TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: June 25, 2024

THREAT INTELLIGENCE ADVISORY REPORT

As the digital landscape is constantly evolving, cyber threats are also evolving with equal vigour. Companies worldwide are focusing on safeguarding their data and strengthening their core security frameworks. Staying updated on emerging cyberattack trends and promptly implementing security updates is vital for any organisation to protect its resources from potential threats.

Tata Communications' weekly threat intelligence advisory has been designed to help you stay ahead of the curve. By providing insights into the latest cyber risks, this report empowers you to implement proactive strategies to strengthen your defences and effectively mitigate potential vulnerabilities.

Critical authentication bypass flaw in Veeam Backup software

Veeam has released a proof-of-concept exploit for a severe authentication bypass flaw in Veeam Backup Enterprise Manager (CVE-2024-29849). The vulnerability allows remote attackers to log in as any user via a flawed REST API service. Veeam advises upgrading to version 12.1.2.172 or following recommended security measures to mitigate the threat.

The flaw involves sending a VMware SSO token to the vulnerable service using the Veeam API. This token bypasses authentication checks, granting attackers administrator access. No active exploitation of CVE-2024-29849 has been reported yet. Still, admins are urged to restrict access to the VBEM web interface, implement firewall rules, enable multi-factor authentication, deploy a web application firewall, and monitor access logs to mitigate potential threats.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Generic, Veeam

Source- https://www.bleepingcomputer.com/news/security/exploit-for-critical-veeam-auth-bypass-available-patch-now/

ALPHV ransomware leverages RDP and ScreenConnect

A sophisticated ransomware attack, starting with a phishing email, has emphasised the urgent need for robust cybersecurity measures. Hackers initially delivered the IcedID malware, followed by installing remote control software and lateral movement through Cobalt Strike and CSharp Streamer RAT. Over eight days, they extracted sensitive data before deploying the ALPHV ransomware.

The attackers used ScreenConnect for remote control, wmiexec for lateral movement, and rclone for data extraction. They persisted in their attack by using scheduled tasks and process injections, ultimately locking crucial data until a ransom was paid. The initial access vector was a malicious email tricking victims into downloading an obfuscated IcedID loader. This sophisticated method allowed the attackers to gain control, move laterally, and deploy ransomware, highlighting the need for businesses to implement stringent cybersecurity protocols.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source- https://gbhackers.com/alphv-ransomware-rdp-screenconnect-deployment/

SSLoad malware uses advanced techniques for surveillance and evasion

Recent reports reveal that SSLoad, a sophisticated malware, has been infiltrating systems through phishing emails. It features a unique loader and a Rust-based downloader, highlighting its adaptability and evasive nature. The malware's initial vector often involves a Word document delivering an SSLoad DLL, which executes Cobalt Strike. Another method includes phishing emails leading to a fake Azure page, which downloads a JavaScript script that ultimately loads the SSLoad payload.

The malware's complexity and use in Malware-as-a-Service operations highlight the need for advanced threat detection. SSLoad's adaptability and sophisticated techniques, such as dynamic string decryption and anti-debugging measures, make it a significant threat. This underscores the necessity for businesses to implement robust cybersecurity measures to combat advancing malware campaigns effectively.

ATTACK TYPE	Malware	SECTOR	Information technology, healthcare, manufacturing, construction, government, oil and gas, defence, e-commerce, BFSI, airlines and aviation, telecommunications
REGION	Global	APPLICATION	Windows

Source- https://intezer.com/blog/research/ssload-technical-malware-analysis/

Chinese hackers launch sophisticated ValleyRAT attack

ValleyRAT, a remote access trojan first reported in early 2023, has resurfaced in a new campaign by a China-based threat actor. The latest version employs advanced techniques like anti-virus evasion, DLL sideloading, and process injection to compromise systems. The attack begins with a downloader retrieving files from an HTTP File Server (HFS). It progresses through multiple stages involving decryption and memory injection to ultimately deploy ValleyRAT.

This updated variant includes improved device fingerprinting, new bot ID generation methods, and additional commands. These advancements highlight the evolving threat posed by ValleyRAT. Its multi-stage delivery mechanism and sophisticated obfuscation tactics make it a formidable challenge for security systems. The campaign's complexity and technical sophistication highlight the persistent and growing threat from state-sponsored threat actors.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source- https://www.zscaler.com/blogs/security-research/technical-analysis-latest-variant-valleyrat

Arm issues urgent fix for exploited GPU vulnerability

Arm has released a security update for a critical vulnerability (CVE-2024-4610) in its Bifrost and Valhall GPU kernel drivers, affecting versions r34p0 to r40p0. The use-after-free flaw allows local non-privileged users to access freed memory, posing significant security risks. Despite being fixed in version r41p0 in November 2022, the issue was recently reclassified as a vulnerability, following new information from an external researcher.

Arm has confirmed that the flaw is actively being exploited but withheld specific details to prevent further abuse. Previously, similar vulnerabilities in Mali GPU drivers were used by commercial spyware vendors in targeted attacks on Android devices. Users are urged to update to the latest driver version r49p0, released in April 2024, to mitigate potential threats.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source- https://thehackernews.com/2024/06/arm-warns-of-actively-exploited-zero.html

INTRODUCTION | VEEAM BACKUP FLAW EXPOSED | ALPHV RANSOMWARE STRIKES | SSLOAD MALWARE ATTACKS SYSTEMS | VALLEYRAT RESURFACES | ARM ISSUES URGENT FIX | SECSHOW GROUP POSES THREATS | MICROSOFT PATCHES FLAWS | WARMCOOKIE TARGETS PROFESSIONALS | HACKERS EXPLOIT MSC FILES | NOODLE RAT TARGETS LINUX SERVERS

Cyberespionage group SecShow and Rebirth botnet pose new threats

Cybersecurity researchers have uncovered the activities of SecShow, a Chinese cyberespionage group conducting extensive global DNS probing since June 2023. Operating from the China Education and Research Network (CERNET), SecShow seeks to exploit DNS servers by probing open resolvers, potentially for malicious purposes. The true extent and aim of their operations remain unclear.

Simultaneously, a new DDoS-as-a-Service botnet, Rebirth, has emerged, targeting the gaming community. Using Mirai malware, Rebirth disrupts game servers through TCP and UDP attacks. Advertised on Telegram and an online store, it offers various plans to facilitate these attacks. This botnet highlights the increasing threat of DNS and DDoS attacks, underscoring the urgent need for strong cybersecurity measures.

ATTACK TYPE	Malware	SECTOR	Information technology, healthcare, financial services, manufacturing, construction, oil and gas, defence, e-commerce, BFSI, airlines and aviation, telecommunications
REGION	Global	APPLICATION	Generic

Source- https://thehackernews.com/2024/06/chinese-actor-secshow-conducts-massive.html

Microsoft patches fifty-one vulnerabilities including KeyTrap zero-day

Microsoft's June 2024 Patch Tuesday addressed 51 security vulnerabilities, including one critical flaw and the publicly disclosed KeyTrap zero-day in the DNS protocol. The release fixed 18 remote code execution (RCE) vulnerabilities, 25 elevation of privilege flaws, and 3 information disclosure issues.

The critical RCE vulnerability was found in Microsoft Message Queuing (MSMQ). Notable patches include several Microsoft Office RCE flaws, such as those in Microsoft Outlook, which can be exploited from the preview pane, and seven privilege elevation flaws in Windows Kernel. The KeyTrap vulnerability tracked as CVE-2023-50868 affected DNSSEC validation, potentially causing denial-of-service attacks. This flaw has now been patched in multiple DNS integrations, including PowerDNS and BIND. Overall, this month's updates emphasise the importance of applying patches promptly to mitigate potential security risks.

ATTACK TYPE	Vulnerability	SECTOR	Healthcare, financial services, manufacturing, construction, government, defence, e-commerce, airline, BFSI, telecommunications
REGION	Global	APPLICATION	Windows

Source- https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2024-patch-tuesday-fixes-51-flaws-18-rces/

INTRODUCTION | VEEAM BACKUP FLAW EXPOSED | ALPHV RANSOMWARE STRIKES | SSLOAD MALWARE ATTACKS SYSTEMS | VALLEYRAT RESURFACES | ARM ISSUES URGENT FIX | SECSHOW GROUP POSES THREATS | MICROSOFT PATCHES FLAWS | WARMCOOKIE TARGETS PROFESSIONALS | HACKERS EXPLOIT MSC FILES | NOODLE RAT TARGETS LINUX SERVERS

Warmcookie malware targets corporate networks through fake job offers

A new malware, Warmcookie, spread via phishing campaigns disguised as job offers poses a significant threat to corporate networks. The malware exhibits advanced capabilities such as machine fingerprinting, screenshot capturing, and deploying additional malicious payloads.

The phishing emails, crafted to appear as personalised job offers, lure recipients to fake recruitment platforms. These fake pages prompt users to download a heavily obfuscated JavaScript file, which executes a PowerShell script to download and run the Warmcookie DLL. Once installed, Warmcookie creates a scheduled task to maintain persistence and communicates with its command-and-control server to begin machine fingerprinting. It can collect detailed system information, capture screenshots, execute commands, and drop additional files. Experts urge users to stay vigilant and implement robust security measures to counter this sophisticated malware threat.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source- https://www.bleepingcomputer.com/news/security/new-warmcookie-windows-backdoor-pushed-via-fake-job-offers/

Hackers exploit MSC files in sophisticated attacks

Hackers are increasingly exploiting Microsoft Management Console (MSC) files to gain unauthorised access to systems, cybersecurity experts warn. These files, typically used for administrative commands, are manipulated to resemble legitimate files, allowing them to bypass security measures and deploy malware. The "Operation Control Plug" campaign by the hacking group DarkPeony is a notable example. This group targets military and government organisations in Myanmar, the Philippines, Mongolia, and Serbia.

DarkPeony's sophisticated multi-stage attacks begin with malicious MSC files, which prompt users to execute a PowerShell script. This script downloads an MSI package that contains a legitimate executable capable of DLL side-loading. The side-loaded DLL then decodes and loads a malicious payload, ultimately deploying the PlugX malware. Researchers urge organisations to enhance their detection capabilities to counter these increasingly sophisticated threats, as MSC file abuse may become more prevalent in future attacks.

ATTACK TYPE	Malware	SECTOR	Government, defence
REGION	Mongolia, Myanmar, the Philippines, Serbia	APPLICATION	Windows

Source- https://gbhackers.com/hackers-weaponizing-msc-files/

Noodle RAT malware targets Linux servers in espionage campaigns

Cybersecurity experts have uncovered Noodle RAT, a sophisticated malware targeting Linux servers. This malware has been used by Chinese-speaking hacker groups for espionage and cybercrime since 2016. Noodle RAT has distinct versions for Windows and Linux, revealing extensive capabilities for file manipulation, reverse shell access, and encrypted command communication.

Recent findings highlight that Noodle RAT, also known as ANGRYREBEL, has been active but often misidentified. Since 2020, it has targeted countries such as Thailand, India, Japan, Malaysia, and Taiwan. The malware's capabilities include downloading and uploading files, running additional modules, and SOCKS tunnelling. Noodle RAT shares similarities with other malware like Gh0st RAT and Rekoobe but is distinct enough to be classified separately. Its control panels and builders indicate a sophisticated ecosystem. This signifies the importance of heightened vigilance and robust cybersecurity measures, particularly for Linux/Unix systems.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Linux

Source- https://gbhackers.com/noodle-rat-to-attack-linux-servers/

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.