TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: MAY 06, 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.

Qilra Ransomware redefines the encrypt, threaten, and leak stratagem

Qilra is a newly identified ransomware strain that encrypts victims' files and threatens to leak sensitive data unless the ransom is paid. Victims receive a ransom note with a 72-hour countdown, offering to decrypt one file for free as a "proof of concept". The ransomware spreads through phishing emails, malicious downloads, and exploitation of software vulnerabilities, primarily targeting Windows-based systems. Its use of double-extortion tactics aligns it with other contemporary ransomware operations that focus not only on disruption, but also on reputational damage and coercion.

To combat threats like Qilra, organisations must enforce email security filters and conduct frequent phishing simulation training. Strong patch management, network segmentation, and behaviour-based endpoint detection are crucial to limit spread. Backups must be isolated, regularly tested, and protected with immutable storage to ensure ransomware cannot tamper with them. Since paying the ransom often doesn't guarantee recovery, building ransomware resilience through layered defences and a rehearsed incident response plan is vital. Threat intelligence sharing can also help detect Qilra's indicators early and coordinate a collective defence.

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

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

TATA COMMUNICATIONS

CrypteVex ransomware deploys time-sensitive extortion at $600 per infection

CrypteVex is a newly-emerged ransomware strain that encrypts victims' data and demands a $600 ransom in Bitcoin, pressuring users with time-sensitive threats. It propagates through phishing emails, malicious websites, and drive-by downloads, locking files beyond recovery unless the decryption key is obtained, typically via ransom payment. As is common with modern ransomware, there's no guarantee that victims who pay will regain access, making preventative controls essential.

To mitigate CrypteVex, organisations must ensure all endpoints are protected with real-time antivirus and anti-ransomware solutions. Email gateways should be configured to block suspicious attachments and links, while user education campaigns must reinforce caution around unsolicited communications. Organisations should also review their data backup strategies to ensure offsite, segmented, and frequently tested backups are in place. Network monitoring tools that detect large-scale file encryption, privilege escalation, and outbound traffic to known ransomware C2s (command-and-control servers) can help stop infections that are in progress. Incident response teams should have clear playbooks for ransomware scenarios and test recovery procedures regularly to minimize downtime.

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

Source - https://www.cyclonis.com/rremove-cryptevex-ransomware/

Kimsuky Group deploys PebbleDash backdoor in phishing campaigns

North Korea-linked APT group Kimsuky has been actively distributing the PebbleDash backdoor through targeted spear phishing campaigns. Attackers lure victims into executing LNK shortcut files, which trigger malicious PowerShell commands to install the malware. Once inside, PebbleDash enables attackers to escalate privileges, deploy additional payloads, and patch core Windows files like termsrv.dll to enable unauthorized RDP access. The shift from open-source tools to proprietary malware signifies a more tailored and persistent espionage campaign.

Organisations must educate users to recognize phishing indicators, particularly unusual LNK files or unsolicited email attachments. Implementing strict PowerShell execution policies and logging is crucial to detecting abuse early. Endpoint detection and response (EDR) systems should monitor for privilege escalation behaviours and DLL tampering. Furthermore, organisations should audit and restrict RDP access, preferably behind VPNs with multifactor authentication. Kimsuky's activity highlights the need for proactive threat hunting and participation in information-sharing frameworks to stay ahead of APT tactics.

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

Source - https://asec.ahnlab.com/ko/87616/

FormBook returns in a new fileless, hollowed-out variant

A new variant of FormBook malware is exploiting CVE-2017-11882 — a legacy Microsoft Office vulnerability — to deliver a fileless payload using deceptive RTF files and malicious DLLs. Once deployed, the malware uses process-hollowing to inject itself into legitimate system processes, helping it evade detection by traditional antivirus solutions. The encrypted payload is disguised as an image file and downloaded from a command-and-control server, making it harder for analysts to track or block the infection chain.

Organisations should urgently audit systems for unpatched Microsoft Office software, particularly older versions still vulnerable to CVE-2017-11882. Application control and memory integrity protections should be enabled to prevent malicious injection techniques. Security teams must monitor outbound traffic for suspicious encrypted communications, which may indicate payload downloads. Additionally, implementing user restrictions on running macros and tightening Group Policy settings for Microsoft Office will help prevent the initial infection. Anti-malware platforms with memory scanning and behaviour analysis are essential to detecting fileless threats like this one.

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

Source - https://www.fortinet.com/blog/threat-research/infostealer-malware-formbook-spread-via-phishing-campaign-part-i

Lumma Stealer uses fake CAPTCHAs and pirated software to harvest data

Lumma Stealer is a sophisticated infostealer operating under a Malware-as-a-Service (MaaS) model. It spreads via fake CAPTCHA pages, cracked software download sites, and Telegram channels. Once executed, it uses in-memory execution, DLL sideloading, and overlay injections to bypass antivirus software and collect a wide range of data, including login credentials, browser history, and cryptocurrency wallet details. Its C2 infrastructure is very active and updated frequently to evade blacklisting.

Organisations should block known piracy and malware-distributing domains at the DNS level and implement browser isolation solutions to protect users from social engineering. Endpoint protection should focus on detecting sideloaded DLLs and overlay behaviour. Businesses should also restrict access to software installations and enforce application allowlisting. For higher-risk departments (e.g., finance), real-time monitoring of credential use and browser data access can limit damage in the event of infections. Security awareness training should highlight fake CAPTCHAs and pirated content as key threat vectors.

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

Source - https://securelist.com/lumma-fake-captcha-attacks-analysis/116274/

Hacktivists target Indian sectors with DDoS and defacements

A new phishing campaign has been uncovered, deploying the notorious LummaStealer malware through fake reCAPTCHA pages. Cybercriminals are luring victims with seemingly legitimate reCAPTCHA verification prompts on compromised websites, tricking users into downloading malicious payloads. LummaStealer, known for stealing sensitive data such as credentials, cryptocurrency wallets, and browser cookies, is being distributed via these deceptive pages. Once installed, the malware exfiltrates critical information, putting individuals and businesses at risk of financial loss and identity theft.

Security experts warn that the campaign exploits user trust in reCAPTCHA systems, highlighting the need for heightened vigilance. Users are advised to verify website authenticity, avoid clicking on suspicious prompts, and keep security software updated. This incident underscores the evolving tactics of cybercriminals, who continue to innovate in their efforts to bypass defences and exploit unsuspecting victims.

ATTACK TYPE	Hacktivist, DDOs	**SECTOR**	Healthcare/hospitals, Government, Transportation, Education, E-commerce and Telecommunications
REGION	India	**APPLICATION**	Generic

Source - TCL Threat Intel team

TATA COMMUNICATIONS

APT36 leverages terror attack lures in Indian espionage campaign

APT36, a state-sponsored Pakistani threat actor, has launched a sophisticated phishing campaign targeting the Indian government and defence personnel. Using lures themed around the Pahalgam terror attack and fake job recruitment materials, APT36 delivers remote access tools such as CrimsonRAT and Poseidon via weaponized documents and spoofed domains. These tools enable long-term surveillance, credential theft, and system control. APT36's infrastructure is robust, using fallback domains and obfuscation techniques to resist takedowns.

To defend against APT36, organisations must enhance phishing defences with sandboxing and advanced threat protection for email. High-risk personnel should receive specialized training to identify social engineering and tailored attacks. Network segmentation and zero-trust access models can restrict lateral movement if a foothold is established. SOCs should monitor for known indicators associated with CrimsonRAT and Poseidon, including unusual outbound C2 traffic or persistence mechanisms. Coordination with national cybersecurity agencies and robust logging will help mitigate the impact of such nation-state campaigns.

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

Source - https://medium.com/@bugtest252/new-type-of-warfare-digital-psyops-from-hacking-apt36-misinformation-and-lies-81bb8eda4704 ; https://medium.com/@d09r/apt36-uses-pahalgam-terror-attack-lure-in-targeted-phishing-against-indian-defense-personnel-4b407f09b9a0 ;

CISA warns of critical bugs in Planet Technology devices

CISA has issued a warning about critical vulnerabilities in several Planet Technology networking devices, including UNI-NMS-Lite, NMS-500, and WGS-804HPT-V2. These flaws allow attackers to gain admin access, tamper with managed databases, and manipulate device settings, potentially enabling full infrastructure compromise. Planet Technology has released patches and federal agencies are urged to apply them immediately.

Organisations using affected Planet Technology products should identify all impacted assets and apply the necessary firmware updates without delay. Until patching is complete, access to management interfaces should be restricted to internal IPs or placed behind VPNs. Firewall rules and intrusion detection systems should be configured to monitor for unusual access patterns and traffic to or from the devices. Security teams should also perform configuration integrity checks and monitor for unauthorized changes in network traffic or device behaviour. In the long term, asset management practices and third-party risk assessments are crucial for identifying vulnerable infrastructure across distributed networks.

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

Source - https://securityonline.info/cisa-warns-of-critical-vulnerabilities-in-planet-technology-products/

Hannibal Stealer is a modular, marketable, and malicious new threat

Hannibal Stealer is a newly branded infostealer built from SHARP and TX codebases, developed in C# , and sold on cybercrime forums. While technically simple, its modular design and robust command-and-control panel make it effective. It harvests browser data, cryptocurrency wallets, VPN credentials, and data from messaging platforms. Its operators frequently promote it via dark web markets and occasionally align with hacktivist messaging, blending ideology with cybercrime.

To defend against Hannibal Stealer, organisations should implement endpoint protection solutions that can monitor for suspicious access to browser files and encrypted traffic to known C2 nodes. Browser sandboxing, access control restrictions, and network egress filtering can help detect and block data exfiltration. Users should be discouraged from storing sensitive credentials in browsers. Organisations should also enforce strict software installation policies to prevent sideloading and rogue tools. Regular vulnerability scans and integration with cyber threat intelligence feeds can aid in identifying emerging stealer variants like Hannibal.

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

Source - https://www.cyfirma.com/research/hannibal-stealer-a-rebranded-threat-born-from-sharp-and-tx-lineage/

SocGholish campaign delivers RansomHub backdoor via fake browser updates

A sophisticated malware campaign using SocGholish malware was found delivering a Python-based backdoor associated with RansomHub affiliates. Victims are lured into downloading fake browser updates hosted on compromised websites. Once clicked, the malware executes system reconnaissance, steals credentials, and deploys a backdoor that proxies network traffic and maintains stealthy, persistent access. This multi-stage attack highlights the evolution of ransomware affiliates into full-scale initial access brokers.

Organisations must enforce strict browser update policies — users should never install updates outside official distribution channels. Browser isolation technologies and domain whitelisting can help block compromised websites from being accessed. Endpoint Detection and Response (EDR) tools should be tuned to identify process anomalies and credential access behaviour. Monitoring DNS queries and outbound traffic patterns may uncover beaconing to C2 infrastructure . Additionally, organisations should establish user behaviour analytics (UBA) to detect anomalies and prepare for multi-stage intrusion scenarios involving ransomware and espionage.

ATTACK TYPE	Ransomware and Malware	**SECTOR**	Healthcare/hospitals and Government
REGION	Global	**APPLICATION**	Microsoft Edge and Windows

Source - https://www.esentire.com/blog/socket-puppet-how-ransomhub-affiliates-pull-the-strings

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.

© 2024 Tata Communications. All rights reserved. TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Private Limited.