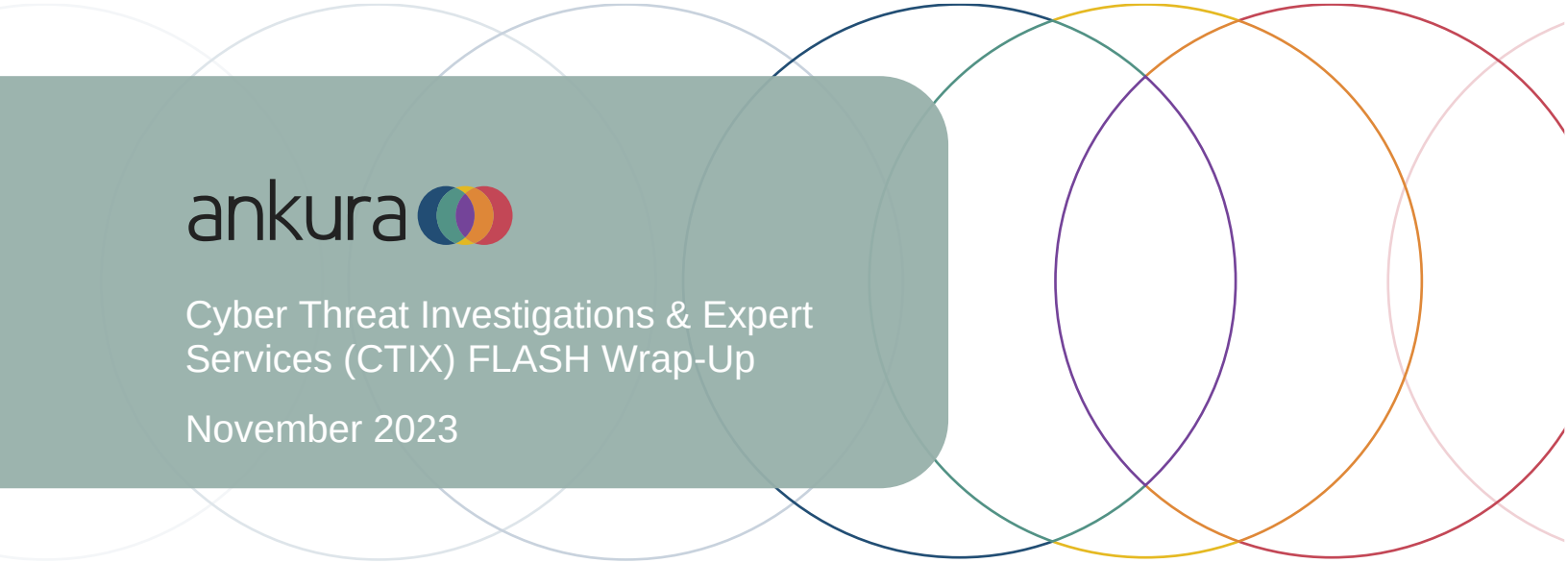

ankura

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

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

North Korean State Sponsored Threat Actors Target Blockchain Engineer Computers with KANDYKORN Malware

Reported in the November 3rd, 2023, FLASH Update

- In what appears to be a continuation of the North Korean strategy to finance the nation using international organized crime rings, cybersecurity researchers established a link between a new malware targeting blockchain engineers and the North Korean state sponsored Lazarus group. Researchers noted that the new malware, which is being used to target the Apple devices of blockchain engineers, shares tactics, techniques, and procedures (TTPs) with the Lazarus group. Researchers stated that these engineers were targeted likely in order to steal cryptocurrency to finance the state's operations and avoid sanctions. Initial access to the systems was achieved through the use of a Python application that was sent to victims through a Discord server used by blockchain engineers. The Python application was supposedly to be used as a cryptocurrency bot that makes transactions automatically based on price differentials throughout the crypto marketplace. This application targets macOS devices and attempted to drop malware the researchers call KANDYKORN. This malware can access and exfiltrate data from the infected device while connecting back to a command-and-control (C2) server to continually upload, execute, and exfiltrate data and programs while avoiding detection. According to researchers, the campaign began in April 2023 and continues into November. Ankura will continue to monitor this ongoing malware campaign.

    - The Record: KANDYKORN Malware Article
    - Cryptonews: KANDYKORN Malware Article

Researchers Detail Dropper-as-a-Service Operation "SecuriDropper" Bypassing Android's "Restricted Settings" Feature

Reported in the November 7th, 2023, FLASH Update

- Researchers have published a new report detailing "SecuriDropper", a Dropper-as-a-Service (DaaS) operation that has been observed bypassing the "Restricted Settings" security measure introduced in Android 13 by Google. The "Restricted Settings" measure was created to restrict privileges that allow the sideloading of applications (typically from sources other than the legitimate Google Play Store). Researchers detailed that the "Restricted Settings" feature prevents sideloaded applications from requesting Notification Listener access as well as accessibility settings, which are commonly sought out and abused by malware. Droppers are primarily used for installing a payload on a compromised device and are notorious for allowing threat actors the ability to "separate the development and execution of an attack from the installation of malware." DaaS operations offer a two (2) stage process that increases the difficulty of detection. The first stage of this process involves the distribution of a malicious application that appears legitimate, which installs the secondary payload onto the device. SecuriDropper utilizes a different Android API than its predecessors to install its payload, which is noted as "mimicking the process used by marketplaces to install new applications." Researchers explained that, with this specific API, the compromised device's Operating System cannot differentiate between the fraudulent application and a legitimate marketplace, which allows the malicious application to bypass "Restricted Settings". Technical details of the SecuriDropper DaaS operation as well as indicators of compromise (IOCs) can be viewed in the report linked below.

    - The Hacker News: SecuriDropper Article
    - Threat Fabric: SecuriDropper Report

New Malvertising Campaign Spotted Disguising as Legitimate Windows News Portal

Reported in the November 10th, 2023, FLASH Update

- A new malvertising campaign has been identified disguising as the legitimate Windows news portal "WindowsReport[.]com" to distribute a malicious installer for the "CPU-Z" processor tool. The campaign is noted to be a part of a large-scale malvertising campaign that has been observed targeting other applications, such as Notepad++, Citrix, and VNC Viewer. Researchers identified a malicious ad at the top of provided search results when searching for "cpu-z", which is a common utility for Windows end-users for troubleshooting their machine. If clicked, the malicious ad redirects the user to a domain impersonating WindowsReport[.]com and uses content directly from the legitimate portal. Researchers emphasized that several additional domains are hosted on the same IP address that are also used in malvertising campaigns. The campaign's payload is a digitally signed installer that contains a loader known as "FakeBat". The loader contains a remote payload for "Redline Stealer" as well. CTIX analysts will continue to monitor malvertising campaigns as they continue to evolve. Indicators of compromise (IOCs) can be viewed in the report linked below.
    - The Hacker News: Windows News Portal Campaign
    - Malwarebytes Labs: Windows News Portal Campaign

BiBi-Linux Wiper Variant "BiBi-Windows Wiper" Identified

Reported in the November 14th, 2023, FLASH Update

- Researchers have discovered "BiBi-Windows Wiper", a Windows-based variant of the "BiBi-Linux Wiper" malware targeting systems in cyberattacks aimed at Israel by a pro-Hamas hacktivist group. Researchers noted that the original Linux-based malware is an x64 ELF executable that currently lacks obfuscation or protective measures. The malware is able to "specify target folders and can potentially destroy an entire operating system if run with root permissions." Additionally, BiBi-Windows Wiper deletes all shadow copies from the system and is multithreaded for increased speed. The Windows variant being established quickly after the Linux-based wiper leads researchers to believe that the campaign is expanding to target end user machines as well as application servers. Researchers emphasized that the current campaign is primarily centered around Israeli IT and government sectors and tactical overlaps between "the hacktivist group, who call themselves Karma, and another geopolitically motivated actor codenamed Moses Staff" were identified. The current infection vectors of both BiBi wipers are currently unknown. Indicators of compromise (IOCs) as well as additional technical details can be found in the report linked below.
    - The Hacker News: BiBi-Windows Article
    - BlackBerry: BiBi-Windows Wiper Report
    - The Hacker News: BiBi-Linux Wiper Article
    - Security Joes: BiBi-Linux Wiper Report

Perry Johnson & Associates Discloses Data Breach Involving PII and PHI of 9 Million Individuals

Reported in the November 17th, 2023, FLASH Update

- Perry Johnson & Associates (PJ&A), a provider of transcription services to healthcare providers in the United States, has disclosed a data breach impacting 9 million individuals following a cyberattack that occurred in March of 2023. In their data breach notice, PJ&A stated that an

unauthorized third-party gained access to the PJ&A network between March 27, 2023, and May 2, 2023, and exfiltrated copies of specific files from their systems. The organization detailed that the files contained personal health information (PHI) belonging to certain individuals and varied per person. Overall, the following information was exposed: name, date of birth, address, medical record number, hospital account number, admission diagnosis, and dates/times of services. For a portion of impacted individuals, Social Security numbers (SSNs), insurance information, and clinical information from medical transition files (such as laboratory and diagnostic testing results, medications, name of treatment facility, and name of healthcare providers) were also exposed. PJ&A confirmed that the data accessed by the threat actor did not contain credit card information, bank account information, usernames, or passwords. There is currently no evidence, according to PJ&A, that the exposed information has been misused "for the purpose of committing fraud or identity theft." CTIX analysts will continue to monitor activity surrounding PJ&A's data breach and will provide updates when available.

- Bleeping Computer: Perry Johnson & Associates Article
- Perry Johnson & Associates: Data Breach Notice

The BORN Ontario Healthcare Organization Discloses Data Breach Due to MOVEit Campaign

Reported in the November 21st, 2023, FLASH Update

- The Better Outcomes Registry & Network (BORN) Ontario healthcare organization has disclosed a data breach impacting approximately 3.4 million individuals. BORN Ontario is a "perinatal and child registry that collects, interprets, shares and protects critical data about pregnancy, birth and childhood in the province of Ontario." The organization, in a cybersecurity incident notice, stated that the breach was caused by the Progress MOVEit campaign that exploited the zero-day vulnerability tracked as CVE-2023-34362 and noted that unauthorized copies of files containing personal health information (PHI) was exfiltrated. The impacted PHI was obtained from a "large network of mostly Ontario health care facilities and providers regarding fertility, pregnancy, newborn and child health care offered between January 2010 and May 2023" and those impacted were described as individuals seeking pregnancy care and newborns born in Ontario between January 2010 and May 2023. The stolen information includes the following data types: full name, home address, postal code, date of birth, and health card number. The following data was exposed for particular care treatments: dates of service/care, lab test results, pregnancy risk factors, type of birth, procedures, and pregnancy/birth outcomes. BORN Ontario emphasized that there is currently no evidence of misuse and no signs of the exfiltrated data being posted or offered for sale on the dark web. CTIX analysts will continue to monitor the BORN Ontario data breach and organizations impacted by the Cl0p MOVEit campaign.
    - Bleeping Computer: BORN Ontario Data Breach Article
    - BORN Ontario: MOVEit Cybersecurity Incident Notice

macOS Targeted with Atomic Stealer Malware in ClearFake Campaign

Reported in the November 28th, 2023, FLASH Update

- The “ClearFake” malicious browser update campaign has continued its spread and is now targeting macOS devices with Atomic Stealer (AMOS) malware. According to researcher Randy McEoin, the ClearFake campaign began back in July of 2023. ClearFake is using non-obfuscated JavaScript on a variety of websites to create a fake pop-up window that informs the user they need to download the latest version of Google Chrome for security updates. This tricks users into

thinking they need to download browser updates, thereby causing the victims to download malware and other targeted payloads. The original malware was using JavaScript to create the fake pop-up and a clickable button that redirected users to a malicious OneDrive file that would load the Amadey trojan to the device. As of November 17, 2023, the ClearFake campaign has expanded to include macOS devices by employing the same tactics previously seen targeting Windows devices. JavaScript is used to create a fake webpage that implores the user to download the latest Safari web browser version, but it instead deploys a payload of Atomic, an information stealing piece of malware. Atomic is capable of harvesting numerous pieces of information from a victim device, including passwords and credit card information stored in browser, crypto currency files, keychain passwords, financial information, and even WiFi passwords. Bleeping Computer reports that approximately 50% of antivirus software is still struggling to identify Atomic once loaded. CTIX analysts will continue to provide updates and monitor the situation and malware payloads utilized by ClearFake.

- Bleeping Computer: Atomic Stealer Article
- The Hindu: Atomic Stealer Article

THREAT ACTOR ACTIVITY

Iranian State Sponsored Threat Actor MuddyWater Conducts Cyber Espionage Campaign Against Israel

Reported in the November 3rd, 2023, FLASH Update

- MuddyWater, an Iranian state-sponsored threat actor, has initiated a spear-phishing campaign against Israeli targets utilizing a tool from N-able, the legitimate administration tool for remote access known as Advanced Monitoring Agent. This marks a shift in the tactics, techniques, and procedures (TTPs) used by MuddyWater (Mango Sandstorm, Static Kitten), but reflects a consistent strategy in their operations. Researchers from multiple cybersecurity firms reported on the campaign, describing a new file-sharing service used for executing multi-stage attacks. These attacks involve sending emails with malicious attachments to deploy remote administration tools, enabling the attackers to perform network reconnaissance. MuddyWater has also developed a new command-and-control (C2) framework known as MuddyC2Go. MuddyWater, active since 2017 and a vital part of Iran's Ministry of Intelligence and Security, continues to evolve its methods while using similar modes of operation with a history of success. The latest incidents feature the use of legitimate remote administration software and sophisticated infection techniques, underlining the growing risk posed by the threat actors and the broader advancements in Iran's cyber threat capabilities.

    - The Hacker News: MuddyWater Campaign Article
    - Deep Instinct: MuddyWater Campaign Report

BlackCat Ransomware Gang Claims Breach on Healthcare Giant

Reported in the November 7th, 2023, FLASH Update

- The BlackCat ransomware group (otherwise known as ALPHV) has recently claimed that they have successfully compromised the networks of the major United States healthcare solutions provider Henry Schein. Henry Schein disclosed mid-October 2023 that they had experienced a cyberattack affecting their manufacturing and distribution operations, which required the organization to take some of their systems offline. The company proceeded by involving law enforcement as well as additional external experts to assist with containing the attack, and recommended that customers place orders through their specified Henry Schein representative or through the company's tele-sales phone number. Approximately two (2) weeks later, BlackCat added Henry Schein to their dark web leak site claiming to have access to thirty-five (35) terabytes of sensitive data, including payroll data and shareholder information. Citing failed ongoing negotiations, the threat actors claimed to have re-encrypted the company's devices as Henry Schein was in the process of restoring their systems. After releasing internal payroll data and shareholder folders, the published data and company’s overall entry were deleted from the leak site, indicating a settlement has been reached or that new ransom negotiations are underway. CTIX analysts will continue to monitor BlackCat’s activity and release updates when applicable.

    - Bleeping Computer: BlackCat/ALPHV Article
    - Tech Radar: BlackCat/ALPHV Article

North Korean Threat Group BlueNoroff Observed Utilizing New macOS Malware Strain

Reported in the November 10th, 2023, FLASH Update

- BlueNoroff (otherwise known as Saphire Sleet or APT38), a North Korean-linked hacking group, has been attributed to targeting financial institutions with a new undocumented malware strain targeting macOS. BlueNoroff is an advanced persistent threat (APT) group that is a subgroup of North Korea's notorious Lazarus Group. Having been first recognized in 2014, the threat group is known to run typical North Korean cyber campaigns focused on attacking financial institutions, cryptocurrency companies, and military entities in leu of growing their nuclear weapons and ballistic missile programs. As part of their larger "RustBucket" malware campaign, BlueNoroff's current financially motivated attacks have targeted cryptocurrency exchanges, venture capital firms, and banks with a starkly simplistic new malware called “ObjCShellz”. The initial access vector is currently unknown; however, it is presumed the malware is delivered through social engineering attacks where attackers disguise themselves as potential partners, investors, or headhunters, which is common in the RustBucket campaign. The malware was not initially present on VirusTotal, but later had submissions in September and October of 2023 originating from Japan and the United States. A domain in the code appears to be linked to a cryptocurrency company, showing communication with a typosquat domain of the cryptocurrency exchange “swissborg[.]com/blog”. This is common practice for the threat actor based on the patterns of previous attacks where the attacker creates a domain looking to be a legitimate crypto or financial company to blend in with network activity. CTIX analysts will stay up to date with relevant updates concerning this campaign.
    - The Record: BlueNoroff Article
    - The Hacker News: BlueNoroff Article

New “Hunters International” Ransomware Group Observed Using Hive's Source Code and Infrastructure

Reported in the November 14th, 2023, FLASH Update

- After being shut down by the Federal Bureau of Investigation (FBI) and other international law enforcement agencies in January of 2023, the notorious Hive ransomware group appears to have sold their source code and infrastructure to a new ransomware group called Hunters International. The now-dismantled Hive Ransomware-as-a-Service (RaaS) operation had an estimated 1,500 targets worldwide, amassing upwards of $100 million in ransom payments and being known to target hospitals, school districts, and financial institutions since their founding in June of 2021. The threat actors associated with the emerging Hunters International have been working to dispel speculations about them being a rebrand of Hive, letting it be known that they purchased the source code and websites from the previous developers to benefit the kick-off of Hunters International's own pursuits in the threat landscape business. Upon analyzing the group's operations, researchers have found Hunters International's ransomware code to be noticeably more simplistic, having "reduced the number of command line parameters, streamlined the encryption key storage process, and made the malware less verbose compared to earlier versions." Having five (5) victims already, it appears that Hunters International is aligning themselves to be a more data exfiltration centric group with less of a focus on data encryption. While there's a significant advantage to having a mature toolkit in their possession, it's unclear what the future holds for Hunters International as well as whether they'll be able to prove their competence. CTIX analysts will continue to monitor relevant threat actor developments and provide updates as operations evolve.
    - The Hacker News: Hunters International Article
    - Bit Defender: Hunters International Report

New Joint Advisory Released by CISA and FBI in Wake of Recent Rhysida Ransomware Attacks

Reported in the November 17th, 2023, FLASH Update

- The Rhysida ransomware gang has been observed partaking in opportunistic attacks recently, leveraging Rhysida ransomware against 'targets of opportunity,' targeting organizations across a range of industries, such as the education, healthcare, manufacturing, information technology, and government sectors. The Federal Bureau of Investigation (FBI) and the US Cybersecurity and Infrastructure Security Agency CISA), along with the Multi-State Information Sharing Agency Center (MS-ISAC), released a joint advisory on November 15th, 2023 in response to these attacks taking place as well in the wake of the US Department of Health and Human Services (HHS) warning that many of the recent attacks on healthcare organizations were the fault of the Rhysida threat actors. Rhysida operates as a Ransomware-as-a-Service (RaaS) model, compromising organizations and splitting ransom payments among affiliates, engaging in double extortion tactics where a ransom is demanded to decrypt victims' data and avoid leaking exfiltrated data. They've been around since May 2023, quickly making a name for themselves after breaching and leaking the stolen data of the Chilean Army. The advisory includes indicators of compromise (IOCs), detection info, and Rhysida tactics, techniques, and procedures (TTPs) observed during investigation. Rhysida threat actors have been observed using phishing attacks, exploiting the Zerologon vulnerability (CVE-2020-1472) to gain initial access and persistence within a network, and hacking into external-facing remote services like VPNs when targeting organizations that didn't have Multi-Factor Authentication (MFA) enabled. The joint advisory also highlighted that Vice Society ransomware group affiliates (aka Vanilla Tempest or DEV-0832) had been recorded shifting to the use of Rhysida ransomware payloads in their attacks starting in July 2023. CTIX analysts recommend that administrators patch actively exploited vulnerabilities and enable MFA across all services, among other recommendations noted in the joint advisory.
    - The Hacker News: Rhysida Article
    - Bleeping Computer: Rhysida Article
    - CISA/FBI: Rhysida Advisory

Researchers Detail Recent ShadowSyndicate Activity in New Report

Reported in the November 21st, 2023, FLASH Update

- A new threat actor group known as ShadowSyndicate, formerly known as Infra Storm, has recently come onto the scene using a wide variety of ransomware families in the past year. The threat actor has been linked to ransomware such as Quantum, BlackCat, Cl0p, Cactus, Nokoyawa, Play, and Royal. They are also known to deploy tools such as Cobalt Strike, Sliver, and IcedID in conjunction with their use of ransomware. The infrastructure for this threat group was discovered and mapped by researchers using an SSH fingerprint that was then traced to eighty-five (85) different servers. Of those eighty-five (85), fifty-two (52) of them were identified as being used as command-and-control (C2) servers for Cobalt Strike. Researchers also described how many of these servers are being attributed to multiple types of ransomwares, noting that the infrastructure appears to be shared between the different Ransomwares-as-a-Service (RaaS). Researchers also noted that there were IP addresses and past SSH clusters from ShadowSyndicate that were linked to Cl0p, indicating that there is possibly a connection between the two (2) threat groups or that they are sharing infrastructure. The identified servers were primarily located in Central America and Europe, specifically Panama, Cyprus, and Russia. CTIX analysts will continue

to monitor the activity of this new group as well as their evolving tactics, techniques, and procedures (TTPs).

- The Hacker News: ShadowSyndicate Article
- Group-IB: ShadowSyndicate Report

UK and South Korea Release Joint Advisory Following Surge in North Korean-linked Attacks

Reported in the November 28th, 2023, FLASH Update

- The United Kingdom and South Korea recently released a joint advisory warning of a surge in software supply chain attacks by North Korean (DPRK) state-linked threat actors. The increased frequency and sophistication of such attacks carried out by North Korean-linked hackers is what prompted the creation of the joint advisory, with Korea's National Intelligence Service (NIS) and Britian's National Cyber Security Centre (NCSC) announcing a new strategic partnership between the nations' governments aimed at bolstering increased security measures that disrupt and deter DPRK malicious cyber capabilities and the associated activities that contribute to their nuclear missiles program. This advisory comes just as the North Korean-linked hackers tracked as Diamond Sleet were associated to another supply chain attack that targeted downstream customers via a trojanized version of a legitimate software application produced by the Taiwanese software developers CyberLink. As outlined in the joint advisory, and consistent with the latest DPRK-associated attack, the threat actors involved in the surge of attacks have been observed leveraging zero-day vulnerabilities and exploits in third-party software to gain access to specific targets or an entire organization via their supply chains. The agencies mentioned that the attacks align with known North Korean state aligned priorities like "revenue generation and espionage, with the theft of advanced technologies across a range of sectors, including but not limited to defense." Along with CyberLink, other recent noteworthy attacks include 3CX, MagicLine4NX, and JumpCloud.
  - National Cyber Security Centre: Joint Advisory
  - The Record: North Korea Article
  - Bleeping Computer: MagicLine4NX Article
  - The Hacker News: CyberLink Article

VULNERABILITIES

Critical Vulnerability Identified in On-Premise Instances of Atlassian Confluence

Reported in the November 3rd, 2023, FLASH Update

- Atlassian has issued an urgent advisory for a critical vulnerability, tracked as CVE-2023-22518, that affects its Confluence Data Center and Server products. In its advisory, Atlassian urged administrators to implement a patch as soon as possible. This vulnerability, which carries a high severity rating (CVSS 9.1/10), allows unauthenticated attackers to potentially sabotage Confluence instances causing significant data loss, however, it does not allow for the extraction of data. The vulnerability does not affect cloud-based or Software-as-a-Service (SaaS) versions of Confluence. No attempts at active exploitation have been reported yet, but the possibility has led to a call for immediate action by Atlassian's CISO, Bala Sathiamurthy. Cybersecurity firms underscore the importance of patching the servers immediately, noting that the risk lies in data deletion rather than data theft. This has been the second critical vulnerability in Confluence in a month, and users are expressing concern over the frequency of such vulnerabilities in Atlassian products. CTIX analysts recommend applying the patch immediately to prevent future exploitation. Additionally, administrators should implement network hardening and defense-in-depth techniques to better protect against other unknown vulnerabilities in the future.

    - Dark Reading: CVE-2023-22518 Article
    - Field Effect: CVE-2023-22518 Advisory

"TellYouThePass" Ransomware Observed Targeting Critical RCE Vulnerability in Public-Facing Apache Servers

Reported in the November 7th, 2023, FLASH Update

- "TellYouThePass", a ransomware variant first discovered in 2019, has resurfaced by affecting internet facing Apache ActiveMQ Servers using CVE-2023-46604. This is a critical vulnerability (with a CVSS Score of 10/10) published in late October 2023 that has already seen a great amount of use. This vulnerability allows for malicious actors to remote execute shell commands on the affected server version. On November 1, 2023, researchers released a report detailing how CVE-2023-46604 was being exploited to install "HelloKitty" ransomware on client Apache ActiveMQ servers while additional researchers identified evidence of this CVE being used to deploy "SparkRAT" malware. According to researchers, TellYouThePass has been deployed onto Apache ActiveMQ servers using the same techniques, file encryption flow, and file enumeration flow as HelloKitty. Additionally, a number of Bitcoin Wallets, IP Addresses, and email addresses were shared between the TellYouThePass and HelloKitty attacks utilizing CVE-2023-46604. For ActiveMQ servers, the attack is initiated through an HTTP request to the server. This creates a CMD process that is then used to download two (2) files that lead to the dropping of a .NET DLL to the system. This DLL does not use obfuscation, which allowed researchers to see its similarity with earlier versions of TellYouThePass. The ransomware then attempts to delete VSS snapshots to make system recovery more difficult before the ransom note titled “READ_ME4.html” is released after the system has been successfully encrypted. Apache has already released a patch for this CVE and is directing its customers to immediately update their environments. Despite this, there are still over 9,200 Apache ActiveMQ servers that are facing the internet with more than half of them still vulnerable to CVE-2023-46604 as of November 5, 2023. CTIX recommends that organizations update any Apache systems or devices currently being utilized to combat this vulnerability and ransomware. Additionally, CTIX will continue to monitor the ongoing ransomware campaigns involved with this vulnerability including the deployment of TellYouThePass.

- BleepingComputer: TellYouThePass Ransomware Article
- Rapid7: CVE-2023-46604 Report
- Arctic Wolf: CVE-2023-46604 Report
- SOC Prime: CVE-2023-46604 Report

CISA Adds Actively Exploited SLP Vulnerability to KEV

Reported in the November 10th, 2023, FLASH Update

- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added an actively exploited high-severity vulnerability in the Service Location Protocol (SLP) to their Known Exploited Vulnerabilities (KEV) catalog. SLP enables systems on a local area network (LAN) to discover and enable generic hardware and software services such as those for printers or file/email servers. The flaw, tracked as CVE-2023-29552, received a CVSS score of 7.5/10 and allows for denial-of-service (DoS) attacks if successfully exploited. This vulnerability also allows for DoS amplification attacks, significantly threatening networks by allowing attackers to register services and send spoofed UDP traffic. While the specific details of the exploitation are unknown at this time, the threat is severe enough that all federal civilian executive branch (FCEB) agencies are mandated to implement mitigation techniques, such as disabling the SLP service on systems within untrusted networks by no later than November 29, 2023. CTIX analysts will continue to follow the exploitation of this vulnerability and provide updates when applicable.

    - The Hacker News: CVE-2023-29552 Article
    - Security Affairs: CVE-2023-29552 Article
    - CISA: KEV

Cl0p Threat Actors Exploit Critical Vulnerability in SysAid

Reported in the November 14th, 2023, FLASH Update

- Cl0p threat actors, otherwise known as TA505 or Lace Tempest, have been observed actively exploiting a zero-day vulnerability in SysAid, a comprehensive IT Service Management (ITSM) solution, to infiltrate corporate servers for data theft and to deploy ransomware. The vulnerability, tracked as CVE-2023-47246, is a path traversal flaw that leads to remote code execution (RCE). The compromise was discovered on November 2, 2023, when attackers breached on-premise SysAid servers. Once successfully exploited, attackers upload a Web Application Resource (WAR) archive containing a webshell to the SysAid Tomcat web service, enabling the malicious activity. This includes executing PowerShell scripts, injecting GraceWire malware into legitimate processes, and avoiding detection by security products like Sophos. SysAid released a report detailing the attack mechanism and the steps taken by the threat actor, including data exfiltration and log deletion to cover their tracks. They also deployed additional scripts for Cobalt Strike listener access on compromised hosts. SysAid has since patched the flaw, and CTIX analysts urge all administrators and maintainers responsible for on premise SysAid servers to update to the latest version immediately. Administrators are also advised to inspect servers for any signs of compromise. SysAid's report provides indicators of compromise (IOCs), including filenames, hashes, IP addresses, file paths, and attacker commands to help detect or prevent intrusions.

    - Bleeping Computer: CVE-2023-47246 Article
    - The Record: CVE-2023-47246 Article
    - SysAid: CVE-2023-47246 Report

Critical Vulnerabilities Exploited to Attack Danish Critical Infrastructure

Reported in the November 17th, 2023, FLASH Update

- In May 2023, Denmark suffered the largest cyberattack against critical infrastructure in its history, after threat actors believed to be Russia-affiliated exploited a critical vulnerability impacting the Zyxel firewalls of twenty-two (22) different companies. The attack was highly sophisticated and targeted, and all victim organizations were exploited simultaneously. The initial vulnerability, tracked as CVE-2023-28771, is a command injection flaw which was exploited to achieve remote code execution (RCE), allowing the threat actors to conduct deep reconnaissance in vulnerable industrial control system (ICS) infrastructure of eleven (11) organizations. Later that month, a second wave of attacks exploited two (2) zero-day Zyxel vulnerabilities (CVE-2023-33009 and CVE-2023-33010), allowing threat actors to takeover over vulnerable endpoints, leveraging them in distributed denial-of-service (DDoS) attacks via the notorious “Mirai” and “MooBot” botnets. SektorCERT, a non-profit organization supported by Danish critical infrastructure companies, originally identified the malicious behavior against ICSs connecting the attacks, attributing them to the hacking arm of Russia's GRU (tracked as Sandworm). The second wave of attacks utilized previously unknown means and infrastructure and cannot currently be confirmed with high confidence to be associated with the Russian threat actors. Further details of the attack campaign can be found in the SectorCERT report linked below. CTIX analysts will continue to publish information about cutting edge attacks against critical infrastructure.
    - The Hacker News: Danish ICS Attack Article
    - SectorCERT: Danish ICS Attack Report

Actively Exploited libwebp Vulnerability Impacts Millions of Applications

Reported in the November 21st, 2023, FLASH Update

- Google has assigned a maximum CVSS severity rating of 10/10 to an actively exploited and previously disclosed zero-day vulnerability that has a scope extending much further than researchers initially thought. The flaw, tracked as CVE-2023-5129, is a heap-based buffer overflow in Google Chrome's libwebp library, specifically rooted in the Huffman coding algorithm. The libwebp library is an open-source toolkit for WebP, a lossy compression graphics format, used by multiple browsers and image editors. A threat actor could exploit this vulnerability by executing out-of-bounds memory writes via maliciously crafted HTML pages. Successful exploitation could cause a system crash, as well as access to privileged data, and arbitrary code execution. This is a very dynamic situation since the flaw was initially thought to only affect the Chrome browser and originally given the identifier CVE-2023-4863. However, researchers found that wasn't the case, prompting them to change the CVE identifier. Ultimately, this was a flaw in the libwebp library itself used to process WebP images by many other browsers and applications including 1Password, Signal, Safari, Mozilla Firefox, Microsoft Edge, Opera, and the native Android web browsers. The vulnerability's extended scope means that it affects millions of applications. This vulnerability has been patched, and CTIX recommends that all readers ensure their browsers are up to date by running the most stable and secure version.
    - Bleeping Computer: CVE-2023-5129 Article
    - The Record: CVE-2023-5129 Article
    - The Hacker News: CVE-2023-5129 Article
    - CISA: CVE-2023-5129 Advisory

North Korean Hackers Exploit Critical Vulnerability in Apache ActiveMQ to Take Control of Vulnerable Instance

Reported in the November 28th, 2023, FLASH Update

- UPDATE: A threat actor known as Andariel, believed to be a member or partner of the North Korean state sponsored threat group Lazarus, has been identified in a cyberattack campaign targeting South Korean entities to spread the NukeSped and TigerRat backdoors. Andariel is known for targeting "national defense, political groups, shipbuilding, energy, telecommunications, ICT firms, universities, and logistics firms." The threat actors were able to install the backdoors by exploiting a critical remote code execution (RCE) vulnerability in Apache ActiveMQ, tracked as CVE-2023-46604. ActiveMQ is an open-source protocol which functions as an implementation of message-oriented middleware (MOM), allowing different applications to send messages between each other. Specifically, the flaw exists in the Java OpenWire protocol marshaller, allowing remote attackers with network access to Java-based OpenWire brokers or clients to run arbitrary shell commands by manipulating class types. Once installed, the backdoors communicate with Andariel command-and-control (C2) servers, allowing the threat actors to take complete administrative control of compromised systems. The exploited vulnerability has been patched, however threat actors knowing that many organizations are slow to patch, are actively scanning and attacking vulnerable versions of ActiveMQ. CTIX analysts recommend that any administrators responsible for infrastructure that may be vulnerable should ensure that their instances of Apache ActiveMQ are running the most recent software version.
    - GBHackers On Security: Apache ActiveMQ Vulnerability Article
    - Apache: ActiveMQ Vulnerability Notification