybrid-cryptography scheme," which encrypts only a specific portion of the original file content rather than the entire file. Researchers emphasized that these capabilities, amongst others, allowed the ransomware to encrypt an environment in only four (4) minutes and thirty (30) seconds. LockBit 3.0, another known fast ransomware strain, encrypted an identical environment in seven (7) minutes. Despite having no clear-cut overlaps with any known ransomware groups, Rorschach has similarities to the leaked source code of Babuk ransomware and is suspected of taking inspiration for some components from LockBit 2.0. The ransom note also has similarities to Darkside and Yanlowang. CTIX analysts will continue to monitor Rorschach for new activity. Indicators of compromise (IOCs) as well as additional technical details can be viewed in the linked report.
    - ○ Bleeping Computer: Rorschach Ransomware Article
    - ○ Checkpoint: Rorschach Ransomware Report

Balada Injector Campaign Compromised 1 million WordPress Websites Since 2017

Reported in the April 11th, 2023, FLASH Update

- Researchers have published a new report detailing a large-scale campaign dubbed “Balada Injector” that has exploited approximately 1 million WordPress websites. This campaign has been tracked by researchers since 2017 and is known for leveraging "all known and recently discovered theme and plugin vulnerabilities" in WordPress websites. The attacks are conducted in waves, typically once a month, with a newly registered domain used in each wave. The domains redirect victims to various fraudulent websites, including lottery, push notification, and tech support scams. Balada Injector's main focus is exfiltrating sensitive information, such as database credentials, in order to maintain persistence in the event that the victim clears the infection and patches their vulnerabilities. The campaign also has the goal of collecting backup archives and databases, files that may contain sensitive data, access logs, and debug information. Adminer and phpMyAdmin are also searched for, as the legitimate tools are used to create new admin users and inject malware into the victims' databases. The campaign operators have also been observed deploying various backdoors to the compromised WordPress websites, with some instances involving dropping backdoors to 176 predefined paths in order to increase the difficulty of removing the malware. The backdoor names are also changed in each wave of the campaign to make detections more difficult. Researchers have emphasized that each wave of attacks in Balada Injector differs, so there are no specific instructions to mitigate the risk of attack at this time due to the wide variety of infection vectors. CTIX analysts urge administrators to use strong passwords and multi-factor authentication (MFA), ensure applications such as WordPress plugins are up to date with the latest patches, and monitor user accounts for suspicious activity. Additional technical details as well as indicators of compromise (IOCs) can be viewed in the report linked below.

    - Bleeping Computer: Balada Injector Article
    - Sucuri: Balada Injector Report

Private Sector Offensive Actor QuaDream Linked to DEV-0196

Reported in the April 14th, 2023, FLASH Update

- Microsoft researchers have linked, with high confidence, a threat group tracked as DEV-0196 to an Israel-based private sector offensive actor (PSOA) known as QuaDream. QuaDream has been targeting the iOS devices of journalists and political figures across Europe, North America, Southeast Asia, and the Middle East with malicious spyware. QuaDream is known to market a surveillance platform to governments for "law enforcement purposes" known as "REIGN," which is "a suite of exploits, malware, and infrastructure designed to exfiltrate data from mobile devices." The malware, dubbed "KingsPawn", is developed by DEV-0196 and has a monitor agent that is responsible for reducing the malware's footprint on the victim device to evade detection. The primary malware agent has the capabilities to collect device data, cellular and Wi-Fi data, access location, gather files, access the device's camera, obtain call logs, and more. Citizen Lab researchers also observed a "zero-click exploit" dubbed "ENDOFDAYS" which they suspect was used to hack into target devices with the iOS versions of 14.4 and 14.4.1. Researchers explained that the exploit uses two (2) backdated and overlapping iCloud calendar invites (that are invisible to the account owner) as an initial attack vector and are automatically processed due to a flaw in iOS 14, which does not notify the account owner of these invites. When deployed, the spyware attempts to bypass detection by covering its tracks. QuaDream has previously been in the media for taking advantage of the FORCEDENTRY zero-click exploit in iMessage in order to deploy REIGN in early 2022, and approximately 250 of its fraudulent Instagram and Facebook accounts that were used to "infect Android and iOS devices and exfiltrate personal data" were taken down in late 2022. Additional technical details regarding DEV-0196 and QuaDream, as well as indicators of compromise (IOCs), can be viewed in the two reports linked below.

- The Record: QuaDream Article
- The Hacker News: QuaDream Article
- Microsoft: QuaDream Report
- Citizen Lab: QuaDream Report

New Domino Backdoor Suspected to be a Collaboration Between Former Conti Members and FIN7

Reported in the April 18th, 2023, FLASH Update

- Researchers have observed a new backdoor dubbed "Domino" that they believe was likely developed by the FIN7 Russian cybercriminal group and is being utilized by former Conti affiliates since at least February 2023. This belief is due to code overlaps between Domino Backdoor and the "Lizar" malware family (also known as "Tirion" and "Diceloader"), which is linked to FIN7. Lizar is known to collect sensitive information from "clipboard, Discord, web browsers, crypto wallets, VPN services, and other apps." Domino's focus is to obtain victims' system information and send the data to its command-and-control (C2) server, where an AES encrypted payload is sent in return. Researchers emphasized that the returned payload, named "Domino Loader", is a second payload that has coded overlaps with Domino Backdoor. Domino is currently being used to deliver "either the Project Nemesis information stealer or more capable backdoors such as Cobalt Strike” and has been observed using the Dave Loader (which has been linked to Conti/Trickbot). Domino has been active in the wild since at least October of 2022. Additional technical details as well as indicators of compromise (IOCs) can be viewed in the report linked below.

    - The Hacker News: Domino Backdoor Article
    - IBM Security X-Force: Domino Backdoor Report

New Details Emerge regarding Three Zero-Click Exploits Used by the NSO Group to Target iPhone Users in 2022

Reported in the April 21st, 2023, FLASH Update

- Newly released research details new Pegasus spyware activity that occurred in 2022, specifically three (3) zero-click exploits that targeted iOS 15 and iOS 16. Researchers explained that the spyware targeted at least three (3) civil society targets from around the globe in 2022, with two (2) targeting members of an organization representing victims of military abuses in Mexico. It has been reported that Mexico's military is "the longest-standing client of Pegasus, and has used the spyware to target more cell phones than any other government agency in the world." The third victim of the latest Pegasus attacks has yet to be revealed by researchers. The first zero-click exploit identified is called "PWNYOURHOME", which was deployed against iOS 15 and iOS 16 around October of 2022. This exploit has two (2) parts: the first step targets the "HomeKit" feature and the second targets iMessage. The second zero-click exploit identified is "FINDMYPWN", which was deployed against iOS 15 around June of 2022. This exploit also has two steps in which it targets the "Find My" feature and then iMessage. Upon reviewing the first two exploits, researchers were able to identify "LATENTIMAGE", which is the first 2022 zero-click exploit released by the NSO Group that was on a single target's mobile device. LATENTIMAGE targets the "Find My" feature with a different method than FINDMYPWN. Researchers emphasized that the NSO Group is actively improving and advancing its spyware to evade detection. The researchers have also not seen any successful attacks involving PWNYOURHOME when victims have had activated iOS's Lockdown Mode feature, which is one way to help mitigate zero-click attacks as it warns the user in real-time of any exploitation attempts. Additional technical details can be viewed in the report linked below.

  - The Record: 2022 Pegasus Exploits Article
  - Citizen Lab: 2022 Pegasus Exploits Report
  - New York Times: Pegasus Targeting Mexico Article

Bumblebee Malware Loader Observed Infecting Machines through Fraudulent Software Installers

Reported in the April 25th, 2023, FLASH Update

- "Bumblebee", a malware loader discovered in April 2022, has been observed in a new campaign utilizing Google advertisements and SEO poisoning to target enterprises with promoted trojanized versions of popular applications, such as Cisco AnyConnect Secure Mobility Client, Zoom, ChatGPT, and Citrix. Bumblebee is often seen in phishing campaigns that deliver "payloads commonly associated with ransomware deployments" and has been actively evolving since its creation. Researchers emphasized that trojanizing installers for software that is "particularly topical (e.g., ChatGPT)" or often used by remote workers increases the likelihood of new infections. It has been observed that once Bumblebee has infected a victim device, the threat actor responsible moves laterally roughly three (3) hours after the initial infection and deploys Cobalt Strike as well as the legitimate AnyDesk and DameWare remote access tools. The actor uses a scheduled task to establish a persistence mechanism for Cobalt Strike, and additional tools are downloaded, such as various scripts and a network scanning utility mechanism. Researchers believe there are multiple threat groups and ransomware operations deploying Bumblebee, including Exotic Lily (a financially motivated threat group that uses ransomware variants such as "Conti" in its campaigns and is believed to be working with FIN12), Quantum, and MountLocker. CTIX analysts urge users to ensure all software is up to date with their latest patches to mitigate this risk. Indicators of compromise (IOCs) can be viewed in the reports linked below.

  - The Record: Bumblebee Malware Article
  - Secureworks: Bumblebee Malware Report

North Korean-Tied "RustBucket" Malware Targeting Apple macOS Devices

Reported in the April 28th, 2023, FLASH Update

- "RustBucket", a new malware targeting Apple macOS devices, has been observed and attributed to the financially motivated North Korean threat group BlueNoroff, which is a subgroup of the Lazarus Group (APT28). Researchers discovered similarities between the observed campaign and a campaign noted in December 2022 targeting Windows machines. The similarities included "malicious tooling on macOS that closely aligns with the workflow and social engineering patterns of those employed in the campaign." The campaign consists of a stage-one malware containing a suspicious AppleScript file which is contained in an unsigned application called "Internal PDF Viewer.app". From there, the malware executes commands to download the stage-two malware from its command-and-control (C2) server, which is also called "Internal PDF Viewer.app". Researchers noted that the malware is broken up into several stages to make any analysis more complicated, which is a common technique. The stage-two malware does not have an AppleScript file and has a different version, size, and bundle identifier data to appear more legitimate. The application is also signed by an ad-hoc signature. From the user perspective, a PDF viewing application is shown when the malicious application is launched, and the application is functional. A specific PDF must be loaded in the application for the malware to take next steps and communicate with the operators. Researchers described the PDF as a document that "shows a venture capital firm that is interested in investing in different tech startups" and noted that the PDF is likely the content from the website of a small but legitimate venture capital firm. The stage-three malware in this campaign is an ad-hoc signed trojan written in Rust that communicates with the C2 server for further instructions. CTIX analysts will provide updates regarding this campaign as they become available and will continue to monitor North Korean threat group activities. Additional technical details as well as indicators of compromise (IOCs) can be viewed in the report linked below.

- The Hacker News: RustBucket Article
- Jamf Threat Labs: RustBucket Report

THREAT ACTOR ACTIVITY

Tactical Octopus Actors Target Users Ahead of Tax Deadlines

Reported in the April 4th, 2023, FLASH Update

- Recently, threat actors operating out of the Tactical Octopus organization have been observed targeting individuals throughout the United States with tax-themed phishing emails. These carefully crafted phishing emails utilize lure documents such as real estate contracts, I-9 forms, and W-2 forms to entice users into unknowingly downloading malicious payloads to their device. The malicious code executes once the user extracts an attached password protected .ZIP archive containing a malicious LNK file that enables the download of a .VBS (Visual Basic Script) file. During execution of the .VSB file, the malicious code will reach out to an actor-controlled command-and-control (C2) server to pull down additional payloads to the system. Heavily obfuscated to evade anti-virus applications, these malware files contain several lines of unrelated comments and phrases to throw off detection algorithms. Furthermore, additional obfuscated PowerShell commands are executed on the system and show relation to code structures from a range of well-known malware such as Cobalt Strike and the “Kovter” RAT. IP addresses observed from C2 communications and malicious code show ties to Russian-hosted Internet Service Providers (ISP), alongside some United States ISPs. CTIX urges users to validate the integrity of email correspondence prior to downloading any attachments or visiting embedded hyperlinks. CTIX continues to monitor threat actor activity worldwide and will provide additional updates accordingly.

    - Securonix: Tactical Octopus Article
    - The Record: Tactical Octopus Article

North Korean Archipelago Attacks Observed

Reported in the April 7th, 2023, FLASH Update

- A North Korean state-sponsored threat actor known as ARCHIPELAGO has been linked to cyberattacks targeting think tanks in South Korea and the U.S. Researchers in South Korea and Google’s Threat Analysis Group (TAG) has tracked the ARCHIPELAGO for over a decade and determined its priorities to line up with the Reconnaissance General Bureau (RGB), North Korea’s foreign intelligence agency. ARCHIPELAGO primarily relies on the use of phishing emails that contain malicious links. These links redirect to recreated fake login pages for credential harvesting. ARCHIPELAGO also takes its time with victims, typically spending weeks building trust with the target before finally sending the malicious link to them. By also applying the “browser-in-the-browser” technique, which renders a fake window within an actual browser window, they can further convince the victim of the login page’s authenticity. Although email is the primary form of malware delivery, ARCHIPELAGO has also experimented with ISO files, Chrome extensions, and encoding commands into drive names, showing a slow but steady increase in sophistication with their attack techniques. ARCHIPELAGO has posed as a variety of actors, including journalists and government agencies in order to trick its victims. CTIX analysts will continue to monitor ARCHIPELAGO and its attacks across the globe.

    - The Hacker News: NK Archipelago Attacks
    - Google TAG: NK Archipelago Attacks

DEV-1084 Linked to MuddyWater Organization

Reported in the April 11th, 2023, FLASH Update

- Recent activity from the DEV-1084 threat group has shown some increased attribution to the Iranian nation-state threat group MuddyWater. DEV-1084 is believed to be a small threat organization working in tandem with MuddyWater, responsible for the post-breach destruction of victim networks and infrastructure. MuddyWater is a well-known threat group responsible for numerous cyberespionage attacks against government entities and critical infrastructure organizations throughout the United States, Southern Asia, and the Middle East. Threat actors from the group operate on the sole mission of gathering intelligence to benefit the Iranian state. Recent intelligence gathered by Microsoft shows that MuddyWater actors would exploit their target victim(s) and DEV-1084 would begin the invasive and crippling attacks on the victim's networks. DEV-1084 utilizes compromised administrative credentials to gain privileges within the environment, allowing for the encryption and exfiltration of company documents, storage, virtual machines/networks, cloud resources, and employee email inboxes. The connections showing relations between DEV-1084 and MuddyWater are a hosting IP address and domain name used by MuddyWater in past attacks, alongside usage of the MULLVAD VPN, Rport, and Ligolo custom scripts utilized by the group. MuddyWater continues to be a major player throughout the threat landscape and is believed to be comprised of several sub-groups, each focusing on a different aspect of the MuddyWater mission. CTIX continues to monitor threat actor activity worldwide and will provide additional updates accordingly.
    - Cyware: DEV-1084 Article
    - Microsoft: DEV-1084 Article

Threat Profile: Read The Manual Gang

Reported in the April 14th, 2023, FLASH Update

- A new ransomware organization has emerged in the threat landscape and is actively being tracked as the “Read The Manual” (RTM) Locker Gang. Motivated by opportunity rather than specific industries, RTM actors operate under the modus operandi of stealth, avoiding headlines in the news all while still making money from ransom demands. What is slightly different with this threat organization is that all mission dossiers and attacks are carried out by individual subgroups of the organization, adhering to strict rules of engagement set by group leaders. RTM actors will utilize social engineering and/or vulnerability exploitation to gain access into victim systems. Once compromised, threat actors will utilize numerous customized scripts to quietly encrypt their victim's data, tactically removing data from the recycle bin and any shadow copies created from the device. After the data is communicated back to actor-controlled command-and-control (C2) servers, victims have forty-eight (48) hours to begin negotiations with the threat actors before their data gets posted on the RTM public leak site. Ransom demands are often low enough that the group does not attract significant attention from the media, fulfilling their modus operandi. CTIX continues to monitor threat organizations throughout the landscape and will provide additional details accordingly.
    - Trellix: Read The Manual Article

SimpleHelp Remote Support Software Used by Iranian Hackers for Persistent Access

Reported in the April 18th, 2023, FLASH Update

- The Iranian threat actor known as Muddy Water, assessed to be a subordinate element within Iran's Intelligence Ministry (MOIS), has a history of deploying legitimate remote administration tools to targeted systems, specifically targeting systems of other Middle Eastern countries and the US. Having previously leveraged ScreenConnect, RemoteUtilities, and Syncro, this time the nation-state group figured out a way to legitimately download SimpleHelp from the official website and effectively use it in their attacks. SimpleHelp is a remote device control and management software tool, and MuddyWater is using it to establish persistence on targeted devices. MuddyWater was first seen leveraging SimpleHelp as far back as June 2022. However, it's still unclear how the software is distributed to host devices and what further actions are taken once downloaded. Researchers believe that spear-phishing emails from already compromised emails are sent with malicious links that download SimpleHelp, and then MuddyWater can use Fast Reverse Proxy (FRP) or Ligolo to establish persistence and extract information for final collection or additional lateral movement. A report released in January earlier this year encapsulated MuddyWater's attacks in Saudi Arabia and Egypt where SimpleHelp was used to deploy a Ligolo reverse tunneling tool and harvest credentials using MKL64. CTIX continues to monitor threat organizations around the globe and will provide additional details accordingly.

    ○ The Hacker News: SimpleHelp Article
    ○ Group-IB: SimpleHelp Blog

Threat Profile: Genesis Day

Reported in the April 21st, 2023, FLASH Update

- Threat actors from an up-and-coming threat organization in China targeted several South Korean academic institutions and research facilities in the early weeks of 2023. This group is tracked as Genesis Day, Teng Snake, or Xiaoqiying, and are primarily motivated by patriotism toward the Chinese state, making those who oppose China susceptible to their attacks. Operationally, Genesis Day actors were observed communicating on two (2) Telegram channels which went dark after news of their South Korean attacks hit the media. Based on harvested logs from the channels, Genesis Day actors have claim to be responsible for a number of attacks on United States, Japan, South Korea, and Taiwan companies. In their most recent campaign, Genesis Day actors targeted education and research institutions websites with multiple web-defacement attacks around the time of the Lunar New Year. Twelve (12) websites in total were affected by these attacks, all of which were believed to have some sort of connection to the United States, Singapore, and Taiwan. In addition, Genesis Day also threatened to target over 2,000 international government entities, specifically mentioning the South Korean Ministry of Tourism, Culture, and Sports. CTIX analysts continue to monitor threat actor activity worldwide and will provide additional updates accordingly.

    ○ The Record: Genesis Day Article
    ○ Recorded Future: Genesis Day Article

Threat Profile: Tomiris Group

Reported in the April 25th, 2023, FLASH Update

- A Russian threat organization has been targeting diplomatic/government entities throughout Central Asia with the objective of intelligence gathering. The group is tracked as Tomiris Group and has been active in the threat landscape since mid-2021, primarily focusing on exploitation of government organizations throughout the Middle East and Southern Asia. Tomiris actors start their attack chain by using either spear-phishing campaigns against employees of the organization, drive-by downloads, or exploiting ProxyLogon vulnerable servers. After the initial point-of-entry, Tomiris actors deploy a variety of malicious trojans and information stealers onto the system. A unique high-level tactic utilized by the group is the deployment of numerous false flag scripts to the victim system, repeatedly deploying them through simplistic distribution protocols. Malware families observed during this campaign include the open-source “WARZONE-RAT”, “Python Meterpreter” or “Roopy” for command-and-control (C2) actions, “Telemiris”, and the “JLORAT” information stealer. Additionally, indicators of compromise and tactics seen in these campaigns from Tomiris show some possible association to the Russian state sponsored Turla organization; however, there is not enough substantial evidence linking the two (2) together. CTIX analysts continue to monitor threat actor activity worldwide and will provide additional updates accordingly.

    ○ Securelist: Tomiris Group

DustSquad Organization Launches Politically Motivated Phishing Campaign

Reported in the April 28th, 2023, FLASH Update

- A group of Russian cyberespionage threat actors have begun targeting Tajikistan individuals with a malicious PaperBug campaign. The group is tracked commonly as DustSquad (Nomadic Octopus) and was a rather quiet threat organization up until now. Specializing in cyberespionage operations, DustSquad primarily targets entities based on political/diplomatic stances and has defaulted to social engineering as the point-of-compromise. The initial point-of-compromise to this recent operation against Tajikistan is unknown; however, DustSquad actors targeted Tajik government bodies, public service providers, and telecommunication companies. Once compromised, DustSquad deployed several toolsets and malicious programs onto the victims’ networks via command-and-control (C2) servers. The main backdoor program that was utilized is called “Octopus” and has the programmatic capabilities to dump Windows system credentials, capture screenshots of the current system, system network information, and sends all information back to actor controlled C2 servers. Attacks carried out during this operation were found to be intrusive and non-stealthy with the intention of general intelligence gathering and surveillance. Operation Paperbug had similar tendencies to that of APT28, another Russian threat organization specializing in espionage efforts against telecommunications in Central Asia. CTIX continues to monitor threat actor activity worldwide and will provide additional updates accordingly.

    ○ ProDaft: DustSquad Article

VULNERABILITIES

Actively Exploited Flaw in WordPress Plugin Allows for Full Site Takeover

Reported in the April 4th, 2023, FLASH Update

- Hackers are actively exploiting a critical vulnerability in Elementor Pro, a popular website builder plugin for WordPress with at least 11 million installs. The flaw was discovered by a researcher from NinTechNet, who published a working proof-of-concept (PoC) exploit at the end of March 2023. The exploit only affects instances of Elementor Pro that are running on a website that has WooCommerce activated. WooCommerce is a very popular open-source software solution used to turn websites into e-commerce shops online. The exploit stems from a broken access control vulnerability which allows any authenticated users visiting the website to make changes to the website's settings, potentially allowing the attacker to conduct a full takeover of the site. If successfully exploited, an authenticated attacker could elevate their privileges to make themselves a website administrator. This would allow them to carry out a number of malicious activities including redirecting all user traffic to an actor-controlled command-and-control (C2) server, as well as uploading backdoors and other malicious code. This vulnerability impacts v3.11.6 and earlier, and CTIX analysts recommend all site administrators leveraging vulnerable instances of Elementor Pro and WooCommerce to upgrade to version 3.11.7 or later as soon as possible.

    - Bleeping Computer: Elementor Pro Vulnerability Article
    - Nin TechNet: Elementor Pro PoC Exploit

Multiple Critical Vulnerabilities in Popular ICS Products and Systems

Reported in the April 7th, 2023, FLASH Update

- On April 6, 2023, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) published seven (7) advisories concerning multiple high-severity vulnerabilities affecting critical Industrial Control Systems (ICS). The flaws impact products and solutions from "Hitachi Energy, mySCADA Technologies, Industrial Control Links, and Nexx." In terms of severity, the vulnerabilities range from CVSS scores of 7.8/10 on the lower end to multiple flaws receiving a score as high as 9.9/10. The majority of the vulnerabilities stem from broken file permission validations and command injection flaws, which could allow attackers to escalate their local system privileges, move laterally across the network, exfiltrate sensitive information, drop malware, remotely execute arbitrary code, and take complete control of vulnerable systems and IoT devices. These vulnerabilities pose great threats to U.S. critical infrastructure and are valuable attack vectors for state sponsored threat actors working with their adversaries. CISA has provided technical details and instructions for all advisories in the alert linked below. CTIX analysts recommend that all administrators and users of the impacted products follow the advisories to prevent future exploitation, whether it be through security patching or via manual mitigation techniques.

    - The Hacker News: CISA Vulnerability Advisory Article
    - CISA: Critical Vulnerability Advisories

CISA Urges Organizations to Patch Critical Vulnerabilities in the Veritas Backup Exec Suite

Reported in the April 11th, 2023, FLASH Update

- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is urging organizations to patch three (3) critical vulnerabilities impacting internet-facing Windows servers running Veritas Backup Exec Installations. Veritas is a data backup and recovery suite that has approximately 8,500 installations according to internet scans. These flaws are being exploited by new ALPHV (aka BlackCat) affiliates tracked as UNC4466 in order to drop the rust-based ransomware. The first vulnerability is tracked as CVE-2021-27876 and is a file access vulnerability that can be exploited via malicious input parameters to take control of a target system. The second flaw, tracked as CVE-2021-27877, is an improper authentication vulnerability that could be exploited by an unauthenticated attacker to authenticate within the system through a SHA authentication scheme. The third flaw, tracked as CVE-2021-27878, is a command execution vulnerability which could allow an attacker to exploit a data management protocol to execute arbitrary code. The UNC4466 attacks were initiated with the Metasploit module "exploit/multi/veritas/beagent_sha_auth_rce", targeting servers running Veritas Backup Exec, and maintaining persistence within the network through Metasploit modules as well. These vulnerabilities impact any instances of Veritas Backup Exec running versions prior to 21.2. CTIX analysts recommend that any organizations running these versions patch their software, as well as conduct manual mitigation techniques like enabling multi-factor authentication (MFA), implementing secure access controls, and segmenting impacted networks. Technical details and indicators of compromise (IOCs) can be found in the report linked below.

  - GBHackers On Security: UNC4466 ALPHV Ransomware Article
  - Mandiant: UNC4466 ALPHV Ransomware Report

Critical Windows Zero-day Exploited in Nokoyawa Ransomware Attacks

Reported in the April 14th, 2023, FLASH Update

- The Cybersecurity and Infrastructure Security Agency (CISA) has added a critical Microsoft Windows zero-day vulnerability to its Known Exploited Vulnerabilities (KEV) catalog. The flaw is being actively exploited by threat actors to conduct Nokoyawa ransomware attacks. The Nokoyawa ransomware group is a financially motivated threat actor first seen in February 2022, and the ransomware is a strain capable of targeting 64-bit Windows systems in double extortion attacks. The flaw, tracked as CVE-2023-28252, is an escalation of privileges (EOP) vulnerability in the Windows Common Log File System (CLFS) that allows attackers to gain SYSTEM privileges on a targeted vulnerable system. The attacks are low complexity, requiring no user interaction, and if successfully exploited, allow the threat actors to conduct a full takeover of targeted Windows systems. The vulnerability affects all supported Windows server and client versions, and its presence on the KEV means that all Federal Civilian Executive Branch (FCEB) agencies must secure their systems against it by May 2, 2023, or face regulatory fines. Microsoft patched this zero-day as part of this month's Patch Tuesday release. Researchers from Kaspersky's Global Research and Analysis Team (GReAT) uncovered the vulnerability in February 2023 as a result of investigations into multiple attempts to execute similar EOP exploits on Microsoft Windows systems. The researchers identified that the Nokoyawa ransomware group has utilized at least five (5) other CLFS exploits to target various industries since June 2022. CTIX analysts urge all Windows users to ensure they have installed the most recent patch to prevent future exploitation.

  - Bleeping Computer: CVE-2023-28252 Article
  - Kaspersky: Nokoyawa Ransomware Attack Report

Google Patches First Actively Exploited Zero-day Vulnerability of 2023

Reported in the April 18th, 2023, FLASH Update

- Google has just released an emergency security update for a critical zero-day vulnerability in the Chrome browser that is being actively exploited by threat actors in the wild. The flaw, tracked as CVE-2023-2033, is a type confusion vulnerability in the V8 JavaScript engine of the Chrome browser. The vulnerability stems from the engine allocating resources using one type but later attempting to access the resource using another type. This causes logical errors because the resources don't have the expected properties, which can lead to out-of-bounds memory access. If successfully exploited, this vulnerability could allow threat actors to crash the target browsers, as well as execute arbitrary code by reading or writing memory out of buffer bounds. The flaw was discovered by a researcher at Google's own Threat Analysis Group (TAG) and, at this time, the technical details of the exploit are being withheld in an attempt to allow as many Chrome users as possible to patch their vulnerable systems. This update patches the desktop versions of the Chrome browser for Windows, Mac, and Linux, and mobile updates will be released in the coming weeks. This is Google's first zero-day vulnerability of 2023, and CTIX analysts recommend that all users ensure their desktop browsers are running the most recent update as well as monitor for the release of the following patches.

  - Bleeping Computer: CVE-2023-2033 Article
  - Dark Reading: CVE-2023-2033 Article
  - Google: CVE-2023-2033 Advisory

Google Patches Zero-day Vulnerability Allowing for Google Account Takeover

Reported in the April 21st, 2023, FLASH Update

- Researchers have published a report detailing the exploitation of a now-patched critical Google Cloud Platform (GCP) zero-day vulnerability, which if exploited, could allow threat actors to install maliciously crafted hidden applications within victims' Google and/or Workspace accounts. The flaw has been coined GhostToken, and stems from an attacker's ability to convert the already authorized OAuth application into a malicious trojan that cannot be seen or removed from a victim's Google account application management page. This is achieved by deleting the GCP project for Oauth, putting it in a hidden "pending deletion" state, while the threat actor modifies and then unhides the application, granting them access to the victim's Google Account by use of the authorized "ghost" Oauth access token. This poses a major threat to companies implementing Google Workspace, as exploitation could allow threat actors to conduct a wide range of malicious activity like viewing and exfiltrating or deleting sensitive company information, as well as sending phishing emails from the victims' compromised accounts. This vulnerability also poses a risk to Google Accounts users in general, as exploitation also allows threat actors to track victim location data, as well as delete data from their Google Calendars, Photos, and Drive. The update to GCP will now show all applications pending deletion in the user application management page. CTIX analysts recommend that all Google Accounts and Workspace users ensure that their software is running the most recent security patch.

  - The Hacker News: GhostToken Article
  - Astrix Security: GhostToken Report

PaperCut Print Management Solution Under Active Exploitation

Reported in the April 25th, 2023, FLASH Update

- A working proof-of-concept (PoC) exploit has been published for an actively exploited critical vulnerability affecting the PaperCut print management software. PaperCut is a powerful print management solution for enabling, tracking, managing, and securing an organization's printing, copying, and scanning needs. The vulnerability, tracked as CVE-2023–27350, was given a CVSS score of 9.8/10 and is a remote code execution (RCE) flaw that allows unauthenticated attackers to execute malicious code on servers running vulnerable versions of PaperCut. Security researchers have reported that two (2) days after the active-exploitation started, threat actors were observed exploiting CVE-2023–27350 to install malicious remote management software from the internet. Once the threat actors had remote control of the targeted servers, researchers observed installation of a malware strain known as “TrueBot”. TrueBot is linked to the notorious Clop ransomware group and their affiliates and was recently deployed to exploit the GoAnywhere vulnerability. Researchers have also observed the exploitation of a related vulnerability, tracked as CVE-2023–27351. This is an authentication bypass vulnerability with a CVSS score of 8.2/10 that could allow unauthenticated attackers to exfiltrate sensitive data. A scan from the Shodan search engine revealed that there are approximately 1,700 PaperCut instances exposed to the public-facing internet, and researchers have reported that approximately 900 of them remain unpatched. The wide availability of vulnerable servers, coupled with the low complexity of the attack, make this flaw particularly troubling. CTIX analysts recommend that all organizations implementing PaperCut NG or MF install the most recent security patch to prevent being targeted by threat actors.

    - Ars Technica: PaperCut Article
    - Horizon3.ai: PaperCut Report
    - Huntress: PaperCut Report

Researchers Attribute the Exploitation of PaperCut Vulnerabilities to Clop Affiliate Lace Tempest

Reported in the April 28th, 2023, FLASH Update

- UPDATE: Researchers from Microsoft have attributed the active exploitation of two (2) critical PaperCut vulnerabilities to threat actors linked to the Clop ransomware operation. A proof-of-concept (PoC) exploit was recently published by researchers, breaking down the vulnerability and giving the technical details for exploitation. The first vulnerability, tracked as CVE-2023–27350, is a remote code execution (RCE) flaw that allows unauthenticated attackers to execute malicious code on servers running vulnerable versions of the very popular PaperCut print management solution. The other vulnerability, tracked as CVE-2023-27351, is an authentication bypass vulnerability that works in conjunction with the RCE vulnerability. The researchers attributed the exploitation to a threat actor tracked as "Lace Tempest", a financially motivated Clop affiliate whose tactics, techniques, and procedures (TTPs) overlap with the FIN11 and TA505 threat actors. In this campaign, the Lace Tempest threat group is exploiting the PaperCut vulnerabilities to install a TrueBot (aka Silence.Downloader) malware loader on vulnerable PaperCut servers. TrueBot aims to infect the victim systems, collecting information to help triage interesting targets, and deploy additional payloads, while sending all relevant intelligence back to an attacker-owned command and control (C2) server. PaperCut produces printing management software for almost every major printer brand, used by government agencies, universities, and large corporations around the world. The Cybersecurity and Infrastructure Security Agency (CISA) has added the vulnerabilities to their Known Exploited Vulnerabilities (KEV) catalog, mandating that all federal civilian executive branch

(FCEB) agencies patch the flaws by May 12, 2023, or face being held accountable by regulators. CTIX analysts will continue to monitor the fallout from this campaign, and further updates may be published if novel findings become public.

- The Record: PaperCut Exploitation Article
- CISA: KEV

HONORABLE MENTIONS

3CX Breach Widens as Second-Stage Backdoor Drops

Reported in the April 4th, 2023, FLASH Update

- UPDATE: The adversary targeting 3CX in a supply-chain attack has employed a second stage backdoor by exploiting CVE-2013-3900, a ten (10) year-old Windows vulnerability. The threat actor has been observed delivering their full-fledged modular backdoor to only a few select companies. This versatile backdoor known as "Gopuram" was deployed on less than ten (10) devices, primarily belonging to cryptocurrency companies. It is still believed that the Lazarus group, a North Korean state-sponsored hacking group, was behind the initial 3CX attack. The precision of the attacks and their specific aim at cryptocurrency companies further ties the North Korean government-backed hackers to the crime, as the sanctions-hit government has a history of targeting cryptocurrencies and other illicit financial assets to help fund their cyber operations. This deployment of a second backdoor aimed specifically at crypto targets helps clarify the intent of the initial attackers and suggests that this was the final payload of the attack chain.

    - Security Week: 3CX Backdoor Article
    - The Hacker News: 3CX Backdoor Article
    - Bleeping Computer: 3CX Backdoor Article

Microsoft's Court Order Grants Them Offensive Capabilities to Combat Cybercrime

Reported in the April 7th, 2023, FLASH Update

- Microsoft finally received the green light to take offensive measures against cybercriminals abusing their software. Working together with the nonprofit Health Information Sharing and Analysis Center (Health-ISAC) and software maker Fortra, Microsoft's Digital Crime Unit (DCU) will go after cracked legacy copies of Fortra's Cobalt Strike which has been abused to wreak havoc on the healthcare industry. Cobalt Strike is an adversary simulator and penetration testing software tool utilized by red teams to proactively find vulnerabilities and prepare for attacks, but cybercriminals have exploited older versions of the software for malicious intents such as distributing malware. Malicious infrastructure hosting Cobalt Strike has been detected in China, the United States, Russia, and other parts of the world, having been linked to sixty-eight (68) ransomware attacks across nineteen (19) countries. After issuing hundreds of Digital Millennium Copyright Act (DMCA) violation notices, this court order finally allows these three (3) entities to collectively pursue cybercriminal servers hosting cracked copies of Cobalt Strike. Microsoft will notify internet service providers (ISPs) and computer emergency readiness teams (CERTs) about command-and-control (C2) servers and other malicious infrastructure leveraging their software in order to take them offline. Disrupting these connections between cybercriminals and infected victim's computers severs the attackers' distribution method and effectively disrupts the criminal ecosystem that exploits the companies' software.

    - The Record: Microsoft Article
    - Bleeping Computer: Microsoft Article
    - The Hacker News: Microsoft Article

Cyberattacks Target Israeli Water Controllers

Reported in the April 11th, 2023, FLASH Update

- The Israeli State was hit with a cyberattack targeting their critical infrastructure. Israel's National Cyber Organization anticipated an influx of threats coming from anti-Israeli hackers during the month of Ramadan, yet that still didn't deter the cyberattack that shut down ten (10) water controllers in the Jordan Valley. The water controllers were down for an entire day as management worked all day Sunday April 4, 2023, to bring the systems back online and into full operation. Cyberattacks with physical consequences have been a looming threat, and their instances are continuing to increase. Attacks on critical infrastructure systems such as water supplies, electric grids, and transportation networks, are increasingly targeted by cybercriminals because of the significant financial damages and geopolitical disruptions they can cause. This attack is another case highlighting the demand for increased cybersecurity monitoring and incident response plans centered around critical infrastructure. Nations such as Russia, Iran, North Korea, and China have threat groups with capabilities that, if executed, would have drastic consequences with potential physical damages and harms to the public.

    - Security Affairs: Israel Article
    - CYBERWARZONE: Israel Article

Secret US Documents Leaked in Private Discord Server Pose Serious Risk to US National Security

Reported in the April 14th, 2023, FLASH Update

- The Pentagon is in the midst of conducting an interagency effort to assess the impact that recently leaked highly classified documents might have on US national security and that of their Allies and partners. The 300 plus photos of classified documents were leaked on a Discord server by the group's leader, alleged to be a man in his early twenties referred to as “OG”. The chat group began as a close-knit group of twenty (20) to thirty (30) individuals who met online during the pandemic, but things shifted as OG started sharing detailed posts with annotations of classified documents. According to his posts in the Discord group, he believed that the US government, law enforcement, and the intelligence community were sinister forces that had overreaching powers and suppressed their citizens. OG's posts didn't pick up much attention from the group until he stopped sending plain-text renderings of the documents and started sending photographs of the classified articles. Members of the group cited that the contents included Ukrainian battlefield charts, Russian-Ukrainian causality tallies, satellite images of Russian missile strikes, North Korean ballistic nuclear missile trajectories, eye-level pictures of the Chinese spy balloon along with diagrams of the technology attached to it, and more. The documents OG uploaded to the Discord server reportedly covered an extensive breadth of military and intelligence reports. It's still unclear how these secret documents started circulating around the world and whether OG shared such documents with individuals outside of the private chat room. While the Pentagon is being careful to certify the validity of the contents within the documents, they have stated that the documents "present a very serious risk to national security and have the potential to spread disinformation." Jack Teixera, a twenty-one (21) year-old who works in the intelligence wing of the Massachusetts Air National Guard, was arrested on Thursday by the FBI for his involvement in leaking massive amounts of secret US documents under his discord alias "OG."

    - Washington Post: Leaked Documents Article
    - Forbes: Leaked Documents Article
    - Associated Press: Leaked Documents Article

- Associated Press: Leaked Documents Article

Microsoft Comes Out with New Threat Actor Naming Taxonomy

Reported in the April 21st, 2023, FLASH Update

- Microsoft recently announced the new naming taxonomy of identifying threat actors by associating them with weather events. This is a change from their previous approach which named threat actors after chemical elements. As threats continue to evolve in complexity and increase in volume, Microsoft sees this as a way to for threat researchers to “instantly have an idea of the type of threat actor they are up against, just by reading the name.” In Microsoft's new taxonomy, nation-state actors will be assigned certain weather conditions. For example, Russia is aligned with Blizzard, China with Typhoon, Iran with Sandstorm, and North Korea with Sleet. Microsoft has assigned four (4) additional weather event "families" to non-state actors based on motivation, using Tempest for financially motivated actors, Tsunami for private sector offensive actors, Flood for influence operations, and Storm for groups in development who don't yet have enough information learned about them to be grouped into another category. For threat actors in the same weather families, an adjective will be added to differentiate them based on differing tactics, techniques, and procedures (TTPs), infrastructure, objectives, and other distinguishing factors. Microsoft's new naming taxonomy is aimed at simplifying the multitude of naming conventions already used amongst the security giants. Especially with the amounts of threat intelligence data that researchers are already confronted with, this new naming convention is seen as a simpler method of tracking and classifying threat groups in a way that's efficient and easy to understand.
    - The Record: Threat Actor Taxonomy Article
    - Microsoft: Threat Actor Taxonomy Article

Cybersecurity Researchers Take Control of a European Space Agency Satellite

Reported in the April 25th, 2023, FLASH Update

- Researchers at Thales just announced their successful joint hacking demonstration where they seized control of a European Space Agency (ESA) satellite. Researchers at Thales and members at ESA specifically orchestrated this satellite hacking exercise in time for the CYSAT conference this week in Paris to showcase the real-world consequences that cyberattacks could have on space systems. This demonstration coincidentally comes soon after highly classified leaked US documents warned about China's development of similar capabilities that could allow them to seize control of satellites they deem to be hostile. The alleged documents shined light on capabilities that shy away from the traditional approach of communication jamming via signal blocking, and instead mimic operator signals that would enable the actor to effectively seize control of a satellite, disallowing support for communications, weapons, surveillance, intelligence, and reconnaissance. Thales performed their demonstration on ESA's OPS-SAT nanosatellite, a satellite about the size of a showbox with “an experimental computer ten times more powerful than any current ESA spacecraft.” While they don't plan to release the hard details of the demonstration until the CYSAT conference, Thales said they were able to hijack a number of ESA satellite systems using traditional cyberattack capabilities. The ethical hackers were able to inject malicious code into the satellite's system by first exploiting its "standard access rights to gain control of its application environment," thus, making it possible to obfuscate data coming back from the satellite, such as imagery, while also concealing any malicious activity to avoid detection. As civilization expands onwards into space, this exercise is an opportunity to raise awareness of flaws and vulnerabilities that exist among the converging sectors of space systems and cybersecurity.

- The Record: ESA Satellite Article
- Financial Post: ESA Satellite Article

Google Granted Court Order to Disrupt CryptBot Info Stealer

Reported in the April 28th, 2023, FLASH Update

- On Wednesday, a federal judge in the Southern District of New York granted Google a temporary court order to disrupt the distribution and infrastructure of the “CryptBot” info stealing malware. The CryptBot info stealer, which is estimated to have infected approximately 670,000 computers in the past year, has been used to infect Google Chrome users and steal their data, including login credentials, credit card information, cryptocurrency wallet data, and other personal or financial data that can be used for fraudulent intents. The malware is traditionally delivered via fake websites that offer "cracked" versions of various software and video games that, in reality, are maliciously modified versions of popular software packages such as Google Earth Pro or Google Chrome. Google originally filed a lawsuit claiming computer fraud and abuse and trademark infringement, targeting CryptBot's infrastructure and distribution network whose major distributors are believed to be based in Pakistan and operate a worldwide criminal enterprise. The court order will enable Google to take down domains associated with CryptBot distribution that are both active and ones registered after the court order was issued, effectively limiting the malware network's growth and decreasing the influx of new infections. Google's court order comes weeks after a similar court order was granted to Microsoft, in coordination with Fortra and the Health Information Sharing and Analysis Center (Health-ISAC), to dismantle servers hosting illegal, legacy copies of Cobalt Strike, signaling an uprise in legal actions that allow companies to take offensive measures against cyber threat actors.
  - Bleeping Computer: Google Article
  - The Hacker News: Google Article