TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: JANUARY 2ND, 2024

THREAT INTELLIGENCE ADVISORY REPORT

In a dynamic digital environment, individuals, businesses, and government entities are continuously facing complex cybersecurity challenges. These risks have the potential to disrupt regular operations, resulting in significant financial and reputational consequences. Therefore, it is crucial to bolster your digital defences and guard against cyber threats that could compromise the integrity, confidentiality, and availability of enterprise data.

Enhance your security measures by utilising our weekly reports, providing the latest cyber threat intelligence. Protect your IT assets from persistent threats through our comprehensive advisory services. In an era where cyber resilience is paramount, our cyber threat intelligence report equips your organisation with the essential knowledge to strengthen its security posture.

New global campaign: Lazarus group uses Log4j to deploy RATs

The North Korea-linked Lazarus Group is using a new global campaign called Operation Blacksmith. This campaign targets manufacturing, agriculture, and physical security sectors. Operation Blacksmith revolves around exploiting CVE-2021-44228, commonly known as Log4Shell, and deploying an undisclosed remote access trojan (RAT) based on DLang, with Telegram serving as its command and control (C2) channel. This breed of malware has been dubbed “NineRAT.”

The ongoing campaign displays resemblances and intersections in tooling and tactics that align with past attacks carried out by the Andariel group under Lazarus. Apart from identifying NineRAT and HazyLoad, researchers have uncovered two other distinct malware families, both rooted in DLang. One of these is a RAT family labelled “DLRAT,” while the other is a downloader referred to as “BottomLoader.” The latter is designed to fetch additional payloads, such as HazyLoad, onto a compromised endpoint.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/

INTRODUCTION
LAZARUS DEPLOYS RATS WITH LOG4J
LINUX RAT KRASUE EVADES DETECTION
APACHE STRUTS 2 VULNERABILITY
APPLE PATCHES IOS, MACOS
PHISHING ATTACKS IN GERMANY, TAIWAN
HACKERS EXPLOIT WSF FOR ASYNCRAT
MICROSOFT ADDRESSES 34 FLAWS
APT28, UAC-0050 PHISHING ATTACKS
STEALER TARGETS BROWSER DATA
KINSING, ANDARIEL ATTACK ACTIVEMQ

A new Linux RAT, Krasue, utilises embedded rootkits to evade detection

The Krasue Linux is a RAT that is primarily targeting organisations in Thailand. Equipped with multiple embedded rootkits catering to various Linux kernel versions, Krasue draws its rootkit inspiration from public sources, specifically three open-source Linux kernel module rootkits.

The rootkit's functionality extends to hooking critical functions such as the kill() syscall, network-related functions, and file listing operations. It uses a rootkit disguised as an unsigned VMware driver for discreet persistence. This allows Krasue to conceal its activities effectively, eluding detection. Notably, the malware employs real-time streaming protocol (RTSP) messages, adopting them as a camouflaged "alive ping," a tactic rarely observed in the wild. It also exhibits code similarities with XorDdos. Deployed in the later stages of an attack chain, Krasue aims to sustain access to a victim host, showcasing its strategic positioning within the broader threat landscape.

ATTACK TYPE	Malware	SECTOR	Telecommunications
REGION	Thailand	APPLICATION	Linux

Source - https://www.group-ib.com/blog/krasue-rat/

Critical RCE vulnerability detected in Apache Struts 2

Apache has issued a critical security advisory for a vulnerability in its Struts 2 web application framework. Tracked as CVE-2023-50164, it allows remote code execution (RCE). It originates from a flawed "file upload" logic. The vulnerability can facilitate unauthorised path traversals, creating a vulnerability that could be exploited in specific scenarios to upload a malicious file, thereby enabling the execution of arbitrary codes.

Struts, as a Java framework, employs the model-view-controller (MVC) architecture to craft web applications tailored for enterprise environments. The affected versions include Struts 2.3.37 (End of Life), Struts 2.5.0 - Struts 2.5.32, and Struts 6.0.0 - Struts 6.3.0. Adversaries are actively seeking to exploit the vulnerability on unpatched Apache Struts servers, leveraging a recently released proof-of-concept (PoC). Patches are available in versions 2.5.33 and 6.3.0.2 or later. Developers are strongly urged to upgrade due to the potential risk, although no current real-world exploits have been reported.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Apache Struts 2

Source - https://thehackernews.com/2023/12/new-critical-rce-vulnerability.html

Apple patches critical flaws in iOS and macOS

Apple has released comprehensive security updates for iOS, iPadOS, macOS, tvOS, watchOS, and Safari. It has addressed multiple vulnerabilities, including two zero-day vulnerabilities on older devices. The fixes include a critical keyboard spoofing flaw, identified as CVE-2023-45866. It represents a significant security concern within Bluetooth, posing the risk of an attacker, situated in a privileged network position, injecting keystrokes through keyboard spoofing. The company has also addressed two critical WebKit vulnerabilities in Safari 17.2. Tracked as CVE-2023-42890 and CVE-2023-42883, they carry the potential for arbitrary code executions and can trigger denial-of-service (DoS) conditions. The available update is compatible with Mac systems operating macOS Monterey and macOS Ventura.

Furthermore, the latest iOS version, 17.2, and its counterpart, iPadOS 17.2, have implemented contact key verification to elevate iMessage privacy. Simultaneously, the prior versions, iOS 16.7.3 and iPadOS 16.7.3, have resolved eight security issues, which encompass actively exploited vulnerabilities within WebKit.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Apple Mac OS, Apple IOS, and Apple Safari

Source - https://thehackernews.com/2023/12/apple-releases-security-updates-to.html

INTRODUCTION | LAZARUS DEPLOYS RATS WITH LOG4J | LINUX RAT KRASUE EVADES DETECTION | APACHE STRUTS 2 VULNERABILITY | APPLE PATCHES IOS, MACOS | PHISHING ATTACKS IN GERMANY, TAIWAN | HACKERS EXPLOIT WSF FOR ASYNCRAT | MICROSOFT ADDRESSES 34 FLAWS | APT28, UAC-0050 PHISHING ATTACKS | STEALER TARGETS BROWSER DATA | KINSING, ANDARIEL ATTACK ACTIVEMQ

New phishing campaigns target Germany and Taiwan with malware

A phishing campaign is targeting Germany with MrAnon Stealer, a Python-based malware. Disguised as a corporate entity seeking hotel room reservations, the phishing email carries a PDF attachment. Upon opening, the infection is triggered, prompting the recipient to download a purportedly updated version of Adobe Flash. This action, however, initiates the execution of .NET executables and PowerShell scripts, ultimately facilitating the launch of a malicious Python script. This Python script possesses the capability to extract data from various applications and transmit it to both a public file-sharing website and the threat actor’s (TA) Telegram channel. Moreover, the script is adept at capturing information from instant messaging applications, VPN clients, and files matching a specified list of extensions.

In the ongoing scenario, Mustang Panda, a group linked to China, is directing its efforts towards the Taiwanese government by employing SmugX, a novel variant of the PlugX backdoor. This underscores the perpetual evolution of cyber threats and emphasises the imperative for increased vigilance.

ATTACK TYPE	Malware	SECTOR	All
REGION	Germany and Taiwan	APPLICATION	Windows

Source - https://thehackernews.com/2023/12/new-mranon-stealer-targeting-german-it.html

INTRODUCTION | LAZARUS DEPLOYS RATS WITH LOG4J | LINUX RAT KRASUE EVADES DETECTION | APACHE STRUTS 2 VULNERABILITY | APPLE PATCHES IOS, MACOS | PHISHING ATTACKS IN GERMANY, TAIWAN | HACKERS EXPLOIT WSF FOR ASYNCRAT | MICROSOFT ADDRESSES 34 FLAWS | APT28, UAC-0050 PHISHING ATTACKS | STEALER TARGETS BROWSER DATA | KINSING, ANDARIEL ATTACK ACTIVEMQ

Hackers exploit WSF scripts for AsyncRAT delivery

The AsyncRAT malware has evolved its distribution method. It is now using Windows script file (WSF) formats disseminated through compressed (.zip) files in phishing emails. Despite countermeasures, TAs are employing innovative techniques, including “fileless” injection. The attack flow involves deceptive file attachments, with the final executed malware identified as AsyncRAT, featuring information exfiltration and backdoor capabilities.

Upon extracting the initially downloaded zip file, users encounter a file with the .wsf extension. This file primarily comprises comments, with a single <script> tag situated in the middle. Upon script execution, the Visual Basic script is downloaded and run. Subsequently, the script retrieves a .jpg file, cleverly disguised as a zip file, from the identical C2 address. Within the downloaded zip file, numerous scripts are present, alongside the Error.vbs file. The final step involves the execution of a pwng.ps1 file, which converts the encapsulated string into a .NET binary, subsequently loading and executing it. This process functions by initiating a regular process (aspnet_compiler.exe) and injecting a malicious binary into the said process.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://asec.ahnlab.com/ko/59377/

INTRODUCTION | LAZARUS DEPLOYS RATS WITH LOG4J | LINUX RAT KRASUE EVADES DETECTION | APACHE STRUTS 2 VULNERABILITY | APPLE PATCHES IOS, MACOS | PHISHING ATTACKS IN GERMANY, TAIWAN | HACKERS EXPLOIT WSF FOR ASYNCRAT | MICROSOFT ADDRESSES 34 FLAWS | APT28, UAC-0050 PHISHING ATTACKS | STEALER TARGETS BROWSER DATA | KINSING, ANDARIEL ATTACK ACTIVEMQ

Microsoft addresses 34 vulnerabilities, one zero-day flaw

This December, Microsoft has released 33 patches addressing CVEs in various products, including Windows, Office, Azure, and Microsoft Edge. The release includes four "Critical" and 29 "Important" patches, making it the lightest December release since 2017. In addition to the 18 vulnerabilities previously addressed by Microsoft in its Chromium-based Edge browser during the November 2023 Patch Tuesday updates, these fixes have been implemented.

An RCE vulnerability on the Windows MSHTML platform used by Internet Explorer has also been highlighted by Microsoft. Tracked as CVE-2023-35628, this vulnerability can be exploited by the attacker through the transmission of a specifically crafted email, which automatically triggers upon retrieval and processing by the Outlook client. Importantly, the exploitation occurs even before the email is viewed in the preview pane. To exploit this vulnerability, the attacker must send a malicious link to the victim via email or convince the user to click the link, often using enticing content in an email or on Instant Messenger. In the worst-case scenario for an email attack, the attacker can send a meticulously crafted email to the user without requiring the victim to open, read, or click on the link, potentially resulting in the execution of remote code on the victim's machine.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://thehackernews.com/2023/12/microsofts-final-2023-patch-tuesday-33.html

APT28 and UAC-0050 utilise phishing techniques for cyberattacks

The Russian state-sponsored threat group, APT28 (ITG05) is using the ongoing Middle Eastern conflict to distribute a customised backdoor named HeadLace. The campaign is targeting entities in at least 13 countries. The TA utilises genuine documents from academic, financial, and diplomatic institutions.

This campaign employs decoys strategically crafted to target European entities, specifically those with a significant role in the distribution of humanitarian aid. Certain attacks within this campaign utilise Roshal archive (RAR) compressed files. They exploit the WinRAR vulnerability, identified as CVE-2023-38831, to facilitate the spread of HeadLace. APT28's tactics have shifted towards using official documents as lures, suggesting a more targeted approach. The revelation follows a week after Microsoft, Palo Alto Networks Unit 42, and Proofpoint jointly outlined the TA's exploitation of a critical security vulnerability (CVE-2023-23397) in Microsoft Outlook. This exploitation aimed to illicitly gain access to victims' accounts within exchange servers. It also coincides with an extensive email-based phishing attack targeting Ukraine and Poland, employing the Remcos RAT and Meduza Stealer.

ATTACK TYPE	Malware	SECTOR	All
REGION	Australia, Azerbaijan, Belgium, Germany, Hungary, Italy, Latvia, Kazakhstan, Poland, Romania, Saudi Arabia, Turkey, and Ukraine	APPLICATION	Windows

Source - https://thehackernews.com/2023/12/russian-apt28-hackers-targeting-13.html

INTRODUCTION | LAZARUS DEPLOYS RATS WITH LOG4J | LINUX RAT KRASUE EVADES DETECTION | APACHE STRUTS 2 VULNERABILITY | APPLE PATCHES IOS, MACOS | PHISHING ATTACKS IN GERMANY, TAIWAN | HACKERS EXPLOIT WSF FOR ASYNCRAT | MICROSOFT ADDRESSES 34 FLAWS | APT28, UAC-0050 PHISHING ATTACKS | STEALER TARGETS BROWSER DATA | KINSING, ANDARIEL ATTACK ACTIVEMQ

New stealer targets browser passwords and cookies

A sophisticated malware campaign named Editbot Stealer has emerged. It is utilising WinRAR archive files to execute a multi-stage attack. The TAs are employing deceptive tactics, posing as a “defective product to be sent back.” They are leading users to visit fraudulent websites, via a Python-based stealer named Editbot. The stealer can extract sensitive information from browsers and execute a persistent, multi-phase attack with social media as a distribution channel.

The campaign deploys open-source code-sharing platforms like Gitlab to obtain subsequent stage payloads. The acquired payload is a recently developed Python-based stealer engineered to extract process details and information stored in browsers, including passwords, cookies, web data, and more. The exfiltration of pilfered information to the TAs is executed through a Telegram channel. This highlights the constant evolution of cyber threats and the need for heightened vigilance.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://cyble.com/blog/new-editbot-stealer-spreads-via-social-media-messages/

Kinsing and Andariel target unpatched ActiveMQ

In early November, the vulnerability CVE-2023-46604 in ActiveMQ was exploited, resulting in the deployment of the HelloKitty ransomware. The fundamental cause behind this vulnerability is the absence of validation in the deserialisation process. Input data undergoes a process known as unmarshalling, tasked with converting binary data into a format that can be utilised.

CVE-2023-46604 represents an RCE vulnerability within the Apache ActiveMQ server, an open-source messaging and integration pattern server. If an unpatched Apache ActiveMQ server is accessible from the external environment, an assailant can seize control of the system by remotely executing malicious commands. The Kinsing intrusion set specifically aimed at vulnerable ActiveMQ versions, underscoring the prevalence of the exploitation. The Andariel group also capitalised on the same vulnerability, uncovering further threats such as Ladon, NetCat, AnyDesk, and z0Miner. The incidents highlight the persistent threat to Apache ActiveMQ services, emphasising the importance of prompt patching and securing services in containerised environments for proactive defence.

ATTACK TYPE	Vulnerability, malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Apache Software Foundation ActiveMQ and Linux

Source - https://blog.sekoia.io/activemq-cve-2023-46604-exploited-by-kinsing-and-overview-of-this-threat/#h-conclusion
https://asec.ahnlab.com/ko/59786/

TATA COMMUNICATIONS

TATA

Visit one of our **Cyber Security Response Centres** to learn how we can help your enterprise navigate the complexities of today’s cyber threat landscape.

Book your visit

All content is provided AS IS and for information purposes only. Tata Communications does not make any representations or warranties of any kind, including completeness, adequacy or accuracy of such information and disclaims all liability in connection with the use of this information. The information contained herein should not be construed as a substitute for professional advice.