TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: June 24, 2025

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.

China-linked campaign targets 70+ global enterprises

From July 2024 to March 2025, a coordinated wave of cyberattacks attributed to China-based groups like PurpleHaze (linked to APT15 and UNC5174) impacted over 70 organisations. Key targets included those in government, finance, logistics, media, and telecom sectors, with activity concentrated in Europe and South Asia. Tactics included deep reconnaissance, exploitation of zero-day vulnerabilities, and deployment of malware such as ShadowPad and GoReShell—tools known for persistent data exfiltration and lateral movement. This widespread campaign underscores a growing pattern of nation-state cyber-espionage. The adversaries' sophistication points to long-term strategic intelligence gathering, particularly against critical infrastructure.

Affected enterprises are advised to strengthen endpoint detection and response (EDR), apply zero-trust principles, and prioritise patching of exploited vulnerabilities. Threat hunting for ShadowPad indicators, MFA deployment, and restricting outbound traffic from sensitive systems are recommended countermeasures. Regular threat intel sharing between sectors is also vital for pre-emptive defence.

ATTACK TYPE	Malware	SECTOR	Information technology , Manufacturing , Government , Broadcast Media Production and Distribution , Telecommunications , Logistics & Shipping
REGION	Europe , South Asia	APPLICATION	Windows

Source - https://securityaffairs.com/178819/apt/china-linked-threat-actor-targeted-70-orgs-worldwide-sentinelone-warns.html

AppleSeed campaign highlights Kimsuky’s cross-platform reach

The North Korea-backed Kimsuky group continues its espionage operations with a new AppleSeed campaign, targeting South Korean activists and defectors. This operation uses Facebook, email, and Telegram to deliver social engineering lures embedded in malicious EGG archive files. These archives deploy obfuscated JScript, which triggers the installation of a remote access trojan (RAT) packed with VMProtect to evade analysis. Data is then stealthily exfiltrated through spoofed PDFs. This campaign showcases Kimsuky's evolving cross-platform tactics and persistent targeting of individuals tied to geopolitical conflicts. The use of encrypted communications and evasion methods makes detection difficult.

Organisations in government, healthcare, and defence must reinforce training against social engineering, especially involving messaging apps. Deploying sandboxing and behavioural analysis tools can help catch fileless or obfuscated malware. Monitoring for unusual outbound traffic and enforcing strict data loss prevention (DLP) policies are critical to mitigate these advanced threats.

ATTACK TYPE	Malware	SECTOR	Healthcare/hospitals , Government , Military , Defence Industry
REGION	South Korea	APPLICATION	Windows

Source - https://www.genians.co.kr/en/blog/threat_intelligence/triple-combo

INTRODUCTION | CHINA’S SHADOWOPS HIT 70+ GLOBAL TARGETS | KIMSUKY’S APPLESEED SOWS SPIES IN SOUTH KOREA | ROUNDCUBE PHISHING EXPLOITS ZERO-CLICK VULNERABILITY | FAKE PM KISAN APP INFECTS INDIAN ANDROID DEVICES | MICROSOFT PATCH TUESDAY FIXES CRITICAL WEBDAV BUG | TELEGRAM-POWERED CYBEREYE RAT SPREADS QUICKLY | BLITZ MALWARE TARGETS GAMERS VIA INFECTED CHEATS | DRAGONCLONE ATTACKS STRIKE CHINESE TELECOMS | DUPLEXSPY RAT OFFERS FULL REMOTE CONTROL OF OPERATIONS | ZV RANSOMWARE LOCKS CRITICAL FILES THEN DEMANDS PAYMENT

CERT Polska flags Roundcube exploit in active phishing campaign

A new spear phishing campaign targeting Roundcube webmail users was reported by CERT Polska. Attackers are exploiting CVE-2024-42009—a vulnerability that activates just by opening a malicious email. Attributed to UNC1151, the operation utilises browser capabilities to silently harvest credentials. Though CVE-2025-49113 is not yet exploited, it is cited as a potential follow-up threat. The campaign is a stark reminder of how vulnerable outdated or unpatched webmail software can be, especially in high-risk sectors like government and education where Roundcube remains common.

Entities using Roundcube must urgently patch all known vulnerabilities and consider migrating to secure alternatives. Implementing email filtering, disabling HTML content rendering, and employing zero-trust network access (ZTNA) can limit exposure. Ongoing user awareness training and regular phishing simulations also bolster resilience against socially engineered emails.

ATTACK TYPE	Phishing , Malware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://cert.pl/en/posts/2025/06/unc1151-campaign-roundcube/

Fake PM KISAN YOJNA Android app targets Indian users

A fraudulent Android application impersonating the Indian government's "PM KISAN YOJNA" app has emerged, acting as a dropper to deploy a secondary stealer variant dubbed "Salvador." Once installed, it uses permissions for SMS and VPN access to extract sensitive data, hide itself, and bypass security checks. Its sophisticated phishing tactics and evasion capabilities indicate a significant evolution in mobile malware targeting Indian users. This threat reflects an increasing trend in attackers exploiting public trust in government services to launch mobile campaigns.

Organisations should advise employees and users to download apps only from verified sources like Google Play. Security teams must incorporate mobile threat defence (MTD) solutions and monitor device behaviour for anomalies. Public awareness campaigns can help reduce victim counts. Enterprises handling citizen data should enable mobile app vetting and enforce security policies via MDM (Mobile Device Management) platforms.

ATTACK TYPE	Malware	SECTOR	All
REGION	India	APPLICATION	Andriod

Source - https://labs.k7computing.com/index.php/android-spyware-alert-fake-government-app-targeting-android-users-in-india/

Microsoft Patch Tuesday fixes 70 flaws including exploited Zero-Day

Microsoft's June 2025 Patch Tuesday addressed 70 CVEs, 10 of which were critical. Among the fixed vulnerabilities is CVE-2025-33053, a WebDAV-related bug currently under active exploitation due to its connection with legacy Internet Explorer components. Several Office vulnerabilities were also patched, including those exploitable via the Preview Pane—allowing code execution without user interaction. This highlights the persistent risk posed by outdated systems and default configurations, especially in large enterprises with diverse asset inventories.

IT teams must prioritise immediate deployment of June's patches, especially to systems vulnerable to CVE-2025-33053. Organisations should retire legacy software like Internet Explorer and enforce application allow-listing to restrict risky behaviours. Security operations should also monitor for exploitation attempts tied to WebDAV and Preview Pane vectors using EDR and SIEM solutions.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2025-patch-tuesday-fixes-exploited-zero-day-66-flaws/

CyberEye RAT abuses Telegram for stealthy command-and-control operations

CyberEye is a .NET-based Remote Access Trojan (RAT) notable for using Telegram as its command-and-control (C2) infrastructure. This allows attackers to bypass traditional network monitoring systems, leveraging a trusted messaging app for malicious communication. CyberEye includes a customisable builder that enables threat actors—even with limited skill—to configure functions like keylogging, credential theft, privilege escalation, and persistence. The malware is designed to evade detection through Windows Defender bypass techniques and strong anti-analysis features. The malware's modularity and public distribution significantly increase its threat surface, making it accessible to a broader set of actors for espionage or financial gain.

Organisations should monitor outbound traffic to Telegram domains and implement application-level controls to limit unauthorised communications. EDR solutions should be tuned to detect behavioural indicators like keylogging or privilege escalation attempts. Development of YARA rules and hash-based IoC detection for CyberEye artefacts is also advised. Employee devices should have endpoint hardening and user privilege restrictions in place to minimise post-infection impact.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cyfirma.com/research/understanding-cybereye-rat-builder-capabilities-and-implications/

Blitz malware lurks in Game Cheats on hugging face platforms

Blitz is a multi-functional malware targeting Windows users via backdoored game cheats—specifically mods for Standoff 2. The malware is spread through popular code-hosting platforms like Hugging Face Spaces, giving it an air of legitimacy. Once installed, Blitz deploys a cryptocurrency miner and spyware modules, while evading detection through standard anti-analysis tricks. Although the malware's creator allegedly abandoned the project in May 2025, its payloads remain live, posing risks to unaware users. Blitz reflects the increasingly blurred lines between legitimate gaming tools and malicious payloads, exploiting the trust of online gaming communities.

Gaming companies and platform moderators must improve validation of third-party code uploads. Enterprises should monitor non-business application use and restrict game-related installations on corporate assets. Behavioural analytics tools can help detect cryptomining activity or unauthorised data access. Affected users should be guided to scan systems for residual payloads and advised to reinstall software from official sources only.

ATTACK TYPE	Malware	SECTOR	Gaming industry
REGION	Russia , Belarus , Kazakhstan , Ukraine	APPLICATION	Windows

Source - https://unit42.paloaltonetworks.com/blitz-malware-2025/

DRAGONCLONE: Sophisticated espionage campaign hits Chinese telecom

Operation DRAGONCLONE, attributed to Chinese threat groups UNC5174 and Earth Lamia, has targeted China Mobile Tietong with high-complexity espionage techniques. The campaign features DLL sideloading, sandbox evasion, and cross-platform malware like VELETRIX and VShell. The infrastructure and reconnaissance patterns reflect coordinated efforts aimed at long-term infiltration and data exfiltration within critical telecommunications infrastructure. The attack demonstrates the ongoing cyber cold war between advanced persistent threat (APT) groups, focusing on surveillance, espionage, and strategic disruption.

Telecom providers should conduct immediate audits for sideloaded DLLs and deploy behavioural analysis tools capable of catching anomalous system calls. Cross-platform defence, including Linux and macOS systems, should be reinforced. Incident response teams must track indicators related to VELETRIX and VShell, while maintaining continuous threat intelligence feeds to stay updated on Earth Lamia’s evolving TTPs (tactics, techniques, and procedures).

ATTACK TYPE	Malware	SECTOR	Telecommunications
REGION	China	APPLICATION	Windows

Source - https://www.seqrite.com/blog/operation-dragonclone-chinese-telecom-veletrix-vshell-malware/

DuplexSpy RAT enables fully remote control and surveillance operations

DuplexSpy is a powerful Remote Access Trojan offering capabilities such as keylogging, screen capture, remote shell access, and control of audio and video devices. Operating through fileless execution, encrypted channels, and privilege escalation, DuplexSpy is hard to detect and dangerous even when run in restricted environments. Though marketed for educational use, the RAT's stealth and comprehensive feature set make it attractive for cybercriminals. Ultimately, this trojan poses a critical threat to organisations with insufficient monitoring or outdated security configurations, especially those allowing Bring Your Own Device (BYOD) policies.

Defenders should employ host-based intrusion detection systems (HIDS) and user behaviour analytics (UBA) to detect suspicious activity. Blocking tools with remote shell and screen capture functionality from unapproved sources is recommended. Security teams must also apply application control and enforce endpoint segmentation, especially for high-risk users and systems. Regular security awareness training can help reduce accidental downloads of such RATs.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows , Linux

Source - https://www.cyfirma.com/research/duplexspy-rat-stealthy-windows-malware-enabling-full-remote-control-and-surveillance/

ZV Ransomware: A new Dharma family variant emerges

ZV Ransomware is the latest variant in the Dharma family, identified by its use of a unique ID and ".ZV" file extension appended to encrypted files. It spreads primarily through phishing emails, fake software downloads, and malicious attachments. The ransomware includes aggressive ransom notes that discourage victims from seeking third-party help. However, like most ransomware, paying the ransom offers no guarantee of data recovery. The malware's relatively simple delivery vector combined with high-impact encryption capabilities makes it especially threatening to small-to-medium enterprises with weak email security controls.

Organisations must enhance their email filtering capabilities and train employees to identify phishing attempts. Regular offline and cloud-based backups should be maintained and periodically tested for restoration. Anti-ransomware solutions, especially those using behavioural analysis and real-time rollback features, can significantly reduce impact. A ransomware response plan—including legal counsel and law enforcement coordination—should be predefined and rehearsed.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cyclonis.com/remove-zv-ransomware/

INTRODUCTION | CHINA'S SHADOWOPS HIT 70+ GLOBAL TARGETS | KIMSUKY'S APPLESEED SOWS SPIES IN SOUTH KOREA | ROUNDCUBE PHISHING EXPLOITS ZERO-CLICK VULNERABILITY | FAKE PM KISAN APP INFECTS INDIAN ANDROID DEVICES | MICROSOFT PATCH TUESDAY FIXES CRITICAL WEBDAV BUG | TELEGRAM-POWERED CYBEREYE RAT SPREADS QUICKLY | BLITZ MALWARE TARGETS GAMERS VIA INFECTED CHEATS | DRAGONCLONE ATTACKS STRIKE CHINESE TELECOMS | DUPLEXSPY RAT OFFERS FULL REMOTE CONTROL OF OPERATIONS | ZV RANSOMWARE LOCKS CRITICAL FILES THEN DEMANDS PAYMENT

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.