TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: JULY 30, 2024

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As the digital domain grows, so do the related cyber threats, which become more complex. Organisations throughout the globe are prioritising data protection and strengthening their basic security mechanisms. Keeping up with new cyberattack trends and quickly installing security patches is essential for any organisation wishing to protect its resources from potential threats.

Tata Communications' weekly threat intelligence advisory is designed to help you stay ahead. This research provides insights into the most recent cyber hazards, helping you apply proactive techniques to strengthen your defences and successfully minimise potential vulnerabilities.

HUSKY Plugin flaw exposes WooCommerce stores

A critical vulnerability (CVE-2024-6457) has been found in the HUSKY – Products Filter Professional for WooCommerce plugin. This flaw exposes more than 100,000 WooCommerce-powered stores to SQL injection attacks. It allows attackers to inject malicious SQL queries into the plugin's database, potentially enabling them to steal customer data, tamper with products or disrupt store operations. This severe flaw, with a CVSS score of 9.8, affects versions 1.3.6 and below.

Since attackers can potentially gain complete control of the database, immediate action is essential. Store owners are advised to update to version 1.3.6.1 or later of the plugin immediately to address this issue. Experts also recommend conducting a security audit after the update to ensure no malicious code was injected during the vulnerability window.

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

Source - https://securityonline.info/cve-2024-6457-cvss-9-8-critical-flaw-in-husky-plugin-threatens-100k-woocommerce-stores/

Critical Apache HugeGraph vulnerability actively exploited

A critical security flaw (CVE-2024-27348) in Apache HugeGraph-Server is being actively exploited, risking remote code execution attacks. It has a CVSS score of 9.8, indicating a severe risk. It has been described as a remote command execution flaw in the Gremlin graph traversal language API. It allows attackers to potentially take complete control of servers.

This vulnerability is particularly concerning because attackers can bypass sandboxing and steal data, disrupt operations or install malware. Users are urged to upgrade to version 1.3.0 with Java11 immediately and enable the Auth system, which fixes the issue. As the exploit codes are publicly available and the attacks are ongoing, implementing additional security features such as authentication and access restrictions is crucial.

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

Source - https://thehackernews.com/2024/07/critical-apache-hugegraph-vulnerability.html

Chinese hackers target organisations with malware

Chinese hacking group APT17 is targeting Italian companies and government entities with an advanced variant of the 9002 RAT malware. Two attacks, perpetrated on June 24 and July 2, 2024, used spear-phishing campaigns to distribute a malicious Skype for Business installer, infecting user systems. This modular trojan facilitates extensive cyberespionage, including network monitoring and remote command execution.

The malware appears to be constantly updated with diskless variants. It is composed of various modules that are activated as needed by the threat actor to reduce the possibility of interception. Immediate attention to security measures is advised. Experts recommend regularly updating and patching all devices, including operating systems and software applications, to address known security vulnerabilities exploited by APT17.

ATTACK TYPE	Malware	SECTOR	All
REGION	Italy	APPLICATION	Windows

Source - https://thehackernews.com/2024/07/china-linked-apt17-targets-italian.html

Scattered Spider adopts new ransomware strains

Microsoft reports that the cybercriminal group Scattered Spider have added RansomHub and Qilin ransomware to their cyberattack arsenal to diversify their attacks. This group, noted for their sophisticated social engineering, previously targeted VMware ESXi servers with BlackCat ransomware. Scattered Spider shares overlaps with activity clusters widely known as 0ktapus, Octo Tempest, Golden Harvest, and UNC3944.

Scattered Spider's adoption of new ransomware underscores the rising threat of diverse malware families. The rise of new ransomware strains highlights the need for strong cybersecurity measures, including user education on social engineering tactics and regular system backups, to protect all sectors from these evolving attacks. Organisations should consider implementing a layered security approach that combines endpoint detection and response (EDR) solutions and network segmentation to further mitigate the risk of ransomware infections.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://thehackernews.com/2024/07/scattered-spider-adopts-ransomhub-and.html

Cybercrime group FIN7 selling security-breaching tool

FIN7, a cybercrime group of Russian and Ukrainian origin active since 2012, is back in the news for selling a tool called AvNeutralizer on dark web forums. The updated version of AvNeutralizer employs anti-analysis techniques. This tool disables security software, making it easier for the threat actors to launch attacks. It leverages a Windows built-in driver called "ProcLaunchMon.sys" in conjunction with the Process Explorer driver to tamper with the functioning of security solutions and evade detection.

FIN7 also refines its phishing and malvertising techniques, while using automated SQL injection attacks. This adaptability makes them a significant threat to organisations globally. Users are urged to keep all software, especially security software and operating systems, updated with the latest patches. Experts also recommend implementing strong email filtering and educating employees on identifying phishing attempts.

ATTACK TYPE	Malware	**SECTOR**	Military
REGION	Global	**APPLICATION**	Windows

Source - https://thehackernews.com/2024/07/fin7-group-advertises-security.html

TAG-100 targets high-profile entities worldwide

Cybersecurity experts have reported a new cyberespionage group TAG-100 launching espionage attacks against high-profile government, intergovernmental, and trade organisations across Asia Pacific. TAG-100 exploits common vulnerabilities in internet-facing apps such as Citrix and Exchange servers. The group then uses open-source malware (Pantegana and SparkRAT) to maintain access. TAG-100 maintains persistent access across Windows and Linux systems, allowing for long-term data collection and potential disruption.

While the exact identity of TAG-100 group remains unknown, the nature of their targets and tactics suggests a potential link to state-sponsored threat actors. Experts suggest patching all systems promptly and prioritising updates for known vulnerabilities exploited by TAG-100. They also recommend implementing multi-factor authentication (MFA) to add an extra layer of security for remote access.

ATTACK TYPE	Malware	**SECTOR**	Government, trading
REGION	APAC	**APPLICATION**	Windows, Linux

Source - https://securityonline.info/tag-100s-global-espionage-campaign-exploiting-open-source-tools/

New malware targets AI & gaming communities

Between April and June 2024, the NullBulge group has emerged targeting users in AI-centric application and gaming communities. Though NullBulge present themselves as hacktivists fighting against the influence of AI in art, their true motives are financial. NullBulge uses advanced tactics, such as "poisoning the well" and using customised LockBit ransomware, to target software distribution platforms and steal sensitive data.

The operations of NullBulge group are well-organised, primarily focusing on AI-related applications and games. Their weapons include advanced tools like Async RAT and Xworm, followed by LockBit ransomware deployment. While claiming to fight for art, NullBulge also profits by selling stolen data, exposing a well-organised criminal operation. Users are urged to store API keys securely and avoid hardcoding them in the code. Experts also recommend routine examination of third-party code elements for any obscure or otherwise suspicious content.

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

Source - https://www.sentinelone.com/labs/nullbulge-threat-actor-masquerades-as-hacktivist-group-rebelling-against-ai/

BadPack malware evades Android security

Cybersecurity researchers have identified a new Android malware variant called "BadPack". It is an APK file intentionally packaged for malicious purposes. BadPack employs advanced evasion techniques to bypass traditional security measures. It manipulates ZIP headers to obstruct the extraction and analysis of critical files, complicating efforts to counteract the malware. This malware hides by tampering with its own code, making it difficult for security software to detect.

Many Android-based banking Trojans like BianLian, Cerberus, and TeaBot use BadPack. Experts warn that traditional tools used to analyse suspicious apps may be fooled by BadPack's clever disguise. BadPack symbolises the evolving nature of mobile malware. Users are urged to refrain from installing applications that originate from third-party sources and to be cautious of Android applications requiring unusual permissions.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Android

Source - https://unit42.paloaltonetworks.com/apk-badpack-malware-tampered-headers/

Deceptive malware targets crypto investors

A sophisticated cyberattack is targeting Indian cryptocurrency users and investors. Attackers are using malicious shortcut (.lnk) file that, when executed, downloads a PowerShell script granting Remote Desktop Protocol (RDP) access. The attack, specifically aimed at users of the popular Indian exchange CoinDCX, employs a decoy PDF to lure victims. Various components are used, including PowerShell scripts, Go-based binaries, and a vulnerable driver. Additionally, it leverages RDPWrapper and Tailscale for remote access and network connections.

Once attackers gain access, they can potentially steal the cryptocurrency holdings. Users need to be cautious of any unsolicited PDFs, especially those claiming to be from CoinDCX. Cybersecurity experts suggest not to click on suspicious links or download unknown files.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	India	**APPLICATION**	Windows

Source - https://cyble.com/blog/new-malware-campaign-abusing-rdpwrapper-and-tailscale-to-target-cryptocurrency-users/

CrowdStrike update crashes Windows machines

Many businesses worldwide faced disruptions on July 20, 2024, after a faulty update from cybersecurity firm CrowdStrike crashed Windows machines. This critical error caused the dreaded Blue Screen of Death, impacting critical cloud services from Google, Microsoft, and Amazon Web Services (AWS).

While CrowdStrike has issued a fix and is investigating the root cause, the incident highlights the importance of a diverse IT infrastructure. This incident affected all sectors globally. By diversifying reliance on multiple vendors and service providers, businesses can minimise the impact of such unexpected issues and ensure smoother operations. In addition, this incident underscores the need for thorough internal testing procedures before deploying security updates.

ATTACK TYPE	Misconfiguration	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic, CrowdStrike

Source - https://www.bleepingcomputer.com/news/security/crowdstrike-update-crashes-windows-systems-causes-outages-worldwide/

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