TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: MAY 13, 2025

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In today's fast-changing digital landscape, organisations must adopt proactive cybersecurity measures to combat rising threats. Our weekly Cyber Threat Intelligence (CTI) reports provide critical insights into emerging risks, vulnerabilities, and attack trends, empowering businesses to fortify defences and stay ahead of cyber adversaries.

Through expert analysis and actionable strategies, we help clients anticipate, detect, and neutralise threats before they escalate. This proactive approach not only protects critical assets, but also ensures business continuity and strengthens stakeholder confidence. With our CTI insights, organisations can build long-term cyber resilience, navigating the digital world with greater security and assurance.

Aurotun Stealer: SideCopy APT’s sophisticated espionage tool

Aurotun Stealer is a Windows-based infostealer developed by the Pakistan-linked SideCopy APT group, targeting the Indian government and the military and defence sectors. Delivered via spear-phishing emails, the malware exfiltrates credentials, browser cookies, and session data. Its advanced evasion techniques, including obfuscation and anti-analysis features, allow it to bypass traditional security solutions and facilitate the deployment of additional payloads. The malware’s focus on credential theft makes it particularly dangerous for high-privilege systems and users.

Organisations must defend against Aurotun with a layered approach. Email filters and sandboxing tools can intercept spear-phishing payloads before user interaction. Endpoint Detection and Response (EDR) solutions should be configured to detect post-execution behaviour such as credential access and persistence mechanisms. Network segmentation limits the lateral movement of attackers, while privileged access management (PAM) can prevent the misuse of high-value accounts. Frequent employee training on phishing identification, combined with routine audits of administrative tools, can significantly reduce exposure to APT campaigns like this.

ATTACK TYPE	Malware	**SECTOR**	Government, Military, and Defence Industry
REGION	India	**APPLICATION**	Windows

Source - CERT-In

Chaos RAT: Cross-platform control at the attacker’s fingertips

Chaos RAT is an open-source, Go-based Remote Access Trojan capable of infiltrating both Windows and Linux environments. It allows full system compromise through remote shell access, file manipulation, and persistence techniques such as modifying /etc/crontab. The malware transmits system and network data back to command-and-control servers, making it a prime tool for espionage and cybercrime alike. Its cross-platform design and simplicity make it highly attractive to a wide range of attackers.

To defend against Chaos RAT, organisations must apply strict access controls, especially on remote access interfaces and administrative tools. Regular patching and system hardening are essential to close off entry points exploited by remote Trojans. On Linux, enforcing file integrity monitoring and auditing changes to critical system files can reveal attempts to maintain persistence. On both platforms, EDR tools with cross-OS visibility are essential to detect unusual activity. Organizations should also review SSH configurations and enforce the principle of least privilege to minimise the radius of a successful breach.

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

Source - CERT-In

Fake WordPress plugin installs persistent backdoor and ads

A stealthy malware campaign is exploiting WordPress sites by disguising a malicious file — WP-antymalwary-bot.php — as a legitimate plugin. Once installed, the malware creates a persistent backdoor via a modified wp-cron.php, grants administrator-level access, and injects obfuscated malicious ads. It avoids detection by hiding from the admin dashboard and communicating silently with external command-and-control servers. Even after removal, the malware can reinstall itself, making remediation challenging.

To mitigate this threat, site administrators must routinely audit WordPress installations, especially custom plugins and recently modified files. Security plugins should be configured to monitor file integrity and unauthorized admin account creation. Regular backups, secure credentials, and plugin signature verification are vital in detecting tampering. Administrators should also restrict plugin uploads to trusted users and disable file editing through the dashboard. Hosting providers and development teams must collaborate to ensure server-level protection — such as web application firewalls (WAFs) — is in place to prevent remote code execution.

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

Source - https://securityonline.info/wordpress-malware-alert-fake-anti-malware-plugin-grants-admin-access-and-executes-remote-code/

DarkWatchman and Sheriff Malware hit Russia and Ukraine

A large-scale phishing campaign has targeted Russian organizations across the financial, transportation, energy, and retail sectors, delivering DarkWatchman, an advanced, stealthy malware linked to the Hive0117 group. DarkWatchman operates in memory, making detection difficult, and enables long-term espionage and credential harvesting. Meanwhile, in Ukraine, researchers uncovered “Sheriff,” a modular backdoor with reconnaissance, persistence, and command-execution capabilities, underscoring growing cyber instability in the region.

To counter these threats, organisations must adopt behaviour-based detection tools capable of identifying in-memory execution and post-exploitation tactics. Email security should include phishing-resistant authentication, attachment sandboxing, and link inspection. SOC teams should monitor for indicators of compromise, such as unusual registry changes, scheduled tasks, and persistence scripts. System hardening, including restricted PowerShell usage and logging, can help reduce risk. In high-risk regions, real-time threat intelligence and geo-fencing can help proactively block malicious infrastructure linked to ongoing campaigns.

ATTACK TYPE	Malware	**SECTOR**	Financial services, Manufacturing, Transportation, Energy, BFSI, Broadcast Media Production and Distribution, Retailer and Distributor, and Telecommunications
REGION	Russia, Estonia, Kazakhstan, Latvia, Ukraine	**APPLICATION**	Windows

Source - https://habr.com/ru/companies/F6/news/905930/

Commvault Azure breach highlights nation-state vulnerabilities

Commvault confirmed that a nation-state actor exploited CVE-2025-3928 to breach its Microsoft Azure environment. While no customer data was accessed, the attack prompted Commvault to rotate credentials, release mitigation guidance, and share a list of malicious IPs. CISA added the CVE to its Known Exploited Vulnerabilities (KEV) catalogue and mandated patching by May 19, 2025. The vulnerability underscores growing risks from supply chain and cloud service compromise.

Organisations using Commvault or related Azure services must immediately apply all available patches and rotate exposed credentials. Cloud infrastructure should be assessed for anomalies, with particular focus on identity and access management (IAM) misconfigurations. Monitoring tools should be updated to provide alerts on known malicious IP addresses associated with the breach. Implementing a zero-trust model and enabling multi-factor authentication across all cloud services will help limit exposure in the event of lateral movement. Additionally, integrating cloud workload protection platforms (CWPP) can strengthen visibility and incident response capabilities in hybrid environments.

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

Source - https://thehackernews.com/2025/05/commvault-confirms-hackers-exploited.html

SonicWall SMA appliances under active exploitation

SonicWall has confirmed active exploitation of two critical vulnerabilities — CVE-2023-44221 and CVE-2024-38475 — affecting its SMA 100 series devices. CVE-2023-44221 allows OS command injection through the VPN interface, while CVE-2024-38475 is tied to Apache's mod_rewrite module, enabling unauthorised file access and session hijacking. Both flaws can be used in tandem to achieve full system compromise. These issues have been added to CISA's Known Exploited Vulnerabilities (KEV) catalogue.

Organisations using SonicWall SMA appliances must patch immediately using the vendor-provided updates. Until patches are applied, administrators should restrict access to management interfaces using VPN or IP whitelisting. Reviewing system logs for unusual behaviour, unauthorised changes, and failed login attempts is critical to identifying signs of compromise. Multi-factor authentication should be enforced on all remote access portals. It is also important to regularly audit VPN configurations and run vulnerability scans on perimeter devices. Given their internet-facing nature, VPN appliances are high-value targets — real-time monitoring and network segmentation should be part of a comprehensive defence-in-depth strategy.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Apache Software Foundation Apache HTTP Server, Sonicwall SMA

Source - https://thehackernews.com/2025/05/sonicwall-confirms-active-exploitation.html

Chinese APT uses IPv6 SLAAC to launch middle-man style attacks

TheWizards, a Chinese APT group, has been exploiting IPv6 SLAAC (Stateless Address Autoconfiguration) spoofing via its tool, "Spellbinder", to conduct Adversary-in-the-Middle (AitM) attacks. It hijacks software update mechanisms — specifically for platforms like Sogou Pinyin and Tencent QQ — to deliver the WizardNet backdoor. Active since 2022, the group operates in China, the UAE, Hong Kong, and the Philippines. Its infrastructure is reportedly supported by Chinese contractors like UPSEC, pointing to state-level backing.

To mitigate SLAAC-based attacks, organisations must disable IPv6 where it is not in use, or enforce Router Advertisement Guard (RA Guard) on Layer 2 devices. Software update integrity should be verified using digital signatures, and all application traffic should be encrypted. Network security monitoring should include detection rules for unauthorised SLAAC messages and rogue IPv6 routers. DNS monitoring can also detect traffic to C2 domains used by WizardNet. In regions where Chinese software is commonly used, updating to signed and vetted versions is vital. Incident response teams must prepare for stealthy AitM attacks that abuse legitimate services.

ATTACK TYPE	Malware	**SECTOR**	China, Philippines, United Arab Emirates, Hong Kong
REGION	All	**APPLICATION**	Windows

Source - https://thehackernews.com/2025/04/chinese-hackers-abuse-ipv6-slaac-for.html

TATA COMMUNICATIONS

MintsLoader delivers stealthy GhostWeaver RAT to vulnerable systems

MintsLoader is a highly evasive loader malware used to deploy the modular GhostWeaver RAT via complex, multi-stage infection chains. It spreads through phishing campaigns and deceptive browser update prompts. Once executed, MintsLoader uses obfuscated PowerShell scripts, domain generation algorithms (DGA), and HTTP-based C2 to fetch GhostWeaver, which performs data exfiltration, command execution, and plugin-based functionality, all while maintaining stealth through encryption and fileless execution.

To counter MintsLoader and GhostWeaver, organisations must enforce email protection measures, including attachment sandboxing and link reputation scoring. Users should be trained to avoid unexpected browser update prompts. Defenders should monitor for obfuscated PowerShell activity, unusual DNS queries (indicative of DGA use), and suspicious outbound HTTP requests. Endpoint protection platforms must include behaviour-based analytics and memory scanning to detect fileless malware. Implementing PowerShell logging and restricting execution policies will help flag or block suspicious scripts. Because these tools are often used by cybercriminal affiliates, threat intelligence feeds should be leveraged to identify campaign infrastructure before it is too late.

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

Source - https://thehackernews.com/2025/05/mintsloader-drops-ghostweaver-via.html

Earth Kasha targets Taiwan and Japan in espionage surge

In March 2025, the Earth Kasha APT group launched an advanced cyber-espionage campaign targeting government institutions in Taiwan and Japan. Attackers deployed malicious Excel documents that triggered in-memory backdoors and established stealthy communications using encrypted DNS channels. These techniques allowed Earth Kasha to maintain long-term access while avoiding detection by traditional security tools. The campaign highlights the group's evolution and its targeting of high-value geopolitical entities.

To defend against Earth Kasha, government agencies and critical infrastructure operators must deploy DNS traffic inspection and anomaly detection. Email defences should include deep scanning of attachments and real-time sandboxing, especially for Office documents with macros. EDR and XDR solutions should monitor for in-memory execution and lateral movement attempts. Network segmentation, role-based access controls, and frequent review of DNS logs can help identify and disrupt exfiltration attempts. Collaborations with regional CERTs and participation in threat intelligence networks will also enhance early detection of state-sponsored activity.

ATTACK TYPE	Malware	**SECTOR**	Government
REGION	Japan, Taiwan	**APPLICATION**	Windows

Source - https://www.trendmicro.com/en_us/research/25/d/earth-kasha-updates-ttps.html

TATA COMMUNICATIONS

Sarcoma Ransomware expands to Windows, Linux, and ESXi

Sarcoma ransomware has evolved into a cross-platform menace targeting Windows, Linux, and VMware ESXi environments. It employs strong encryption, snapshot deletion, and self-deletion to maximise impact. Before encrypting files, Sarcoma exfiltrates sensitive data for double extortion. The malware embeds ransom instructions in its binary and communicates via secure channels to avoid detection. Its ability to target virtual infrastructure significantly raises the stakes for enterprise environments.

Organisations must secure hypervisors and virtual environments by isolating management interfaces, enabling two-factor authentication, and backing up virtual machine snapshots offline. Regular system patching and disabling unnecessary services can reduce exposure. Network segmentation is key to limiting it from spreading across different OS platforms. Security teams should monitor for mass file encryption behaviour, suspicious lateral movement, and signs of exfiltration. Ransomware-specific behavioural detection tools and immutable backups are critical for swift recovery. Finally, security playbooks should address the nuances of multi-platform ransomware response, including containment across hybrid IT ecosystems.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	VMWare ESXi, Windows, Linux

Source - https://medium.com/@shindepallavi563/sarcoma-ransomware-48fdae2dad8e

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