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

January 2023

Washington, DC
2000 K Street NW, 12th Floor
Washington, DC, United States 20006
+1.202.797.1111

Ankura Incident Response Services
Incident@ankura.com | 24/7 Assistance

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 January 2022, originally published in CTIX FLASH Updates throughout Janaury. 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

Louisiana's Largest Medical Complex Discloses Data Breach Associated to October Attack

Reported in the January 3rd, 2023, FLASH Update

- On December 23rd, 2022, the Lake Charles Memorial Health System (LCMHS) began sending out notifications regarding a newly discovered data breach that is currently impacting approximately 270,000 patients. LCMHS is the largest medical complex in Lake Charles, Louisiana, which contains multiple hospitals and a primary care clinic. The organization discovered unusual activity on their network on October 21, 2022, and determined on October 25, 2022, that an unauthorized actor gained access to the organization's network as well as "accessed or obtained certain files from [their] systems." The LCMHS notice listed the following patient information as exposed: patient names, addresses, dates of birth, medical record or patient identification numbers, health insurance information, payment information, limited clinical information regarding received care, and Social Security numbers (SSNs) in limited instances. While LCMHS has yet to confirm the unauthorized actor responsible for the data breach, the Hive ransomware group listed the organization on their data leak site on November 15, 2022, as well as posted files allegedly exfiltrated after breaching the LCMHS network. The posted files contained "bills of materials, cards, contracts, medical info, papers, medical records, scans, residents, and more." It is not unusual for Hive to claim responsibility for the associated attack as the threat group has previously targeted hospitals/healthcare organizations. CTIX analysts will continue to monitor the Hive ransomware group into 2023 and provide updates on the Lake Charles Memorial Health System data breach as necessary.

    - The Record: LCMHS Data Breach Article
    - Bleeping Computer: LCMHS Data Breach Article
    - LCMHS: Cybersecurity Incident Notice

New Phishing Campaign Utilizes Fraudulent Shops "Selling" Flipper Zero Products

Reported in the January 6th, 2023, FLASH Update

- Security-interested members of the Flipper Zero community are being targeted by a new phishing campaign. Flipper Zero is a portable Tamagotchi-like multi-functional cybersecurity tool used to interact with access control systems. Since its Kickstarter campaign was launched in 2020, security researchers have demonstrated the product's capabilities on social media, which generated interest in the infosec community for the release of the product. Threat actors have begun to take advantage of this interest and lack of product availability in 2022 by creating fraudulent Twitter accounts and shops that claim to be selling the product. One (1) of the two (2) currently identified shops is still online as of January 4, 2022, and is claiming to sell the Flipper Zero, the Wi-Fi module, and the case at the same price as the products on the legitimate website. The phishing campaign's apparent goal is to obtain the victims' email addresses, full names, and shipping addresses. The buyers are able to "pay" for the products with Ethereum or Bitcoin cryptocurrency. It is noted that the shop may use new wallets after each transaction, as the wallet on the site as of January 4 has not received any payments. As interest about Flipper Zero remains and the shortage of product continues, it is expected that actors will continue to target the community. CTIX analysts will continue to monitor for newly discovered phishing campaigns and provide context regarding notable incidents.

    - Bleeping Computer: Flipper Zero Article
    - Bitdefender: Flipper Zero Article

Health and Human Services Organization Discloses Ransomware Attack and Breach from Early 2022

Reported in the January 10th, 2023, FLASH Update

- On January 5, 2023, Maternal & Family Health Services (MFHS) disclosed that a ransomware attack occurred on April 4, 2022, and unauthorized actors had access to their systems prior to the attack, specifically since August 21, 2021. MFHS is a private non-profit health and human services organization that serves Northeast Pennsylvania. The organization confirmed that breach notification letters began being sent to those potentially impacted, including former and current employees, patients, and vendors, on January 3, 2023. The information that may have been compromised during the ransomware attack includes, but is potentially not limited to, names, addresses, dates of birth, driver's license numbers, Social Security numbers (SSNs), financial account and payment card data, usernames, passwords, medical information and/or health insurance information. MFHS currently has no evidence that the compromised data has been misused and a ransomware group has yet to be attributed to the April 2022 attack. CTIX analysts will continue to monitor for advancements and update accordingly.
    - The Record: MFHS Breach Article
    - PR Newswire: MFHS Notice of Cybersecurity Incident

New SEO Poisoning Campaign Utilizing "Gootkit" Malware Loader Targets the Australian Healthcare Sector

Reported in the January 13th, 2023, FLASH Update

- The operators of the "Gootkit" malware loader (otherwise known as "Gootloader") have started a new search engine optimization (SEO) poisoning campaign targeting Australian healthcare organizations. This campaign leverages VLC Media Player in order to deploy the post-exploitation toolkit Cobalt Strike onto compromised machines in order to establish initial access into the corporate networks. Trend Micro researchers detailed that the campaign began in October of 2022 and was able to rank highly in Google's search results for medical-related keywords, including "enterprise agreement", "hospital", "medical", and "health" when combined with Australian city names. The websites commonly used in Gootkit campaigns are compromised sites with JavaScript injected to display fraudulent Q&A forums containing links to the malware. The threat actors in this latest campaign are utilizing "a direct download link for what is supposedly a healthcare-related agreement document template inside a ZIP archive." Once the archive is opened by a victim and the JavaScript file is launched, the Gootkit loader malware is downloaded to the machine. The malware downloads an executable that is a legitimate and signed copy of VLC Media Player that is disguised as the Microsoft Distributed Transaction Coordinator (MSDTC) service. The malware also downloads a dynamic linked library (DLL) that is embedded with the Cobalt Strike module. When the executable is launched, a DLL side-loading attack commences that leads to a PowerShell script initiating the final execution chain events that allow the actors to "perform network scans, move laterally throughout the network, steal account credentials and files, and deploy more dangerous payloads such as ransomware." It should be noted that the PowerShell script retrieves data only after a waiting period of a few hours to roughly two (2) days, which is "a distinctive feature of Gootkit loader's operation." Technical analysis as well as indicators of compromise (IOCs) can be viewed in Trend Micro's report linked below.
    - Bleeping Computer: Gootkit Campaign Article
    - The Hacker News: Gootkit Campaign Article

- Trend Micro: Gootkit Campaign Report

PayPal Discloses December 2022 Security Incident Involving Credential Stuffing Attacks

Reported in the January 20th, 2023, FLASH Update

- PayPal has begun sending out notification letters to individuals impacted by a security incident that occurred in early December 2022. On December 20, 2022, PayPal confirmed that unauthorized third-party actors had access to customer accounts using login credentials between December 6 and December 8. The actors obtained access through credential stuffing attacks, in which previously compromised usernames and password pairs are used by actors to attempt to access various accounts. This type of attack is significant to users who use the same password for multiple accounts and do not change their passwords upon being notified of a breach. The actors were able to view and potentially exfiltrate personal information from certain users, which could contain users' names, addresses, Social Security numbers (SSNs), individual tax identification numbers, and/or dates of birth. PayPal emphasized that there is no evidence that any personal information accessed has been misused and there is no evidence that login credentials were obtained from a PayPal system, meaning that their platform was not breached. Approximately 35,000 users have been impacted by this incident and the compromised accounts' passwords have been reset by PayPal. CTIX analysts will continue to monitor for advancements regarding this incident.

    - Bleeping Computer: PayPal Article
    - PayPal: Security Incident Notice

Recent Uptick in Malicious Microsoft OneNote Attachments Identified in Phishing Campaigns

Reported in the January 24th, 2023, FLASH Update

- Security researchers have noted a recent uptick in phishing campaigns utilizing Microsoft OneNote attachments to spread malware. Phishing emails typically contain Microsoft Word documents or Excel files that are embedded with malicious macros as well as ISO images or password-protected ZIP files. With Microsoft disabling default macros, threat actors have turned to OneNote, the digital notebook application included by default in Microsoft Office 2019 and Microsoft 365, which can be used to open the OneNote file format despite not being used by the user. In December 2022, Trustwave SpiderLabs researchers noted actors leveraging Microsoft OneNote documents to spread the "Formbook" malware, an information-stealing trojan sold as malware-as-a-service since mid-2016. Once the attachment was opened, a large "View Document" image was shown over a blurred document that had malicious attachments underneath. When the researchers clicked on the image (and hidden attachments), a Windows Script File (WSF) was executed, and a standard security warning was shown. If a user was to click "OK" on the warning, a decoy OneNote file and an executable containing the malware payload would be downloaded. Threat actors then have the ability to remotely access the compromised device to exfiltrate files, save browser passwords, and take screenshots. Rare cases of recording video with the machine's webcam have also been identified. Additional campaigns have been recently identified leveraging OneNote, including campaigns using DHL shipping notification, invoice, ACH Remittance form, mechanical drawing, and shipping document lures. CTIX analysts urge Microsoft users to be vigilant against suspicious emails and, if an attachment prompts a security warning upon opening, to reevaluate the received email and attachment.

    - Bleeping Computer: Phishing Campaign Article

- Trustwave: Phishing Campaign Article

Mimic Ransomware Identified Abusing Legitimate Windows "Everything" Tool's APIs

Reported in the January 27th, 2023, FLASH Update

- Trend Micro researchers published a new report about "Mimic," a new ransomware that was first observed in June 2022, abusing the Windows Everything tool's APIs. The ransomware is an executable that drops various binaries and a password-protected archive that is disguised as "Everything64.dll". The archive contains the ransomware payload and tools that disable Windows Defender and other legitimate binaries. Once executed, the executable drops and extracts its contents as well as drops a session key file that is used for continuing the encryption process even if it is interrupted. The ransomware is renamed to "bestplacetolive.exe" and all other files are deleted from the %Temp% directory. Mimic has an array of capabilities, such as creating persistence through the “RUN” key, removing indicators, disabling sleep mode and shutdown of the compromised machine, collecting system information, and more. "Everything32.dll", a legitimate Windows filename search engine, is leveraged by Mimic to query specific file extensions and filenames using the tool's APIs in order to retrieve the file's path for encryption. The "Everything_SetSearchW" function is also used to avoid encrypting certain files. Once files have been encrypted, the ".QUIETPLACE" file extension is added and a ransom note is displayed. Mimic is noted to target primarily English and Russian-speaking users and has code similarities with the Conti ransomware builder, which was leaked in March 2022. Some similarities noted by researchers include the enumeration of the encryption modes sharing the same integer for both ransomwares, the port scanning capabilities are based on Conti, and Conti's Windows Share Enumeration code is being used by Mimic. Additional technical details as well as indicators of compromise (IOCs) can be reviewed in Trend Micro's report linked below.

    - Bleeping Computer: Mimic Ransomware Article
    - Trend Micro: Mimic Ransomware Article

THREAT ACTOR ACTIVITY

Kimsuky Threat Actors Target South Korean Policy Experts in New Campaign

Reported in the January 3rd, 2023, FLASH Update

- Threat actors from the North Korean-backed Kimsuky group recently launched a phishing campaign targeting policy experts throughout South Korea. Kimsuky is a well-aged threat organization that has been in operation since 2013, primarily conducting cyber espionage and occasional financially motivated attacks. Aiming their attacks consistently at entities of South Korea, the group often targets academics, think tanks, and organizations relating to inter-Korea relations. In this recent campaign, Kimsuky threat actors distributed spear-phishing emails to several well-known South Korean policy experts. Within these emails, either an embedded website URL or an attachment was present, both executing malicious code to download malware to the compromised machine. One (1) tactic the threat actors utilized was distributing emails through hacked servers, masking the origin IP address(es). In total, of the 300 hacked servers, eighty-seven (87) of them were located throughout North Korea, with the others from around the globe. This type of social engineering attack is not new for the threat group as similar instances have occurred over the past decade. In January 2022, Kimsuky actors mimicked activities of researchers and think tanks in order to harvest intelligence from associated sources. CTIX continues to urge users to validate the integrity of email correspondence prior to visiting any embedded emails or downloading any attachments to lessen the risk of threat actor compromise.
    - Cyware: Kimsuky Article

Threat Profile: Blind Eagle/APT-C-36

Reported in the January 6th, 2023, FLASH Update

- Threat actors associated with the Blind Eagle threat organization (APT-C-36) have recently launched major phishing operations in an apparent resurgence of the group. Active since 2018, Blind Eagle is a financially motivated organization targeting entities throughout various South American countries, including entities within manufacturing, financial, and oil/gas industries. This type of activity has been seen in the apparent resurgence from the group during their recent campaign. Blind Eagle actors launched campaigns with improved infection chains and customized tooling, mainly targeting organizations in Colombia and Ecuador. Phishing emails distributed by threat actors in this campaign generically imitate a government institution and contain a malicious URL and PDF file attachment. Unlike other recent phishing campaigns, Blind Eagle threat actors employ a geofencing protocol to only execute malicious code for users within the allowed area (in this case, Colombia, and Ecuador). Otherwise, the malicious code will not execute and the user will be redirected to a legitimate website of the imitated government entity. The malware, “QuasarRAT”, detonated in this campaign is unusual in the fact that the malware is typically associated with cyber-espionage operations from other threat organizations. Analysis of the embedded code shows that Blind Eagle actors utilized QuasarRAT to gather banking information from these compromised devices, fitting their modus operandi. CTIX continues to monitor threat actor activity worldwide and will provide additional updates accordingly.
    - Checkpoint: Blind Eagle Article

Cold River Threat Actors Target United States Nuclear Research Labs

Reported in the January 10th, 2023, FLASH Update

- Recent research has revealed that Russian threat actors targeted several United States nuclear research laboratories in late summer 2022. The threat actors are tied to the Cold River (Callisto, TAG-53) organization, a Russian state-sponsored group known to commonly conduct cyberespionage operations. It is believed that affiliations between the threat group and the Russian state surfaced when data trails led back to an IT employee in Syktyvkar named Andrey Korinets. Several email addresses tied to Korinets were used in connection with Cold River operations between 2015 and 2020 alongside discussions on several Russian dark web forums. Between August and September of 2022, Cold River launched a social engineering campaign targeting nuclear scientists with fake login portals in an attempt to steal credentials. Specifically, threat actors mimicked copies of the Argonne, Brookhaven, and Livermore National Laboratories login pages and distributed them in their phishing emails. It has not been determined if any further compromise has occurred from this campaign or why these facilities were specifically targeted. Recent activity from the group shows that Cold River registered several domain names imitating non-governmental organizations investigating war crimes in the Russia/Ukraine conflict. CTIX will continue to monitor for any fallout from these campaigns and provide additional updates accordingly.
    - Reuters: Cold River Article
    - Cyware: Cold River Article

Threat Profile: Dark Pink

Reported in the January 13th, 2023, FLASH Update

- An emerging threat organization has shown their presence after targeting military and government organizations throughout Europe and the Asia-Pacific region. Tracked as Dark Pink, this organization has been reportedly active since mid-2021 and is currently not attributed to any other threat affiliates. Activity from Dark Pink actors significantly increased through the back half of 2022 and seven (7) cyber espionage related attacks have been uncovered so far. These espionage attacks targeted two (2) military clusters in Malaysia and the Philippines, a religious organization in Vietnam, and government agencies throughout the region. Tactics, techniques, and procedures (TTPs) observed thus far show that Dark Pink actors utilize social engineering tactics to deliver malicious payloads to victims. Through phishing correspondence(s) posing as an individual applying for an internship, threat actors embedded a hyperlink which brings the victim to a file sharing platform where malicious payloads are downloaded. Prior to infection, the downloaded file(s) communicated back to GitHub and downloaded further malicious scripts to further the infection. As it stands, the same GitHub repository was utilized throughout the cyberespionage attacks. Malicious payloads utilized by the group include “Ctealer”, “Cuck Stealer”, and “KamiKaKaBot”, which were used to infect and exfiltrate sensitive information, capturing audio recordings, and other data from messaging platforms. CTIX continues to monitor threat actor activity worldwide and will provide additional updates accordingly.
    - The Record: Dark Pink Article
    - Group-IB: Dark Pink Article

BackdoorDiplomacy Targets Iranian Government Networks

Reported in the January 20th, 2023, FLASH Update

- Chinese threat actors conducted a cyberespionage campaign targeting Iranian government entities in the second half of 2022. Tracked as BackdoorDiplomacy, these threat actors have been active since 2017 and often target foreign affairs and telecommunications companies throughout Europe, Asia, Middle East, and Africa. In previous operations, these actors utilized several proxy/tunneling tools, a variant of the "Quarian" backdoor, and lateral movement techniques to further their espionage capabilities. This recent cyberespionage campaign was in operation between July 2022 through December 2022 and compromised several Iranian government networks, including the network tied to the Ministry of Foreign Affairs and the Natural Resources Organization. BackdoorDiplomacy actors utilized variants of the "Turian" backdoor which included upgraded obfuscation tactics, decryption algorithms, and the ability to execute remote commands and spin up reverse shells. As this cyberespionage campaign aged on, the threat actors continued to update their Turian backdoor variant to adapt to new environments and establish stealthy command-and-control (C2) communications. CTIX continues to monitor threat actor activity worldwide and will provide additional updates accordingly.
    - Cyware: BackdoorDiplomacy Article

Vice Society Shifts to Targeting Manufacturing with Custom Ransomware Variant

Reported in the January 24th, 2023, FLASH Update

- Threat actors from the Vice Society group have opened the new year by targeting organizations throughout the manufacturing industry with a variety of attacks. Vice Society is a Russian-speaking threat group that historically targeted the healthcare industry in their ransomware operations, among other attacks. Recently, Vice Society has shifted to exploiting manufacturing organizations with custom ransomware scripts developed with advanced encryption methods. The typical flow of these attacks commonly begins with Vice Society actors exploiting vulnerable public-facing software or using compromised credentials sold on dark web marketplaces. Once compromised, threat actors deploy Cobalt Strike to control and maintain the infected endpoint, followed by the installation of several other malicious scripts for lateral network movement, credential dumping (Mimikatz) and copying of files (Kape). Occasionally Vice Society will deploy the Zeppelin ransomware strain, but often opt to use custom ransomware as Zeppelin's encryption is weaker. Since November 2022, Vice Society activity has been detected throughout thirty-four (34) manufacturing organizations, all of which appear to reside in Brazil. Activity from the Vice Society organization is predicted to continue in the months to come across several industries including communications, healthcare, insurance, and manufacturing. CTIX continues to monitor threat actor activity worldwide and will provide additional updates accordingly.
    - TrendMicro: Vice Society Article

Hive Ransomware Seized, Decryption Keys Released to Victims

Reported in the January 27th, 2023, FLASH Update

- A major ransomware enterprise was disrupted on Thursday as a result of a joint task force operation by the Federal Bureau of Investigation (FBI), Department of Justice (DOJ), US Secret Service (USSS), and other international agencies. Hive Ransomware's leak sites was seized by authorities

and currently displays the statement [translated from Russian] "The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against Hive Ransomware." One (1) of the significant reasons Hive Ransomware was targeted for seizure was due to their repeated attacks against hospitals and healthcare centers throughout the world. One (1) attack carried out in Midwestern United States caused a hospital to turn away sick patients after ransomware was deployed on their systems. Another attack didn't compromise the integrity of hospital systems, but Hive actors exfiltrated sensitive patient data on 270k individuals from hospital systems. According to the DOJ, the FBI had successfully infiltrated Hive systems back in July 2022 and captured decryption keys for over a thousand victims, releasing them for free. This act alone saved victims from paying over $130 million in ransom demands. While Hive Ransomware operations may be disrupted for now, a rebranding or reemergence is predictable alongside minimal disruption of the entire ransomware landscape. CTIX continues to monitor fallout from the Hive Ransomware seizure and will continue to provide additional updates accordingly.

- Department of Justice: Hive Ransomware
- TheRecord: Hive Ransomware

VULNERABILITIES

Netgear Patches Critical Vulnerability Leading to Arbitrary Code Execution

Reported in the January 3rd, 2023, FLASH Update

- Network device manufacturer Netgear has just patched a high-severity vulnerability impacting multiple WiFi router models. The flaw, tracked as CVE-2022-48196, is described as a pre-authentication buffer overflow security vulnerability, which, if exploited, could allow threat actors to carry out a number of malicious activities. These activities include stealing sensitive information, creating Denial-of-Service (DoS) conditions, as well as downloading malware and executing arbitrary code. In past attacks, threat actors have utilized this type of vulnerability as an initial access vector by which they pivot to other parts of the network. Currently, there is very little technical information regarding the vulnerability and Netgear is temporarily withholding the details to allow as many of their users to update their vulnerable devices to the latest secure firmware. Netgear stated that this is a very low-complexity attack, meaning that unsophisticated attackers may be able to successfully exploit a device. CTIX analysts urge Netgear users with any of the vulnerable devices listed in Netgear's advisory to patch their device immediately.

    - The Record: CVE-2022-48196 Article
    - Bleeping Computer: CVE-2022-48196 Article
    - Netgear: CVE-2022-48196 Advisory

Synology Patches Multiple Critical Vulnerabilities

Reported in the January 6th, 2023, FLASH Update

- In a published advisory, networking device manufacturer Synology stated that it patched a critical remote code execution (RCE) vulnerability affecting their VPN Plus Server solution for Synology Router Manager (SRM). The flaw, tracked as CVE-2022-43931, received the maximum severity with a CVSS score of 10/10. The vulnerability is described as an out-of-bounds write flaw specifically impacting the remote desktop functionality and could be exploited by threat actors to remotely execute arbitrary code and commands on the target system. VPN Plus is an add-on package that enables Synology NAS devices to become VPN servers, allowing Synology DiskStation Manager (DSM) users over the internet to securely access the resources shared in a Synology device's network. Successful exploitation of this vulnerability could allow threat actors to completely take over a vulnerable system and carry out devastating follow-on attacks. A week prior to Synology's RCE advisory, the company released a patch advisory for multiple other vulnerabilities (some were demonstrated at the December 2022 Pwn2Own contest) which could allow remote attackers to execute arbitrary commands, conduct denial-of-service (DoS) attacks or read arbitrary files after exploiting a vulnerable version of SRM. These are very low-complexity attacks which could be exploited by unsophisticated threat actors. To prevent exploitation of any of the vulnerabilities, CTIX analysts urge all SRM users to immediately update to the latest secure version of their device firmware. Specific details surrounding the updates can be found in the Synology advisories linked below.

    - The Hacker News: CVE-2022-43931 Article
    - Synology: CVE-2022-43931 Advisory
    - Synology: Multiple Vulnerabilities Advisory

Okta Autho Patches Critical RCE Vulnerability Impacting a Very Prolific Open-Source Library

Reported in the January 10th, 2023, FLASH Update

- A critical remote code execution (RCE) vulnerability has been patched in the popular JsonWebToken open-source encryption library maintained by Okta Autho. The library is downloaded from Node Package Manager (NPM), a free library and registry for the publishing of JavaScript software packages utilized by developers. Specifically, JsonWebToken is utilized to digitally create, sign, and verify a JSON Web Token (JWT), the open-source standard defining how to securely transmit information between parties as a JSON object. The vulnerability, tracked as CVE-2022-23529, is described as an input validation flaw. A threat actor could exploit this vulnerability by manipulating the "secretOrPublicKey" argument in JsonWebToken's verify() method, used to verify and return the unencrypted information. This can be carried out via maliciously crafted code input, allowing the attacker to gain control over a key retrieval parameter to take over accounts, impersonate users, steal sensitive information, and elevate privileges to carry out malicious follow-on activity. Although it is rated as high severity, the flaw received a CVSS score of 7.6/10 due to the fact that the attacker would still need to compromise the key management process between an application and a JsonWebToken server before being able to exploit this vulnerability. With an estimated 36 million NPM downloads per month, the popularity of the JsonWebToken poses a massive risk to supply chains. The patch implements additional checks for the "secretOrPublicKey" parameter, and CTIX analysts urge all JavaScript developers dependent on the library to upgrade to the secure version immediately.

    - Bleeping Computer: CVE-2022-23529 Article
    - Dark Reading: CVE-2022-23529 Article
    - GitHub: CVE-2022-23529 Advisory

CISA Adds Windows EOP Vulnerability to the KEV

Reported in the January 13th, 2023, FLASH Update

- The Cybersecurity and Infrastructure Security Agency (CISA) has added a critical Microsoft zero-day vulnerability to the Known Exploited Vulnerabilities (KEV) Catalog, mandating that all Federal Civilian Executive Branch (FCEB) agencies patch the flaw no later than January 31, 2023. The vulnerability, tracked as CVE-2023-21674, is a Windows Advanced Local Procedure Call (ALPC) elevation of privilege (EOP) vulnerability. ALPC is an inter-process message-passing protocol allowing applications to access APIs and services, as well as make Remote Procedure Calls (RPC), requesting services from programs located in another system on a network. If successfully exploited, an attacker could perform a sandbox escape, escalating their local privileges to SYSTEM, giving them the permissions they need to carry out follow-on attacks. Once an actor has escalated their privileges, they could make configuration changes, view sensitive data, and create more privileged user accounts, as well as download malicious programs. EOP vulnerabilities are usually exploited in tandem with malware, as well as other vulnerabilities like remote code execution (RCE). This flaw affects millions of organizations across the world, and due to its low complexity, it can be exploited without any victim user interaction. CTIX analysts urge all Windows users to update to the most recent secure patch immediately to prevent exploitation.

    - The Record: CVE-2023-21674 Article
    - CISA: KEV Advisory

Hackers Exploiting a Critical Vulnerability in ManageEngine Products by Zoho

Reported in the January 20th, 2023, FLASH Update

- Security researchers at Rapid7 have published a blog post warning that they have observed the active exploitation of a critical vulnerability affecting specific ManageEngine on-premise products by Zoho. ManageEngine is an IT service management solution used by hundreds of companies for monitoring and managing all of the hardware and software devices on their networks. The flaw, tracked as CVE-2022-47966, is a pre-authentication remote code execution (RCE) vulnerability stemming from a vulnerable third-party dependency on Apache Santuario for XML signature validation. Specifically, the flaw is exploitable if a user has enabled Security Assertion Markup Language (SAML) single-sign-on, authorizing access to multiple web applications with a single credential set. Attackers could exploit this vulnerability by issuing an HTTP POST request that contains a maliciously crafted SAML response, allowing for RCE. If successfully exploited, an attacker could take complete control of the system that a vulnerable ManageEngine project is running on, steal credentials, deploy malware, and pivot laterally across the network. This product is very popular, being utilized by nine (9) out of every ten (10) Fortune 100 companies, making these vulnerable organizations a very lucrative target for threat actors. Researchers from Horizon3.ai have published a working proof-of-concept (PoC) for exploiting this vulnerability and state that the attack is easy to exploit, making it even more likely that there will be exploitation attempts by sophisticated nation state hackers, financially motivated threat groups, and unsophisticated attackers with limited skills. This vulnerability was patched in October and November of 2022, and CTIX analysts recommend that organizations leveraging any of the products listed in ManageEngine's security advisory upgrade their infrastructure immediately to prevent exploitation attempts.

    - Horizon3.ai: CVE-2022-47966 PoC Exploit
    - ManageEngine: CVE-2022-47966 Advisory
    - The Record: CVE-2022-47966 Article

High Severity iOS Flaw Allows for RCE on Older Vulnerable Models

Reported in the January 24th, 2023, FLASH Update

- Apple has patched an actively exploited critical iOS zero-day vulnerability affecting older models of the iPhone, iPad, and iPod touch devices. The flaw, tracked as CVE-2022-42856, is described as a type confusion bug impacting the browser engine in Apple's Webkit browser. Attackers could exploit this flaw by socially engineering a victim into clicking a link to a maliciously crafted actor-controlled website. Successful exploitation would give attackers the ability to conduct arbitrary remote code execution (RCE) on the vulnerable operating system, from which they could perform further malicious activity like moving laterally across the network, creating privileged user accounts, and dropping malware or ransomware payloads. Due to its active exploitation, The Cybersecurity and Infrastructure Security Agency (CISA) added this vulnerability to its Known Exploited Vulnerability (KEV) catalog, mandating that all Federal Civilian Executive Branch (FCEB) agencies patch the flaw no later than January 4, 2023. At this time, Apple has not released the technical details of the exploit, allowing as many of their users to upgrade their operating systems as possible. With the exploitation relying on an older model iOS device, it is likely that any active exploitation attempts were highly targeted. That being said, CTIX analysts urge any and all iOS customers still using the devices listed in Apple's advisory, to upgrade their operating systems immediately to prevent exploitation.

- Bleeping Computer: CVE-2022-42856 Article
- Apple: CVE-2022-42856 Advisory
- CISA: KEV

Malicious Botnets Leveraged Against Vulnerable Supply Chain Network Infrastructure

Reported in the January 27th, 2023, FLASH Update

- Security researchers stated in a new report that they have observed a sharp uptick in the exploitation of a years old remote code execution (RCE) vulnerability affecting the Realtek Jungle SDK. Realtek Jungle chipsets have become a staple in hundreds of routers, switches, and other IoT devices used by supply-chain organizations across the world. Only days after the flaw was originally disclosed in August 2021, researchers and security personnel observed as many as 1 million vulnerable devices being attacked at one time. By December 2022, researchers stated they observed approximately 134 million exploitation attempts, and that the attack is still ongoing. The vulnerability, tracked as CVE-2021-35394 (CVSS 9.8/10), is a combination of memory corruption and command injection flaws in a Realtek Jungle SDK diagnostic tool called "MP Daemon", and compiled as a "UDPServer" binary. The exploitation of this vulnerability is being leveraged by multiple malicious botnet variants, mainly Mirai, Gafgyt, Mozi, and derivatives of them, as well as a new GO-based botnet known as "RedGoBot", leveraged in distributed denial-of-service (DDoS) attacks. These botnets have been observed delivering three (3) different malware payloads. Supply-chain vulnerabilities pose an especially lucrative opportunity for threat actors, and the nature of the supply chain itself often leaves it very vulnerable. This flaw was patched in August 2021; however, depending on the organization's part in the supply chain, shutting down operations to update their infrastructure could cause a critical loss to business or even threaten national security. CTIX analysts urge any administrators responsible for vulnerable infrastructure to begin developing a plan for patching this flaw that will impact operations the least, through rolling updates where the organization is patched piece-by-piece. The exploitation of this flaw is expected to stay high throughout the beginning of 2023, and CTIX analysts will continue to monitor this campaign.

    - Bleeping Computer: CVE-2021-35394 Article
    - Unit 42: CVE-2021-35394 Report