TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: June 18, 2024

THREAT INTELLIGENCE ADVISORY REPORT

Cyber threats pose a persistent challenge for enterprises globally. Focussing on data security only is not enough anymore. Building and maintaining a robust security foundation is important for businesses to safeguard their operational framework. The key to success lies in resilience.
Tata Communications' weekly threat intelligence advisory is your key to staying ahead of the curve.

By leveraging our insights into the latest cyber risks, you can implement proactive strategies to strengthen your defences and effectively mitigate potential vulnerabilities. Gain invaluable intelligence and elevate your organisation's overall cybersecurity posture, ensuring business continuity and success.

Critical RCE flaw in PHP affects all versions for Windows

On May 7, 2024, researchers reported a critical remote code execution vulnerability, tracked as CVE-2024-4577, in the PHP programming language. This flaw affects all PHP versions for Windows since version 5.x and potentially enables unauthorised attackers to gain complete control of affected PHP servers. A patch was released but widespread deployment challenges may leave many systems exposed.

The flaw arises from an oversight in handling character encoding conversions in CGI mode. This allows attackers to bypass previous protections and execute arbitrary code. XAMPP installations on Windows are particularly vulnerable. Admins are advised to upgrade to patched versions PHP 8.3.8, PHP 8.2.20, or PHP 8.1.29 or disable the PHP CGI feature. System administrators should also consider migrating to more secure alternatives such as FastCGI, PHP-FPM, or Mod-PHP.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	PHP

Source- https://www.bleepingcomputer.com/news/security/php-fixes-critical-rce-flaw-impacting-all-versions-for-windows/

Cyberespionage campaign SickSync targets defence forces

The Ukrainian Computer Emergency Response Team (CERT-UA) has issued a warning against a cyberespionage campaign named "SickSync" targeting the nation's defence forces. The campaign is attributed to the UAC-0020 (Vermin) hacking group, operating under Luhansk's law enforcement. The attackers use spear-phishing emails containing a RAR archive, which includes a decoy PDF and a trojan SyncThing application.

The campaign uses a malware called SPECTR, active since 2019, to exploit SyncThing's standard sync functionality to steal sensitive data. Once activated, it captures screenshots, collects files, extracts data from USB drives, and steals credentials from web browsers and applications like Signal and Skype. The stolen data is transferred to the attacker via SyncThing's synchronisation process. CERT-UA provides detailed indicators of compromise and recommends monitoring network indicators for suspicious activity related to SyncThing infrastructure.

ATTACK TYPE	Malware	SECTOR	Defence
REGION	Ukraine	APPLICATION	Windows

Source- https://securityaffairs.com/164250/intelligence/spectr-malware-used-in-sicksync-campaign.html

Muhstik botnet exploits Apache RocketMQ flaw

The Muhstik botnet is exploiting a critical vulnerability in Apache RocketMQ, identified as CVE-2023-33246, to hijack servers and expand its reach. This flaw, disclosed over a year ago, remains unpatched on many servers, enabling remote code execution. Muhstik targets Linux servers and IoT devices for DDoS attacks and cryptocurrency mining. The botnet uses a shell script from a remote IP to download the Muhstik malware binary and ensures persistence by copying to multiple directories and modifying system files.

Despite the disclosure of the vulnerability, over 5,000 instances of Apache RocketMQ remain exposed. Organisations are urged to update to the latest version to mitigate these risks. Additionally, securing MS-SQL servers against brute-force attacks and ensuring regular password updates are essential to prevent further exploitation.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source- https://thehackernews.com/2024/06/muhstik-botnet-exploiting-apache.html

INTRODUCTION | RCE FLAW AFFECTS PHP | SICKSYNC TARGETS DEFENCE FORCES | MUHSTIK EXPLOITS APACHE ROCKETMQ | WORDPRESS FLAW AFFECTS THOUSANDS | CRIMSON PALACE LAUNCHES ATTACKS | TARGETCOMPANY FOR LINUX EMERGES | FOG RANSOMWARE ATTACKS ENTERPRISES | RANSOMHUB EMERGES FROM KNIGHT | AGENT TESLA VARIANT ATTACKS | SAPPHIRE WEREWOLF TARGETS BUSINESSES

Critical vulnerability in WordPress plugin affects thousands of sites

A severe security flaw, CVE-2024-4295, has been discovered in the popular WordPress plugin Email Subscribers. This unauthenticated SQL injection vulnerability has a CVSS severity rating of 9.8, making it highly exploitable. The flaw allows attackers to inject malicious code into database queries, potentially leading to significant data breaches. With over 90,000 active installations, the vulnerability poses a substantial risk.

The issue stems from insufficient escaping of user input via the 'hash' parameter and inadequate preparation of SQL queries. This can allow attackers to append their own SQL commands, compromising website security. Users are urged to update to version 5.7.21 or later immediately to protect sensitive information. They should review their databases for unauthorised access and implement additional security measures, such as web application firewalls and intrusion detection systems, to mitigate risks.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	WordPress

Source- https://securityonline.info/cve-2024-4295-critical-vulnerability-in-popular-wordpress-plugin-exposes-90k-sites/

Cyberespionage campaign attacks prominent government agency

A sophisticated Chinese state-sponsored cyberespionage campaign called "Crimson Palace" has targeted an unnamed Southeast Asian government agency since March 2023. The campaign, aiming to support Chinese state interests, involves advanced malware and three distinct activity clusters, indicating a coordinated operation. Researchers identified the campaign's goal as maintaining network access to gather sensitive military and technical data. They suspect the targeted nation is involved in territorial conflicts with China, possibly the Philippines.

Crimson Palace comprises three clusters: Alpha, Bravo, and Charlie. These clusters use various malware, including PocoProxy and EAGERBEE, and employ novel evasion techniques such as DLL side-loading. Cluster Alpha focuses on server subnet mapping and Active Directory reconnaissance. Cluster Bravo uses valid accounts for lateral movement. Cluster Charlie deploys PocoProxy for persistence and HUI Loader to deliver Cobalt Strike. The campaign's complexity highlights the need for cutting-edge cybersecurity measures to protect critical infrastructure from state-sponsored threats.

ATTACK TYPE	Malware	SECTOR	Government
REGION	Southeast Asia	APPLICATION	Windows

Source- https://thehackernews.com/2024/06/chinese-state-backed-cyber-espionage.html

INTRODUCTION | RCE FLAW AFFECTS PHP | SICKSYNC TARGETS DEFENCE FORCES | MUHSTIK EXPLOITS APACHE ROCKETMQ | WORDPRESS FLAW AFFECTS THOUSANDS | CRIMSON PALACE LAUNCHES ATTACKS | TARGETCOMPANY FOR LINUX EMERGES | FOG RANSOMWARE ATTACKS ENTERPRISES | RANSOMHUB EMERGES FROM KNIGHT | AGENT TESLA VARIANT ATTACKS | SAPPHIRE WEREWOLF TARGETS BUSINESSES

Linux variant of ransomware targets VMware ESXi

Researchers have discovered a new Linux variant of the TargetCompany ransomware, specifically targeting VMware ESXi environments using a custom shell script. This variant, also known as Mallox, FARGO, and Tohnichi, has been active since June 2021. It previously targeted databases but has now shifted focus to VMware ESXi machines, demonstrating advanced attack strategies. The ransomware ensures administrative privileges before executing its payload, moves data to multiple servers for redundancy, and encrypts files with VM-related extensions. A ransom note is then left with instructions for decryption.

Researchers attribute these attacks to an affiliate named "Vampire" and recommend enabling multi-factor authentication, creating regular backups, and keeping systems updated to mitigate such threats. The shift to targeting ESXi environments indicates the ransomware's changing tactics. Researchers stress the importance of innovative cybersecurity measures to protect against these sophisticated attacks.

ATTACK TYPE	Ransomware	SECTOR	IT
REGION	Global	APPLICATION	VMWare ESXi, Linux

Source- https://www.bleepingcomputer.com/news/security/linux-version-of-targetcompany-ransomware-focuses-on-vmware-esxi/

Fog ransomware targets education and recreation sectors

On May 2, 2024, a new ransomware variant named Fog began targeting organisations in the US, particularly in the education and recreation sectors. The attackers use compromised VPN credentials to gain access and employ sophisticated techniques such as pass-the-hash and credential stuffing to infiltrate systems. The ransomware encrypts files and disables defences without extracting data, differing from the recent trend of double or triple extortion tactics. Instead, Fog seeks quick payouts by swiftly encrypting data stored in virtual environments like Hyper-V and Veeam.

Four out of five reported attacks have affected educational institutions, exploiting their often underfunded and understaffed IT departments. Researchers emphasise the importance of advanced security measures and secure backups to mitigate such threats, suggesting better credential management to prevent lateral movement and privilege escalation by attackers.

ATTACK TYPE	Ransomware	SECTOR	Education
REGION	US	APPLICATION	Windows

Source- https://www.darkreading.com/threat-intelligence/fog-ransomware-rolls-in-to-target-education-recreation-sectors

INTRODUCTION | RCE FLAW AFFECTS PHP | SICKSYNC TARGETS DEFENCE FORCES | MUHSTIK EXPLOITS APACHE ROCKETMQ | WORDPRESS FLAW AFFECTS THOUSANDS | CRIMSON PALACE LAUNCHES ATTACKS | TARGETCOMPANY FOR LINUX EMERGES | FOG RANSOMWARE ATTACKS ENTERPRISES | RANSOMHUB EMERGES FROM KNIGHT | AGENT TESLA VARIANT ATTACKS | SAPPHIRE WEREWOLF TARGETS BUSINESSES

RansomHub emerges from Knight ransomware

A new ransomware strain, RansomHub, has emerged from the Knight ransomware, which originated from Cyclops. RansomHub targets multiple operating systems using sophisticated techniques such as double extortion and obfuscation. Researchers revealed that RansomHub first appeared in February 2024 and has since been linked to high-profile attacks on organisations like Change Healthcare, Christie's, and Frontier Communications. The ransomware employs strategic targeting and advanced evasion tactics, including exploiting known security flaws like ZeroLogon.

RansomHub’s payload, written in Go, is noted for its obfuscation and ability to restart hosts in safe mode before encryption. It uses stolen credentials for initial access and deploys remote desktop software before launching its attack. Experts recommend robust security measures, including multi-factor authentication, regular backups, and timely security updates, to defend against such adaptive and persistent cyber threats.

ATTACK TYPE	Ransomware	SECTOR	Healthcare
REGION	Global	APPLICATION	----

Source- https://thehackernews.com/2024/06/rebranded-knight-ransomware-targeting.html

New Agent Tesla variant targets users in phishing campaign

Researchers have identified a sophisticated phishing campaign targeting Spanish-speaking individuals. This operation uses a phishing email disguised as a SWIFT transfer notification, containing an Excel attachment that exploits MS Office vulnerabilities. The Excel attachment leverages CVE-2017-0199 and CVE-2017-11882 vulnerabilities and employs fileless techniques and JavaScript and PowerShell scripts to deliver the Agent Tesla Remote Access Trojan (RAT). Once installed, the malware steals extensive user data, including login credentials, banking details, and email contacts from over 80 software applications. It also captures keystrokes and screenshots and moves the stolen data to an FTP server.

Researchers warn that the malware evades detection by running fileless and detecting analysis environments. To mitigate risks, users are advised to remain cautious of phishing emails, regularly update their systems, use strong passwords, and invest in reputed anti-malware solutions.

ATTACK TYPE	Malware	SECTOR	All
REGION	Spain	APPLICATION	Windows

Source- https://hackread.com/phishing-campaign-stealthy-jpgs-drop-agent-tesla/

Sapphire Werewolf cyberespionage campaign attacks industries

Since March 2024, the Sapphire Werewolf cyberespionage campaign has targeted various Russian industries, using an advanced version of the SapphireStealer malware known as Amethyst. This campaign has resulted in over 300 attacks, aiming to harvest employee authentication data. Attackers disguise their phishing emails as official documents to infiltrate systems and steal sensitive information. The sophisticated techniques employed by Sapphire Werewolf include the use of scheduled tasks and decoy documents to maintain persistence. Amethyst helps attackers in executing these advanced strategies.

Industries affected include education, manufacturing, IT, defence, and aerospace engineering. The campaign sheds light on the adaptive and persistent nature of modern cyber threats, highlighting the necessity for strict cybersecurity measures. Organisations are urged to stay vigilant against phishing attempts and to strengthen their security protocols to mitigate risks.

ATTACK TYPE	Malware	SECTOR	Manufacturing, IT, Education, Aerospace, Defence Industry
REGION	Russia	APPLICATION	Windows

Source- https://thehackernews.com/2024/06/sticky-werewolf-expands-cyber-attack.html

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.