ankura

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

September 2024

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 ***3***

Malware Activity ***4***

Cicada3301 Ransomware: An Evolution of BlackCat? 5
MacroPack Red Teaming Tool Abused by Threat Actors Globally 5
Lazarus Group Continues Campaign Against Developers and IT Professionals 6
New Malware Tied to APT34 Targets the Iraqi Government 6
Malware Locks Browser in Kiosk Mode, Frustrating User into Entering Credentials 7
New SambaSpy Malware Targeting Italian Users in Phishing Campaign 7
New Splinter Post-Exploitation Red Team Tool Abused by Attackers 8
AI-Generated Malware Deployed in Phishing Attacks 8

Threat Actor Activity ***10***

North Korean-linked Citrine Sleet Exploiting Chromium Zero-Day 11
North Korea's Continued Social Engineering Campaigns Target Crypto Industry 11
New Sophisticated Espionage Group Launches Campaign Targeting Taiwanese Drone Makers 12
Emerging Threat Actor CosmicBeetle Using New Ransomware to Target Small Businesses 12
RansomHub Claims Another Victim, Publishing Kawasaki's Stolen Data 13
Vanilla Tempest Using INC Ransomware Against the US Healthcare Sector 14
Iranian APT UNC1860 Gaining Initial Access to Many Middle Eastern Organizations 14
Chinese Hackers, Salt Typhoon, Infiltrating Deep Inside US Internet Service Providers 15

Vulnerabilities ***16***

Multiple Vulnerabilities Identified in Microsoft Applications for macOS 17
Cisco Patches Critical Vulnerability in its Identity Services Engine (ISE) Solution 17
Progress Software Patches Maximum Severity Vulnerability in LoadMaster and MT Hypervisor 17
Ivanti Patches Multiple Critical Vulnerabilities in their Endpoint Management Solution 18
Critical Ivanti Vulnerability Under Active Exploitation by Threat Actors 18
GitLab Patches Critical SAML Authentication Bypass Vulnerability 19
Critical Stack-Based Overflow Flaw Found in Microchip Advanced Software Framework (ASF) "tinydhcp" Server 19
CISA adds Critical Ivanti Virtual Traffic Manager Flaw to its Known Exploited Vulnerabilities Catalog 20

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 September 2024, originally published in CTIX FLASH Updates throughout September. 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

Cicada3301 Ransomware: An Evolution of BlackCat?

Reported in the September 4th, 2024, FLASH Update

- Cicada3301 ransomware is attacking companies in North America and Europe with a sophisticated form of ransomware resembling BlackCat. Cicada3301 is a ransomware-as-a-service (RaaS) operation which emerged in June 2024, shortly after the ALPHV/BlackCat ransomware group performed an exit scam in March 2024 after stealing a $22 million ransom from one of their affiliates. Cybersecurity researchers believe that Cicada3301 may be an offshoot of the BlackCat group based on the similarities in techniques between the two (2) threat actors. Both forms of ransomware are written in Rust, use the encryption algorithm, perform identical virtual machine (VM) shutdown and snapshot-wiping commands, use intermittent encryption on larger files, and use the same file naming convention and ransom note decryption method. Cicada3301's ransomware includes both Windows and Linux/VMware ESXi encryptors. Cicada3031 is also distinguished from BlackCat's ransomware in many ways: its encryption process is more customizable, it uses stolen credentials on the fly to automatically feed into psexec for privilege escalation and lateral movement, and it is delivered behind an EDR-bypassing tool "EDRSandBlast". In addition, the threat actors behind Cicada3301 have been improving obfuscation capabilities so that the malware evades detection by antivirus and security products. Similar to BlackCat, Cicada3301 ransomware appends encrypted files on victim machines with a random seven-character extension and leaves a ransom note named "RECOVER-[extension]-DATA.txt". According to Cicada3301's leak site, they have compromised 21 companies in the past few months. The threat group's victims have been concentrated in North America and Europe, and the majority have been small businesses. CTIX analysts will continue to report on new and emerging forms of malware and associated campaigns.
    - Bleeping Computer: Linux Version of New Cicada Ransomware
    - Dark Reading: BlackCat Spinoff Uses Stolen Creds on the Fly, Skirts EDR

MacroPack Red Teaming Tool Abused by Threat Actors Globally

Reported in the September 6th, 2024, FLASH Update

- Content Researchers have discovered that MacroPack – an attacker emulation software – is being abused by multiple cyber threat actors. MacroPack is a proprietary tool leveraged by red and purple teams to test prevention and detection mechanisms. Security researchers discovered its use for nefarious purposes by analyzing document submissions made to VirusTotal from around the globe. Submissions from the United States, China, Russia, and Pakistan indicate that MacroPack had been used to craft malicious VBA code delivered via Microsoft Office documents to spread final malware payloads such as Havoc, Brute Ratel, and PhantomCore. The documents analyzed all contained VBA subroutines embedded in the documents which indicate they had been created using MacroPack. Researchers believe that multiple different threat actors are behind these campaigns given the variation of lures and targets related to the identified documents. MacroPack includes advanced features that threat actors can abuse, such as anti-malware bypass techniques, code obfuscation, and undetectable VB scripts. Once a victim opens an infected document, MacroPack decodes a shellcode stage which then kicks off a DLL payload that connects to a command-and-control (C2) server. Final payloads observed include post-exploitation C2 tools such as Havoc and Brute Ratel and Remote Access Trojan (RAT) Phantom Core. Brute Ratel is a post-exploitation attack framework much like Cobalt Strike. CTIX analysts recommend that organizations utilize Endpoint Detection and Response (EDR) and Next-Generation Anti-Virus (NGAV) to prevent and detect these types of threats, and to ensure the Indicators of Compromise (IOCs) related these campaigns are blocked. CTIX analysts will continue to report on new and emerging forms of malware and associated campaigns.

- BleepingComputer Article: MacroPack
- The Hacker News Article: MacroPack
- Cisco Talos: MacroPack

Lazarus Group Continues Campaign Against Developers and IT Professionals

Reported in the September 10th, 2024, FLASH Update

- Researchers at Group-IB have recently released a new report on ongoing and new threats posed by Lazarus Group's financially-motivated campaign against job seekers. CTIX analysts discussed the emergence of this campaign in our April 30, 2024 flash. Since then, Lazarus has expanded its capabilities and has introduced new malware targeted at MacOS to steal information and cryptocurrency from job seekers in the IT and Software Development fields. The campaign is rooted in a fictitious job posting and interview process that tricks seekers into downloading a "Node.js" project containing malware. Researchers have observed updated versions of the major forms of malware used in this campaign dubbed BeaverTail and InvisibleFerret. BeaverTail is a JavaScript or Python-based InfoStealer with the ability to steal credentials stored in browsers and vaults as well as data from browser extensions and cryptocurrency wallets. InvisibleFerret is Python-based malware that acts as a backdoor, keylogger, and infostealer. Both forms of malware are under active development. The recent Python versions of BeaverTail are delivered via a simple JavaScript downloader and fetches a bundle of scripts called CivetQ to modularize the malware's capabilities. Researchers have also noted that Lazarus has included additional job search platforms in their campaign in an apparent attempt to target professionals skilled in Blockchain. This tactic could have been introduced to increase the attackers' likelihood of infecting a victim with cryptocurrency on their machine. Platforms added to their campaign beyond LinkedIn include WWR, Moonlight, and Upwork. They have also started using fraudulent video conferencing applications to spread the initial BeaverTail loader as an alternative initial infection vector to the fake "Node.js" project. Researchers discovered a cloned website of a legitimate free conferencing software application which hosts the fake video conference application "FCCCall". Installers for both Windows and MacOS were discovered by researchers. CTIX analysts urge individuals to remain vigilant online and to vet potential employers prior to engaging in the job interview process. CTIX analysts will continue to report on new and emerging forms of malware and associated campaigns.
    - HackRead Article
    - Group-IB Article

New Malware Tied to APT34 Targets the Iraqi Government

Reported in the September 13th, 2024, FLASH Update

- Researchers have discovered a new set of malware used in attacks against Iraqi entities allegedly including the Prime Minister's Office and the Ministry of Foreign Affairs. The malware dubbed "Veaty" and "Spearal" have ties to malware families used by APT34, a cyber group affiliated with the Iranian Ministry of Intelligence and Security also known as "OilRig". The malware identified in the campaign is bespoke and along with the techniques deployed, resembles custom backdoors such as "Karkoff" and "Saitama" previously associated with APT34. While the original infection pathway is unknown, the initial files used to kick-off the campaign were likely delivered to victims through social engineering. These initial files use double extensions to appear legitimate. Examples of file names include "Avamer.pdf.exe" and "Protocol.pdf.exe". These files execute PowerShell or Pyinstaller scripts to deploy the "Veaty" and "Spearal" malware payloads and configuration files and maintain persistence by modifying the Windows registry under "\CurrentVersion\Run". The "Spearal" malware is a .NET backdoor that uses DNS tunneling using

a custom Base32 encoding scheme for command-and-control (C2) communication. “Spearal” can execute PowerShell commands, read file contents, retrieve data from the C2 server, and send data back to the C2 server. The “Veaty” malware is also a .NET-based malware which uses compromised email accounts in the victim organization for C2 communications. In the malware sample analyzed by researchers, the malware used email accounts at the gov-iq[.]net domain to execute commands. The malware can upload and download files, execute commands, and run scripts through specific mailboxes. Researchers also identified an XML configuration file capable of setting up an SSH tunnel which the threat actor likely used as a third backdoor. The tactics, techniques, and procedures used in this campaign suggest that APT34/OilRig is responsible. The use of custom C2 mechanisms is notable among these newly identified backdoors. CTIX analysts will continue to report on new and emerging forms of malware and associated campaigns.

- The Hacker News Article
- Medium Article
- Check Point Article

Malware Locks Browser in Kiosk Mode, Frustrating User into Entering Credentials

Reported in the September 17th, 2024, FLASH Update

- A recent malware campaign has been identified that traps users in their browser's kiosk mode on Google's login page, compelling them to enter their Google credentials out of annoyance. The malware locks the browser, disabling the "ESC" and "F11" keys, which prevents users from easily exiting kiosk mode. Kiosk mode is a specialized setting in web browsers or apps that allows them to operate in full-screen mode without standard user interface elements such as toolbars, address bars, or navigation buttons. This mode is intended to restrict user interactions to specific functions, making it perfect for public kiosks. However, in the case of this attack, kiosk mode is misused to confine user actions to the Google login page, presenting the sole option of entering account credentials This tactic aims to frustrate users into entering their credentials and "unlocking" the computer, which are then stolen by the StealC information-stealing malware. This attack method has been active since at least August 22, 2024, and is mainly utilized by Amadey, a malware loader known for information theft and system reconnaissance. Amadey deploys an AutoIt script that scans for available browsers and launches one in kiosk mode directed to Google's change password page. This creates an opportunity for users to reenter and save their credentials, which StealC subsequently steals. If users find themselves trapped in kiosk mode, they should avoid entering any sensitive information and try alternative hotkeys like 'Alt + F4' or 'Ctrl + Shift + Esc' to exit the browser. If these methods fail, performing a hard reset and running a full antivirus scan in Safe Mode is recommended to remove the malware.
    - Bleeping Computer: Amadey Kiosk Article

New SambaSpy Malware Targeting Italian Users in Phishing Campaign

Reported in the September 20th, 2024, FLASH Update

- A newly discovered malware dubbed SambaSpy is exclusively targeting Italian users through a phishing campaign led by a suspected Brazilian Portuguese-speaking threat actor. The attack begins with phishing emails containing HTML attachments or embedded links that initiate the malware infection process. The HTML attachment opens a ZIP archive that deploys a downloader or dropper to launch the remote access trojan (RAT) payload. SambaSpy's infection chain is elaborate, redirecting users to either legitimate invoices or malicious web servers based on specific criteria such as browser type and language settings. Users meeting these criteria are served a malicious JAR file from MediaFire, leading to the deployment of the RAT, which is capable of extensive remote-control functions such as file management, keylogging, webcam control, and

more. The malware also steals credentials from various web browsers and can load additional plugins to enhance its capabilities. Evidence indicates that the threat actor may expand its operations to Brazil and Spain, reflecting a broader trend of Latin American cybercriminals targeting European countries with related languages. This development comes alongside a surge in banking trojan campaigns in Latin America, employing sophisticated phishing scams to steal sensitive banking credentials and execute unauthorized transactions. These campaigns utilize advanced evasion techniques, such as obfuscated PowerShell scripts and malicious ISO files, to avoid detection.

- The Hacker News: SambaSpy Article

New Splinter Post-Exploitation Red Team Tool Abused by Attackers

Reported in the September 24th, 2024, FLASH Update

- Cybersecurity researchers have recently discovered a new red-teaming tool – "Splinter"- lurking on compromised systems post-incident. Splinter is similar to the well-known post-exploitation tool Cobalt Strike, but less advanced. Researchers dub the tool "Splinter" based on the internal project name spotted in a debugging artifact in its code. It is not yet known who developed Splinter or which threat groups have been attributed to its misuse. Splinter is developed in Rust, and its samples are very large due to the number of external libraries the file uses. Splinter uses a JSON format for its configuration data which contains the implant and targeted endpoint identifiers as well as the command-and-control (C2) server details. Splinter connects to its C2 server over HTTPS. Splinter's capabilities include running Windows commands, remote process injection, file uploads and downloads, information harvesting, and self-destructing. Splinter is a red team tool, which when used as intended provides adversary simulation frameworks that allow organizations to test and improve their defenses. CTIX analysts reported earlier this month on another red team tool "MacroPack" that is being used by threat actors to escalate privileges and download malware on victim machines. These two developments this month indicate that threat actors are using different post-exploitation tools likely in the attempt to evade detection as Cobalt Strike has notoriously been used by threat actors for malicious purposes. CTIX analysts will continue to report on new and emerging forms of malware and associated campaigns.
  - The Register: Splinter Article
  - Unit 42: Splinter Blog

AI-Generated Malware Deployed in Phishing Attacks

Reported in the September 27th, 2024, FLASH Update

- Cybersecurity researchers have recently identified an email phishing campaign that deploys a malware dropper likely produced by a generative AI model. Cybercriminals have been known to use "Dark" AI to enhance their social engineering attacks, better articulating their pretext and eliminating tell-tale grammatical and spelling errors. CTIX analysts reported on the emergence of "Dark" AI this summer. Now it is evident that unsophisticated cybercriminals are leveraging generative AI tools trained for malicious intent to build malware, further lowering the barrier of entry into the cybercrime industry. Researchers at HP Wolf Security recently released their analysis of a phishing email with an invoice lure and encrypted HTML attachment. Once the HTML attachment is decrypted, a website opens and a VBScript runs that drops the AsyncRAT infostealer onto the victim machine. The VBScript writes various variables to the Windows Registry to establish persistence. A JavaScript file is also dropped into the user directory which is run by a scheduled task. The JavaScript executes a PowerShell script which makes use of the Registry variables and starts the malware payload after injecting it into a legitimate process. It is the

VBScript and JavaScript files that researchers believe were likely created with the help of generative AI. For one, the scripts are very neatly structured with detailed and commented code. In addition, the scripts are written in French (which is not commonly the language used by malware architects). Sophisticated attackers do not comment their code, in fact they attempt to make their malware as difficult as possible to analyze through obfuscation and confusion. The infostealer payload, AsyncRAT, is a free and readily accessible malware that could be picked up and used by any novice cybercriminal. These circumstances reflect the high likelihood that the malware campaign was created by an unseasoned cybercriminal with the help of generative AI. CTIX analysts are keeping an eye out for any additional developments that would suggest generative AI is being used to generate malware payloads beyond just droppers. CTIX analysts will continue to report on new and emerging forms of malware and associated campaigns.

- Bleeping Computer: Generative AI Article
- Security Week: Generative AI Article

THREAT ACTOR ACTIVITY

North Korean-linked Citrine Sleet Exploiting Chromium Zero-Day

Reported in the September 4th, 2024, FLASH Update

- A recently patched zero-day vulnerability in Google Chrome (CVE-2024-7971) has been exploited by North Korean-linked threat actors in a campaign targeting the cryptocurrency industry. The threat actor, identified as Citrine Sleet (also known as AppleJeus, Labyrinth Chollima, and UNC4736), is linked to North Korea's Reconnaissance General Bureau and is considered a subgroup within the notorious Lazarus Group. This campaign, detected on August 19, 2024, involved sophisticated social engineering techniques, including the creation of fake websites mimicking legitimate cryptocurrency trading platforms. These sites lured victims into downloading malicious crypto wallets or trading apps, which facilitated the theft of digital assets. The zero-day exploit in question, CVE-2024-7971, is a high-severity type confusion vulnerability in the V8 JavaScript engine used by Chromium-based browsers. The exploitation of this flaw enabled remote code execution (RCE) within the sandboxed Chromium renderer process. Victims were typically directed to a malicious website (voyagorclub[.]space) where the exploit was triggered. Upon successful exploitation, the attackers deployed shellcode containing a Windows sandbox escape exploit (CVE-2024-38106) and the FudModule rootkit. This rootkit allows attackers to gain SYSTEM privileges, perform direct kernel object manipulation, and maintain persistent access to compromised systems. The FudModule rootkit has been in use since 2021 and is shared among various North Korean hacking groups, including Diamond Sleet and BlueNoroff. This zero-day exploit chain is part of a broader strategy by North Korean actors to target financial institutions and cryptocurrency firms for financial gain. The Citrine Sleet group has previously used similar tactics, such as fake job applications and weaponized software, to compromise their targets. This activity aligns with North Korea's broader objective of generating revenue through cyber operations, having reportedly netted $3 billion from cryptocurrency attacks between 2017 and 2023. The U.S. government has added CVE-2024-7971 to its catalog of known exploited vulnerabilities, mandating federal agencies to patch the flaw by September 16, 2024.
    - The Hacker News: Citrine Sleet Article
    - Bleeping Computer: Citrine Sleet Article
    - The Record: Citrine Sleet Article

North Korea's Continued Social Engineering Campaigns Target Crypto Industry

Reported in the September 6th, FLASH Update

- The FBI has issued a warning about North Korean hacking groups aggressively targeting cryptocurrency companies and their employees through sophisticated social engineering attacks aimed at stealing crypto assets. These state-sponsored groups, including the notorious Lazarus Group, Kimsuky, and others, have stolen an estimated $3 billion in cryptocurrency since 2017. Recent campaigns have focused on cryptocurrency exchange-traded funds (ETFs) and related financial products, deploying meticulously planned attacks that involve extensive pre-operational research and the use of social engineering techniques to gain unauthorized access to networks. The attackers identify specific DeFi (decentralized finance) and cryptocurrency businesses and target their employees, often posing as recruiters or offering investment opportunities. They use fluent English and detailed personal information to enhance credibility. The FBI highlights that these malicious actors also employ stolen images and professionally crafted websites to appear more legitimate. Indicators of suspicious activity, as noted in the FBI's public service announcement, include requests to use non-standard software and unusual communication patterns. The FBI has provided guidelines for cryptocurrency companies and their employees to mitigate these risks. The Bureau has also warned of related scams, such as fake remote job ads and unlicensed cryptocurrency transfer services, which can result in significant financial losses.

Despite the sophisticated technical judgement of DeFi and cryptocurrency firms, they still remain vulnerable to these highly tailored social engineering campaigns. North Korean hackers have been linked to several high-profile crypto heists, including the theft of $620 million from Axie Infinity's Ronin network bridge, the largest crypto hack to-date. The FBI's alert underscores the persistent threat posed by North Korean cyber actors to companies handling large quantities of cryptocurrency assets.

- The Record: North Korea Article
- Bleeping Computer: North Korea Article
- FBI: North Korea Report

New Sophisticated Espionage Group Launches Campaign Targeting Taiwanese Drone Makers

Reported in the September 10th, 2024, FLASH Update

- A newly identified threat actor, dubbed TIDRONE, is targeting drone manufacturers in Taiwan, with a broader focus on military and satellite-related industrial supply chains. This espionage-driven campaign, which began in early 2024, is believed to have connections to other Chinese-speaking groups. TIDRONE employs sophisticated attack methods, including the deployment of custom malware such as CXCLNT and CLNTEND, often using enterprise resource planning (ERP) software or remote desktop tools like UltraVNC to infiltrate targets. The exact vector for initial access remains unclear, but commonalities among victims suggest a potential supply chain attack. Once inside a network, TIDRONE's attack chain involves three (3) stages designed to escalate privileges, dump credentials, and evade defenses by disabling antivirus software. The malware is typically introduced via sideloading a rogue DLL through the Microsoft Word application, enabling the attackers to collect a wide range of sensitive information. CXCLNT is equipped with basic file upload and download capabilities, trace-clearing functions, and tools for gathering victim information such as file listings and computer names. It can also download and execute additional portable executable (PE) and DLL files. CLNTEND, first detected in April 2024, is a more advanced remote access tool (RAT) supporting multiple network protocols, including TCP, HTTP, HTTPS, TLS, and SMB (port 445). Analyses highlight that TIDRONE's operations align with other Chinese espionage activities, supported by the consistency in file compilation times and operational patterns. The threat actors have continually updated their toolsets and optimized their attack chains, employing anti-analysis techniques in their loaders to alter execution flows and evade detection. The campaign's reach extends beyond Taiwan, with artifacts from VirusTotal indicating varied targeted countries, prompting a warning from CTIX analysts for global vigilance against this threat.
    - The Hacker News: TIDRONE Article
    - Dark Reading: TIDRONE Article

Emerging Threat Actor CosmicBeetle Using New Ransomware to Target Small Businesses

Reported in the September 13th, 2024, FLASH Update

- CosmicBeetle, an emerging ransomware group also known as NONAME, has developed a new ransomware strain called ScRansom, targeting small and medium-sized businesses (SMBs) across Europe, Asia, Africa, and South America. Active since at least 2020, the group is considered relatively immature in the ransomware landscape, even sometimes relying on the reputations of more established threat actors like LockBit to coerce victims into paying ransoms. Despite its lack of sophistication, ScRansom has caused significant damage to various industries, including pharmaceuticals, healthcare, technology, hospitality, and financial services. ScRansom first appeared in March 2023, with researchers noting a continuous development of the ransomware over its lifespan. To gain access to target systems, CosmicBeetle employs brute-force methods

and exploits old vulnerabilities in software commonly used by SMBs, which often lack robust patch management processes. The group also uses a variety of tools, such as Reaper, Darkside, and RealBlindingEDR, to terminate security-related processes before deploying ScRansom. CosmicBeetle's connection to RansomHub, a ransomware gang active since March 2024, has been observed through the deployment of both ScRansom and RansomHub payloads on the same machines within short timeframes. This affiliation is likely an attempt to leverage RansomHub's more established reputation and tools to compensate for the group's own technical shortcomings. CosmicBeetle has also been observed experimenting with the leaked LockBit builder, further indicating its reliance on the tools and reputations of more sophisticated ransomware groups. Additionally, the group has utilized various vulnerabilities to infiltrate networks, including CVE-2017-0144 (EternalBlue) and CVE-2020-1472 (ZeroLogon). The ransomware's encryption scheme is complex, involving multiple key exchanges, which sometimes introduce errors that complicate the decryption process and can result in permanent data loss for victims, even if they pay the ransom. CosmicBeetle has been using RansomHub's EDR killer tool to disable security agents on compromised devices, further solidifying its affiliation with RansomHub. CosmicBeetle's emergence and activities highlight an evolving threat. CTIX analysts recommend heightened vigilance, particularly from SMBs in the sectors and geographical areas this threat actor has been known to operate in.

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

RansomHub Claims Another Victim, Publishing Kawasaki's Stolen Data

Reported in the September 17th, 2024, FLASH Update

- Kawasaki Motors Europe is recovering from a recent cyberattack attributed to the RansomHub ransomware gang, which has claimed to have stolen four hundred and eighty-seven (487) gigabytes of data from the company. The attack, which occurred in early September 2024, led to the temporary isolation of Kawasaki's servers as a precautionary measure. The company's IT department, in collaboration with external cybersecurity experts, spent the following week meticulously checking each server for any suspicious material such as malware before reconnecting them back to the corporate network. Thus far, Kawasaki Motors Europe has restored over 90% of its server functionality, ensuring that operations involving motor vehicle dealers, third-party suppliers, and logistics are not significantly impacted. The company, which reported over $3 billion in earnings last quarter, is a major player in the motor vehicle industry, manufacturing motorcycles, utility vehicles, and other motorized products. The cyberattack has drawn further attention to RansomHub, a ransomware gang that has emerged as a significant threat following the dissolution of earlier gangs like LockBit and AlphV. RansomHub has been linked to at least two hundred and ten (210) ransomware attacks on various organizations since launching in February 2024, according to the FBI and other law enforcement agencies. Notable recent victims include Rite Aid, Frontier, Planned Parenthood, Halliburton, and Christie’s. The group's tactic involves adding victims to its extortion portal on the dark web, with a timer set to publish stolen data if ransom demands are not met. The timer for Kawasaki was set to expire on Saturday, September 14, 2024. CTIX analysts’ own research found that Kawasaki’s data has indeed been published on the RansomHub leak site. Despite the severity of the attack, Kawasaki has not publicly commented on whether customer data was included in the stolen files. The company has also not responded to media inquiries about the incident.
    - The Record: Kawasaki RansomHub Article
    - Bleeping Computer: Kawasaki RansomHub Article

Vanilla Tempest Using INC Ransomware Against the US Healthcare Sector

Reported in the September 20th, 2024, FLASH Update

- A financially motivated threat actor named Vanilla Tempest (formerly known as DEV-0832 and Vice Society) has been identified deploying the INC ransomware strain in attacks on US healthcare organizations. This marks the first observed use of INC ransomware by Vanilla Tempest, which has a history of targeting sectors like education, healthcare, IT, and manufacturing with various ransomware strains, including BlackCat, Quantum Locker, Zeppelin, and Rhysida. Vanilla Tempest's recent attack involved gaining network access through the GootLoader malware downloader, introduced by the Storm-0494 threat actor. After initial access, the attackers deployed the Supper backdoor, AnyDesk remote monitoring tool, and MEGA data synchronization tool for persistence and data exfiltration. They used Remote Desktop Protocol (RDP) and the Windows Management Instrumentation (WMI) Provider Host for lateral movement before deploying the INC ransomware payload. The attack on the healthcare sector follows a pattern of ransomware groups like BianLian and Rhysida using Azure Storage Explorer and AzCopy to exfiltrate sensitive data to cloud storage, aiming to evade detection. In May 2024, a threat actor named "salfetka" attempted to sell the source code for INC ransomware's Windows and Linux/ESXi versions for $300,000 on two (2) separate hacking forums. The same ransomware strain was linked to a cyberattack on Michigan's McLaren Health Care hospitals, causing significant disruptions to IT and phone systems and forcing the rescheduling of some medical procedures. Vanilla Tempest's activities, particularly in the healthcare sector, highlight the ongoing threat of growing ransomware attacks. CTIX analyst will continue to monitor emerging threat actor activity.
    - Bleeping Computer: Vanilla Tempest Article
    - The Hacker News: Vanilla Tempest Article

Iranian APT UNC1860 Gaining Initial Access to Many Middle Eastern Organizations

Reported in the September 24th, 2024, FLASH Update

- A sophisticated cyber operation within Iran's Ministry of Intelligence and Security (MOIS) has been identified as a significant initial access broker for other Iranian hackers, providing persistent entry into telecommunications and government organizations across the Middle East. This Iranian APT, UNC1860, has been active since at least 2020 and has developed a collection of specialized tools and passive backdoors that support other Iranian hacking activities, including espionage and network attack operations. The FBI just recently reported that the group of Iranian hackers who attempted to steal and disseminate documents from former President Donald Trump's campaign are likely associated with UNC1860. UNC1860's tools are designed to evade antivirus software, maintaining long-term, stealthy access to compromised systems. These tools have been utilized by other MOIS-affiliated groups, such as APT34, and have been linked to destructive cyber operations, including attacks on Israel in 2023 and Albania in 2022. The group's arsenal includes various malware controllers like TEMPLEPLAY and VIROGREEN, which provide remote access and facilitate post-exploitation activities within target networks. The tools and techniques employed by UNC1860 include a range of backdoors and loaders, such as OATBOAT, TOFUDRV, TOFULOAD, and TEMPLELOCK, which facilitate initial access, lateral movement, and information gathering within victim networks. These tools highlight the group's capability to maintain persistent access and conduct extensive reconnaissance without detection. The increasing sophistication and boldness of Iranian cyber operations have drawn significant attention from security researchers and government agencies. As tensions continue rising in the Middle East, UNC1860's ability to gain and maintain access to high-priority networks is considered a valuable asset for Iran's cyber ecosystem, capable of adapting to evolving objectives.
    - The Hacker News: UNC1860 Article

- The Record: UNC1860 Article

Chinese Hackers, Salt Typhoon, Infiltrating Deep Inside US Internet Service Providers

Reported in the September 27th, 2024, FLASH Update

- A newly discovered advanced persistent threat (APT) group, dubbed Salt Typhoon, has been implicated in a series of cyber espionage operations targeting U.S. internet service providers (ISPs). This group, believed to be backed by Beijing, has reportedly compromised several ISPs to establish a persistent presence within their networks. The ultimate aim is to gather sensitive information and potentially prepare for future disruptive cyberattacks. Salt Typhoon, also known as FamousSparrow and GhostEmperor, has a history of targeting high-profile entities in Southeast Asia and other regions. The attacks are part of a broader pattern of Chinese state-sponsored efforts to infiltrate critical infrastructure. Investigators are examining whether the intruders accessed Cisco Systems routers, which are crucial for internet traffic routing. This campaign follows a series of similar intrusions by other Chinese APT groups, such as Flax Typhoon and Volt Typhoon, known for targeting U.S. critical infrastructure, government, and military networks. These groups have been linked to extensive cyber espionage and data theft operations. Salt Typhoon's recent activities highlight China's strategic priorities, including reconnaissance and pre-positioning for potential military conflicts. By compromising ISPs, the group could monitor high-value targets, including federal agencies, military contractors, and Fortune 100 companies. This capability aligns with China's broader goals of controlling regional assets and preparing for possible conflicts, such as over Taiwan. The U.S. government and cybersecurity agencies are actively responding to these threats. Recent actions include the disruption of a 260,000-device botnet controlled by Flax Typhoon and heightened warnings about ongoing Chinese cyber campaigns. CTIX analysts advise organizations to review the latest advisories and implement stringent security practices to protect against these sophisticated cyber threats.
    - The Hacker News: Salt Typhoon Article
    - Dark Reading: Salt Typhoon Article
    - The Register: Salt Typhoon Article

VULNERABILITIES

Multiple Vulnerabilities Identified in Microsoft Applications for macOS

Reported in the September 4th, 2024, FLASH Update

- Eight (8) security vulnerabilities have been identified in several Microsoft applications for macOS, presenting a potential risk that attackers could exploit to gain elevated privileges or unauthorized access to sensitive data. These vulnerabilities allow malicious actors to bypass the macOS permissions-based model, which relies on Apple's Transparency, Consent, and Control (TCC) framework. This framework is designed to give users visibility and control over how their data is accessed by different applications, ensuring that only approved applications can access specific types of data. The affected applications include widely used programs such as Outlook, Teams, Word, Excel, PowerPoint, and OneNote. The vulnerabilities stem from the ability to inject malicious libraries into these applications, which can then inherit the applications' entitlements and permissions. This could allow an attacker to send emails from a user's account, record audio, take photos, or capture videos without the user's awareness or interaction. If successfully exploited, a trusted application could act as a proxy, allowing the attacker to perform actions that would normally require explicit user consent. It's important to note that for these attacks to be successful, the attacker must already have gained initial access to the target system. Microsoft has implemented fixes in its OneNote and Teams applications to mitigate the potential risks. The broader challenge of securely handling plugins within macOS remains, with options like notarization of third-party plugins being a possible solution. This would require either Microsoft or Apple to sign third-party modules after verifying their security, adding an extra layer of protection against such exploits.
    - The Hacker News: macOS Microsoft App Vulnerabilities Article

Cisco Patches Critical Vulnerability in its Identity Services Engine (ISE) Solution

Reported in the September 6th, 2024, FLASH Update

- Cisco has recently patched a critical command injection vulnerability in its Identity Services Engine (ISE), a network access control solution widely used in enterprise environments. This vulnerability, tracked as CVE-2024-20469, allows attackers with existing administrator privileges to escalate their access to root, granting them full control over the system. The issue stems from inadequate validation of user-supplied input in certain CLI commands, which local attackers can exploit by submitting malicious commands. This flaw is considered low complexity, requiring no user interaction, making it particularly concerning. Although Cisco has released the necessary security updates, proof-of-concept (PoC) exploit code is already available to the public, raising the potential risk of future exploitation. Fortunately, Cisco has not observed any evidence of attackers actively exploiting this vulnerability in the wild. In addition to this critical patch, Cisco warned of a backdoor account in its Smart Licensing Utility Windows software, which has also been addressed. This backdoor could have allowed attackers to log into unpatched systems with administrative privileges. The patch for CVE-2024-20469 follows a series of other critical security updates from Cisco, including fixes for an Integrated Management Controller (IMC) vulnerability (CVE-2024-20295) and a vulnerability in its Security Email Gateway (SEG) appliances (CVE-2024-20401), both of which also allowed for privilege escalation and could be exploited to crash systems or add rogue users. CTIX analysts urge users to install the updates immediately to secure their systems from potential exploitation.
    - Bleeping Computer: CVE-2024-20469 Article

Progress Software Patches Maximum Severity Vulnerability in LoadMaster and MT Hypervisor

Reported in the September 10th, 2024, FLASH Update

- Progress Software has released an emergency fix for a highly critical vulnerability, affecting its LoadMaster and LoadMaster Multi-Tenant (MT) Hypervisor products. This vulnerability, tracked as CVE-2024-7591, has a maximum CVSS score of 10/10 since it enables unauthenticated attackers to conduct remote code execution (RCE) by exploiting an improper input validation flaw. The attack can be facilitated through a maliciously crafted HTTP request targeting the management interface of affected devices. Once successful, the attacker can gain control over vulnerable systems without needing authentication. The flaw affects all versions of LoadMaster up to 7.2.60.0 and MT Hypervisor up to 7.1.35.11, including Long-Term Support (LTS) and Long-Term Support with Feature (LTSF) branches. At this time, Progress has confirmed that no reports of active exploitation have been received. Security researcher Florian Grunow is credited with discovering the issue. To mitigate the risk, Progress released a patch that can be installed on any affected version. The fix works by sanitizing user inputs to prevent arbitrary command execution. However, the patch does not apply to the free version of LoadMaster, leaving it exposed to potential exploitation. Progress strongly advises all users to apply the patch immediately by navigating to the system's configuration interface and following their recommended security hardening guidelines. Failing to address this flaw could leave critical infrastructure and network environments vulnerable to remote command injection attacks, posing a significant risk to organizations relying on these solutions for load balancing, traffic management, and application delivery. CTIX analysts urge all administrators of the affected devices to install the patch immediately to prevent exploitation.
    - Bleeping Computer: CVE-2024-7591 Article
    - The Hacker News: CVE-2024-7591 Article

Ivanti Patches Multiple Critical Vulnerabilities in their Endpoint Management Solution

Reported in the September 13th, 2024, FLASH Update

- Ivanti has released critical security patches for multiple vulnerabilities across its Endpoint Manager, Cloud Service Appliance, and Workspace Control products. Among the most severe is a remote code execution (RCE) vulnerability, tracked as CVE-2024-29847 in Endpoint Manager. This flaw is caused by deserialization of untrusted data, which could allow unauthenticated attackers to gain access to the core server. This vulnerability has been patched in Endpoint Manager 2024 and 2022 Service Update 6 (SU6), with no current evidence of exploitation in the wild. Ivanti also fixed nearly two dozen additional critical and high-severity vulnerabilities across its products, including SQL injection flaws that could be exploited by administrators, as well as OS command injection, and local privilege escalation vulnerabilities in Workspace Control and Cloud Service Appliance. Ivanti attributes the rise in detected vulnerabilities to improved internal scanning, manual testing, and a stronger vulnerability disclosure process. Although past zero-day vulnerabilities in Ivanti's VPN appliances have been exploited, the company has no evidence of current vulnerabilities being exploited and continues to improve its security measures for its extensive global customer base. CTIX analysts recommend that all Ivanti customers ensure that they are running the most secure version of software for their products to prevent exploitation.
    - Bleeping Computer: CVE-2024-29847 Article
    - Security Week: CVE-2024-29847 Article

Critical Ivanti Vulnerability Under Active Exploitation by Threat Actors

Reported in the September 17th, 2024, FLASH Update

- Ivanti has disclosed that a high-severity vulnerability in its Cloud Service Appliance (CSA) is actively being exploited in attacks, prompting action from both the company and federal agencies. The vulnerability, tracked as CVE-2024-8190, allows for remote code execution (RCE) by attackers with

administrative privileges and impacts CSA version 4.6, which has reached its end-of-life status. Ivanti has released a patch (CSA 4.6 Patch 519), but strongly advises customers to upgrade to the supported CSA version 5.0, which is not affected by this vulnerability and continues to receive updates. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added the flaw to its Known Exploited Vulnerabilities (KEV) catalog, mandating that federal agencies secure vulnerable systems by no later than October 4, 2024. Ivanti also noted that configurations following best practices, such as dual-homed CSA setups, are at a lower risk of exploitation. In addition to addressing this vulnerability, Ivanti has also patched other critical flaws, including a maximum-severity issue in its Endpoint Management software (EPM). The company has ramped up internal scanning, testing, and responsible vulnerability disclosure practices to improve its security response. With its products widely used by over 40,000 companies, including federal agencies, the urgency for upgrading and securing these systems is crucial to prevent further exploitation. CTIX analysts recommend that all administrators responsible for instances of Ivanti Cloud CSA ensure that their platforms are safeguarded against these flaws by patching and following best security practices.

- Bleeping Computer: CVE-2024-8190 Article
- The Record: CVE-2024-8190 Article
- The Hacker News: CVE-2024-8190 Article

GitLab Patches Critical SAML Authentication Bypass Vulnerability

Reported in the September 20th, 2024, FLASH Update

- GitLab has released crucial security updates to address a severe authentication bypass vulnerability that affects both its Community Edition (CE) and Enterprise Edition (EE) for self-managed installations. The flaw tracked as CVE-2024-45409 (CVSS score: 10/10), originates from improper validation within the OmniAuth-SAML and Ruby-SAML libraries, which are used to handle SAML-based authentication, a protocol allowing single sign-on (SSO) across multiple services. Specifically, the vulnerability allows an attacker to manipulate the SAML response from an identity provider (IdP) by crafting a malicious response that bypasses authentication, effectively granting unauthorized access to GitLab instances by tricking the system into recognizing the attacker as an authenticated user. The patches released by GitLab upgrade OmniAuth-SAML to version 2.2.1 and Ruby-SAML to 1.17.0, addressing the insufficient validation of key elements in SAML assertions, such as the "extern_uid" (external user ID). Although GitLab has not confirmed the active exploitation of this vulnerability in the wild, it has provided indicators of potential exploitation attempts. These signs include unusual or multiple "extern_uid" values in authentication logs, SAML-related log events, and errors such as "RubySaml::ValidationError". GitLab also advises monitoring for abnormal authentication activity, such as access attempts from unfamiliar IP addresses, which could indicate an attack. These updates come amid heightened security awareness, with the U.S. Cybersecurity and Infrastructure Security Agency (CISA) adding similar critical vulnerabilities, including one affecting Apache HugeGraph-Server, to its Known Exploited Vulnerabilities (KEV) catalog. This underscores the importance of timely patching to defend against emerging threats in the cybersecurity landscape. CTIX analysts strongly urge users running affected versions to upgrade immediately, particularly for self-managed installations, and emphasizes enabling two-factor authentication (2FA) for all accounts and disabling the SAML two-factor bypass option as temporary mitigations for those unable to update right away.
    - Bleeping Computer: CVE-2024-45409 Article
    - The Hacker News: CVE-2024-45409 Article

Critical Stack-Based Overflow Flaw Found in Microchip Advanced Software Framework (ASF) "tinydhcp" Server

Reported in the September 24th, 2024, FLASH Update

- A critical vulnerability has been identified in Microchip's Advanced Software Framework (ASF), which could allow for remote code execution (RCE) facilitated by a stack-based overflow in the implementation of the "tinydhcp" server. This flaw, tracked as CVE-2024-7490, stems from inadequate input validation of DHCP requests, carrying a high CVSS score of 9.5/10 and affecting ASF version 3.52.0.2574 and earlier versions. The CERT Coordination Center (CERT/CC) at Carnegie Mellon University issued an advisory warning that the vulnerability could be widely present in IoT devices due to its nature. The vulnerability remains unpatched, and CERT/CC recommends replacing the tinydhcp service to mitigate the risk, as the affected ASF version is no longer supported. Additionally, forks tinydhcp projects on GitHub could be similarly impacted. The disclosure of this flaw aligns with another serious vulnerability in MediaTek Wi-Fi chipsets (CVE-2024-20017), which also allows for RCE. Although MediaTek released a patch in March 2024, the risk of exploitation has increased following the release of a proof-of-concept (PoC) exploit in August 2024. Both vulnerabilities highlight significant security concerns in IoT and networking technologies. CTIX analysts urge all affected users to follow the CERT/CC guidance and replace the tinydhcp service with another one that is not vulnerable to this exploit.
    - The Hacker News: CVE-2024-7490 Article
    - Security Week: CVE-2024-7490 Article

CISA adds Critical Ivanti Virtual Traffic Manager Flaw to its Known Exploited Vulnerabilities Catalog

Reported in the September 27th, 2024, FLASH Update

- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has flagged a critical vulnerability in Ivanti's Virtual Traffic Manager (vTM) as under active exploitation and added it to its Known Exploited Vulnerabilities (KEV) catalog. This flaw, tracked as CVE-2024-7593, has a CVSS score of 9.8/10, and is due to an incorrect implementation of the authentication algorithm, allowing remote attackers to bypass authentication on Internet-exposed vTM admin panels and create rogue administrator accounts. Although Ivanti released patches in March and May 2024 to address this vulnerability, the company has confirmed that proof-of-concept (PoC) exploit code is publicly available. While Ivanti is unaware of active exploitation at the time of disclosure, it urges users to update their systems and restrict access to the management interface by binding it to private networks or trusted IPs. CISA has mandated that Federal Civilian Executive Branch (FCEB) agencies patch the vulnerability by no later than October 15, 2024, in accordance with Binding Operational Directive (BOD) 22-01, while private organizations worldwide are strongly advised to prioritize securing their systems against this flaw. Ivanti has been working on enhancing its internal security measures and disclosure processes following repeated attacks on its product lines in recent months. CTIX analysts urge any administrators impacted by this flaw to ensure that their systems are as hardened as possible to prevent exploitation.
    - Bleeping Computer: CVE-2024-7593 Article
    - Security Affairs: CVE-2024-7593 Article