TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: MARCH 5TH, 2024

THREAT INTELLIGENCE ADVISORY REPORT

Cybersecurity has rapidly become one of the top priorities for organisations across the globe. As cyber threats become more sophisticated, businesses are continually striving to protect their assets and maintain operational integrity. It’s not just about protecting data anymore but also about securing the very foundation upon which modern organisations stand, making them resilient against a wide range of emerging threats.

Enhance your organisation’s cybersecurity preparedness with Tata Communications’ weekly threat intelligence advisory report. Obtain practical insights into the latest cyber threats and establish proactive measures to strengthen your defences and reduce potential risks.

VMware urges admins to update authentication methods to address security risks

VMware, a leader in virtualisation and cloud computing, has warned of critical vulnerabilities in its VMware Enhanced Authentication Plug-in (EAP). These common vulnerabilities and exposures (CVE)-2024-22245 and CVE-2024-22250, respectively, have severity scores of 9.6 and 7.8. CVE-2024-22245 could potentially mislead EAP-enabled browsers into issuing Kerberos service tickets for active directory service principal names (SPNs) without user consent. In contrast, CVE-2024-22250 could allow attackers to hijack privileged EAP sessions on Windows systems.

To mitigate these risks, VMware has advised administrators to either disable or uninstall the affected plugin and its corresponding Windows service. Additionally, the company has suggested implementing more secure authentication methods such as Active Directory over Lightweight Directory Access Protocol Secure (LDAPS) and Microsoft Active Directory Federation Services (ADFS) to enhance security and defend against potential exploits.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://www.bleepingcomputer.com/news/security/vmware-urges-admins-to-remove-deprecated-vulnerable-auth-plug-in/

New Migo malware targets Redis servers, disabling security features

A new malware named Migo is actively targeting Linux-based Redis (remote dictionary servers), employing tactics to weaken the system and perform cryptojacking by mining Monero, a type of cryptocurrency. Redis is particularly vulnerable due to its widespread use in industries requiring real-time data processing, such as technology, healthcare, and financial services. This malware exploits these servers by initially disabling key security features through command line interface (CLI) commands, such as deactivating "protected mode", allowing the malware to spread its payload more effectively.

After breaching the system, Migo proceeds to download a modified "XMRig miner", specifically tailored for Monero mining, while employing evasion strategies such as compile-time obfuscation and packaging itself as an executable compressed with ultimate packer for executables (UPX). It ensures its unnoticed presence by establishing a "systemd" service and deploying a user-mode rootkit to conceal its activities.

ATTACK TYPE	Vulnerability, Malware	SECTOR	All
REGION	Global	APPLICATION	Redis

Source - https://www.cadosecurity.com/migo-a-redis-miner-with-novel-system-weakening-techniques/

ConnectWise issues an urgent patch for a critical remote code execution

A US software company, ConnectWise, urgently resolved critical vulnerabilities discovered in its ScreenConnect, a remote desktop software. These vulnerabilities impact all versions up to 23.9.7. The first issue, CVE-2024-1709, an authentication bypass, attained the highest CVSS score of 10/10. It allows threat actors to circumvent security controls using alternative methods. Meanwhile, the second flaw, CVE-2024-1708, with a CVSS score of 8.4, exposes a path traversal vulnerability, facilitating RCE and presenting a significant security risk.

In response, the software firm promptly released emergency patches upon receiving several proof-of-concept (PoC) exploits. Investigations revealed that threat actors were establishing unauthorised administrative accounts and uploading malicious extensions to execute arbitrary code remotely, endangering sensitive data and system integrity. Additionally, ConnectWise notified its users about three internet protocol (IP) addresses associated with these exploitation attempts. The firm strongly advised all users, especially those running on-premises or self-hosted systems, to promptly apply these updates.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://www.bleepingcomputer.com/news/security/connectwise-urges-screenconnect-admins-to-patch-critical-rce-flaw/

C3RB3R ransomware spreads via Confluence server vulnerability

A severe security flaw has been discovered in Atlassian's Confluence Server and Data Centre, spanning versions 8.0.x to 8.5.3. This vulnerability, rated with a CVSS score of 10, exposes the systems to template injection risks. Threat actors have taken advantage of this by running arbitrary commands via the object-graph navigation language (OGNL). The initial wave of exploitation saw the deployment of C3RB3R ransomware, which encrypted files, created "read-me3.txt" ransom notes, and appended ".L0CK3D" extensions to compromised files. The rapid exploitation of this flaw underscores the critical need for immediate updates.

In the aftermath of the ransomware attacks, several adversaries shifted their focus to deploying crypto miner malware, specifically targeting systems to mine Monero. This change in tactics highlights attackers' adaptability and the broad range of threats emanating from a single vulnerability. It is imperative for companies to quickly implement the latest security updates to protect against the diverse risks posed by this vulnerability's exploitation.

ATTACK TYPE	Vulnerability, Ransomware	SECTOR	All
REGION	Global	APPLICATION	Atlassian Confluence

Source - https://arcticwolf.com/resources/blog/confluence-cve-2023-22527-leading-to-c3rb3r-ransomware/

Agniane Stealer malware silently targets financial information

The Agniane Stealer, a malware that emerged in August 2023, targets users' cryptocurrency wallet information. It deceives victims into downloading a zipped (ZIP) file from compromised websites. Upon extraction, this ZIP file triggers a batch (BAT) file, which in turn launches a PowerShell script. This script, made complex by ConfuserEx obfuscation, makes detection and analysis difficult. It creates a payload, encrypted with Exclusive OR (XOR), capable of circumventing standard security measures through advanced anti-sandbox techniques.

In its execution, the Agniane Stealer shows an advanced level of command-and-control (C2) communication, allowing it to deliver precise instructions for infiltrating systems and stealing sensitive data, including cryptocurrency credentials. The malware's dissemination via a Telegram channel to cybercriminals not only widens its distribution but also indicates a highly organised marketplace for malicious software.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://blogs.cisco.com/security/agniane-stealer-information-stealer-targeting-cryptocurrency-users

China-linked hackers target Asia with “DOPLUGS” malware

Mustang Panda, a cyberespionage group with ties to China, has been launching sophisticated cyberattacks across Asia, deploying a variant of the PlugX malware known as “DOPLUGS”. This advanced backdoor discreetly breaches systems to execute remote commands. Notably, the malware incorporates the “KillSomeOne” plugin, enhancing its ability to spread malware, collect data, and steal documents, especially via Universal Serial Bus (USB) drives.

Moreover, by initiating spear-phishing campaigns and using dynamic link library (DLL) side-loading techniques, Mustang Panda showcases its intricate operational methods. Targeting regions including India, Taiwan, Vietnam, Hong Kong, Japan, Malaysia, Mongolia, and even China, the group employs DOPLUGS to secretly access sensitive information. This extensive espionage activity impacts national security, economic stability, and diplomatic relations across the region.

ATTACK TYPE	Malware	SECTOR	Government
REGION	Asia	APPLICATION	Windows

Source - https://thehackernews.com/2024/02/mustang-panda-targets-asia-with.html

INTRODUCTION | VMWARE ISSUES SECURITY ALERTS | MIGO MALWARE HITS REDIS | CONNECTWISE RELEASES CRITICAL PATCHES | C3RB3R RANSOMWARE EXPLOITS CONFLUENCE | AGNIANE STEALER TARGETS FINANCIAL INFO | CHINA HACKERS DEPLOY “DOPLUGS” | DPR KOREA BACKDOORS THE RUSSIAN GOVT. | ANONYMOUS SUDAN STRIKES UAE SATS | LOCKBIT RANSOMWARE RESURFACES | SCREENCONNECT IN PHISHING ATTACKS

North Korean hackers target Russian government with backdoored software

A cyberespionage attack has compromised software used by the Russian Ministry of Foreign Affairs (MID), deploying Konni, a remote access trojan (RAT) also known as UpDog. This operation, linked to the Democratic People's Republic of Korea (DPRK), specifically targeted the “Statistika KZU” tool, essential for MID’s secure internal communications. Threat actors altered the software’s Microsoft Installer (MSI) file, a strategic move to infiltrate Russian systems and exfiltrate sensitive data.

Upon activation, the modified MSI file connects to a C2 server, initiating a series of unauthorised actions. Since 2014, DPRK-affiliated groups, including Kimsuky and ScarCruft (APT37), have utilised Konni RAT for espionage, demonstrating its effectiveness in cyber operations. However, how these threat actors acquired the installer remains undisclosed.

ATTACK TYPE	Malware, Cyberespionage	SECTOR	Government
REGION	Russia	APPLICATION	Windows

Source - https://thehackernews.com/2024/02/russian-government-software-backdoored.html

INTRODUCTION | VMWARE ISSUES SECURITY ALERTS | MIGO MALWARE HITS REDIS | CONNECTWISE RELEASES CRITICAL PATCHES | C3RB3R RANSOMWARE EXPLOITS CONFLUENCE | AGNIANE STEALER TARGETS FINANCIAL INFO | CHINA HACKERS DEPLOY “DOPLUGS” | DPR KOREA BACKDOORS THE RUSSIAN GOVT. | ANONYMOUS SUDAN STRIKES UAE SATS | LOCKBIT RANSOMWARE RESURFACES | SCREENCONNECT IN PHISHING ATTACKS

Anonymous Sudan claims responsibility for targeting UAE satellites

Tata Communication's Threat Intelligence Team has identified a significant threat targeting United Arab Emirates' Thuraya Communications, a leading provider in the mobile satellite service industry. The team believes that the source of this threat is the Anonymous Sudan group, known for carrying out distributed denial-of-service (DDoS) attacks against various Western organisations and governmental bodies, and for its pro-Islamic and pro-Russian ideologies. Allegedly, they are retaliating against the UAE's support for Sudan's Rapid Support Forces, accused of serious crimes. These attackers have also claimed responsibility for a series of assaults on satellite operations, leading to disruptions in TV broadcasts.

This specific attack on Thuraya severely disrupted its operational capabilities, rendering its online platform non-functional. Although the company managed to promptly restore its services, the financial toll is expected to be significant. Such incidents underscore the critical need for robust cybersecurity measures within the satellite communication sector.

ATTACK TYPE	Hacktivism, DDOS	SECTOR	All
REGION	UAE	APPLICATION	Generic

Source - NA

LockBit ransomware returns, with increased attacks on government entities

After law enforcement disrupted its network, the notorious ransomware group LockBit quickly rebuilt its operations, setting up new infrastructure and signalling an ongoing threat, especially to government entities. Although "Operation Cronos" took down their network, including 34 servers, the threat actors have revealed plans to strengthen their methods for cyberattacks.

The group also acknowledged that neglecting updates on their hypertext preprocessor (PHP) servers led to a compromise through the CVE-2023-3824 vulnerability. In response, LockBit has improved its security measures and now offers rewards for identifying vulnerabilities in its updated system. They are shifting towards a decentralised model to better protect affiliate panels across various servers, aiming to reduce the chances of future disruptions. This strategy highlights LockBit's determination to persist with its ransomware activities, despite aggressive crackdowns by law enforcement.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://www.bleepingcomputer.com/news/security/lockbit-ransomware-returns-restores-servers-after-police-disruption/

ScreenConnect is used in phishing attacks on healthcare and crypto users

Cybersecurity experts recently exposed a phishing campaign that threat actors have launched, targeting the cryptocurrency and healthcare sectors in the US. These threat actors are exploiting ConnectWise ScreenConnect, a popular remote access and administration software, to carry out their attacks. They craft sophisticated phishing websites and execute subdomain takeovers to deceive individuals into installing compromised ScreenConnect clients.

The success of this campaign is largely attributed to the cybercriminals' ability to convincingly impersonate legitimate cryptocurrency services and healthcare providers, thereby increasing the chances of individuals falling prey to their schemes. Once the malicious ScreenConnect client is installed, the malicious actors gain unauthorised access, exposing the system to a myriad of threats. These include severe data breaches, malware outbreaks, and interruptions to essential services, highlighting the urgent necessity for enhanced cybersecurity vigilance and the implementation of stringent security measures.

ATTACK TYPE	Phishing	SECTOR	Healthcare/hospitals
REGION	United States	APPLICATION	Apple's macOS, Windows, Linux

Source - https://cyble.com/blog/ongoing-phishing-campaign-targets-healthcare-and-cryptocurrency-users-via-screenconnect/

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.