TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: June 17, 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.

SparkLocker ransomware demands a $5,000 ransom for your data

SparkLocker is a Windows-targeting ransomware strain that encrypts user files with a ".spark" extension and demands a $5,000 ransom in Bitcoin. Distributed via phishing emails, malicious downloads, and infected USB devices, SparkLocker's ransom note directs victims to pay via darknet sites, offering no assurance of data recovery even after payment. The ransomware disables system recovery and often deletes shadow copies to obstruct data restoration efforts.

To defend against SparkLocker, organisations must deploy layered ransomware protection strategies. Email gateways should be configured to block executable attachments and phishing content. Anti-malware tools must be updated to detect SparkLocker indicators of compromise (IOCs), including registry changes and file extension modifications. Regular backups, stored offline or in immutable environments, are critical to ensure recovery without ransom payment. Organisations should also enforce application allowlisting and restrict autorun capabilities on removable media. Educating employees on phishing detection and secure browsing habits adds a vital human layer of defence. Infected systems should be isolated immediately, and incident response procedures must be enacted to assess the scope of compromise and initiate remediation.

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

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

Chaos RAT masquerades as network tools to hijack systems

Chaos RAT, a remote access trojan written in Go, is spreading through phishing campaigns that disguise the malware as legitimate network utilities and fake Trust Wallet apps. The RAT targets both Windows and Linux systems, granting attackers full control for data theft, surveillance, and additional malware delivery. It maintains persistence through scheduled tasks and has been linked to cryptocurrency mining operations. Vulnerabilities in its admin panel also suggest broader potential for supply-chain abuse or reconfiguration by other threat actors.

Organisations must validate all software and scripts before deployment, especially network diagnostic tools and cryptocurrency apps. EDR and XDR platforms should be configured to detect suspicious child processes, PowerShell abuse, or unauthorised scheduled tasks. Linux systems must be protected with file integrity monitoring and SSH hardening to prevent unauthorised remote access. Threat intelligence feeds should be regularly updated to detect known C2 infrastructure tied to Chaos RAT. Network segmentation and privilege reduction can help mitigate post-compromise lateral movement. Proactive monitoring for cryptomining patterns – such as GPU/CPU spikes or outbound traffic to mining pools – is also recommended.

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

Source - https://thehackernews.com/2025/06/chaos-rat-malware-targets-windows-and.html

Play ransomware breaches surge past 900 victims worldwide

The Play ransomware group has breached over 900 organisations globally, with attacks intensifying since early 2025. Known for using recompiled malware, credential theft, and aggressive extortion — including direct phone threats — Play targets Windows, Linux, and macOS environments. The group often exploits vulnerabilities in Remote Monitoring and Management (RMM) tools to gain initial access, bypassing traditional security measures. Rather than negotiating through Tor, Play uses email for ransom communication, complicating response tracking.

To counter Play ransomware, organisations must secure RMM tools with MFA, access restrictions, and regular patching. Endpoint protection should detect lateral movement and unusual encryption activity, while backup systems must be kept offline and tested for integrity. Segmentation of critical systems reduces ransomware propagation risks. Organisations should develop and rehearse ransomware-specific incident response playbooks, including communication protocols for executive teams. SOCs must track TTPs related to Play's tactics, especially the use of living-off-the-land binaries (LOLBins) and service abuse. Given Play's scope and persistence, businesses should treat any indicators as urgent and prioritise containment.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Apple Mac OS, Windows, Linux

Source - https://www.bleepingcomputer.com/news/security/fbi-play-ransomware-breached-900-victims-including-critical-orgs/

Veluth ransomware demands Bitcoin via Signal messaging app

Veluth ransomware encrypts user data, appending a ".veluth" extension and delivering a ransom note directing victims to contact attackers via the Signal app for payment instructions. This unusual communication channel, combined with strong encryption and threats against using recovery tools, heightens the urgency of attacks. Veluth spreads via phishing emails and malicious software downloads. Victims are left with few recovery options if they lack secure backups, as no public decryptor currently exists.

To mitigate Veluth infections, organisations should implement strong email filtering policies to detect spoofed senders and malicious attachments. Endpoints should be monitored for file extension changes and unauthorised system alterations. Backup strategies must include versioning and offsite storage, ensuring data remains recoverable even after ransomware impact. Blocking the Signal desktop app in enterprise environments may help reduce attacker communications. SOC teams should monitor for new IOCs and abuse of file-sharing platforms where Veluth samples may be hosted. Regular tabletop exercises should include ransomware simulations that incorporate emerging tactics like non-traditional communication channels.

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

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

Chrome Zero-day CVE-2025-5419 actively exploited in the wild

Google has released an emergency patch for Chrome, addressing CVE-2025-5419 — a high-severity zero-day vulnerability in the V8 JavaScript engine. Exploited in the wild via malicious HTML content, the flaw allows attackers to corrupt memory and potentially execute arbitrary code on vulnerable systems. This update also affects other Chromium-based browsers like Edge and Brave. Users and enterprises are urged to upgrade to Chrome 137.0.7151.68/.69 immediately.

Organisations should automate browser updates using centralised device management tools (e.g., GPO, Intune, Jamf) to minimise delay in patch deployment. Vulnerability scanners should verify browser version compliance across enterprise assets. Web gateways can help block access to known exploit-hosting domains, while browser isolation technologies add an additional safeguard. Security awareness campaigns should caution users against clicking on suspicious links or downloading files from unfamiliar sources. In environments where browsers are used for accessing critical applications, network segmentation and sandboxing are strongly advised. Enterprises relying on embedded or kiosk browsers should validate patch compatibility and rollout timelines swiftly.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Google Chrome

Source - https://thehackernews.com/2025/06/new-chrome-zero-day-actively-exploited.html

TATA COMMUNICATIONS

Crocodilus trojan evolves to target global mobile banking networks

The Crocodilus Android banking trojan has undergone significant evolution, expanding its geographic reach from Europe into South America and beyond. The latest variants feature sophisticated obfuscation, automated cryptocurrency theft, and advanced social engineering capabilities — such as inserting fake contacts or overlaying fake login pages — to trick users into surrendering credentials. Delivered primarily through deceptive mobile ads and fraudulent app updates, Crocodilus poses a growing threat to mobile banking customers and financial institutions.

Organisations in the banking and fintech sectors should adopt mobile threat defence (MTD) solutions to detect malicious apps and abnormal device behaviours. App stores must enforce stricter review processes to prevent Trojanised apps from reaching users. Customers should be educated on how to identify phishing overlays and avoid downloading applications outside official marketplaces. Financial institutions should implement biometric and behavioural fraud detection mechanisms and monitor for signs of compromised accounts. Where possible, authentication tokens and secure mobile SDKs should replace username/password logins. As Crocodilus continues to adapt, cross-platform monitoring and threat intelligence sharing are critical for keeping pace with its evolving tactics.

ATTACK TYPE	Malware	**SECTOR**	BFSI
REGION	South America, Europe	**APPLICATION**	Android

Source - https://thehackernews.com/2025/06/android-trojan-crocodilus-now-active-in.html

Zen ransomware: Dharma-based threat targets global systems

Zen ransomware is a newly observed variant from the Dharma family, designed to encrypt Windows systems and append a ".zen" extension to compromised files. It spreads through common ransomware vectors including Remote Desktop Protocol (RDP) brute-forcing, phishing emails, and malicious file downloads. After successful infiltration, Zen encrypts critical files and deletes local backups to inhibit recovery. Victims receive a ransom note instructing them to contact the attackers for decryption in exchange for Bitcoin, along with stern warnings against using third-party recovery tools.

To prevent Zen infections, organisations must restrict RDP access to only essential personnel and secure it with strong, unique credentials and multi-factor authentication. Firewall rules and intrusion detection systems should block brute-force attempts. Email security should filter malicious attachments and links, while endpoint protection must detect abnormal encryption behaviours and file modifications. Regular, offline backups stored on immutable systems are crucial for recovery. Incident response teams should maintain updated playbooks for ransomware scenarios and monitor for file extension anomalies and registry tampering. Awareness training is also essential to reduce phishing-related entry points for ransomware like Zen.

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

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

TATA COMMUNICATIONS

Transparent Tribe (APT36) cyber infrastructure mapped through DNS forensics

A new investigation into Transparent Tribe (APT36), a Pakistan-linked APT group, has revealed additional C2 infrastructure and assets through advanced DNS telemetry and HTTP response analysis. By starting with known phishing indicators and pivoting via ETag matching, subdomain enumeration, and host behaviour, analysts uncovered a broader range of servers used in attacks against Indian defence and government sectors. Some assets were previously unreported, highlighting the value of infrastructure-focused hunting in pre-empting APT operations.

Organizations — especially those in the public sector — should adopt DNS telemetry, passive DNS analysis, and HTTP fingerprinting to detect malicious infrastructure before full exploitation. Threat hunters should pivot from known indicators using passive recon and analyse TLS certificates, headers, and redirects for clues to related assets. Firewalls and proxies should block traffic to suspicious subdomains or IPs tied to Transparent Tribe. Continuous monitoring for spear-phishing campaigns targeting officials and government workers remains essential, as the group frequently deploys credential harvesting and backdoor malware via infected Office documents. Collaboration with threat intelligence providers enhances detection capabilities, particularly for persistent, regionally focused actors like APT36.

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

Source - https://x.com/ValidinLLC/status/1929591911406309745 ; https://hybrid-analysis.com/sample/bd5bad8ae151d32347eb6b06ee28f8a1ba6e1f80cd966ecb0f8fd23a7ee10b46/682d700331422f38f40ce377 ; https://www.validin.com/blog/illuminating_transparent_tribe/ ; https://x.com/ThreatBookLabs/status/1929918244837609527

TATA COMMUNICATIONS

Finance execs hit by global NetBird-based phishing campaign

A stealthy spear-phishing campaign is targeting finance and energy sector executives with fake job offers from Rothschild & Co. The lure leads to Firebase-hosted phishing pages with CAPTCHAs and downloads of VBS scripts that install NetBird — a legitimate open-source remote access tool. This grants threat actors persistent access to corporate environments without triggering traditional malware alerts. Researchers noted overlap with infrastructure from other phishing campaigns, suggesting a larger coordinated effort.

Organisations must treat remote access tools with high scrutiny, even if they are legitimate. Application control systems should flag and review unsanctioned installations of NetBird and similar software. Endpoint monitoring should look for suspicious VBS/MSI activity, while firewalls and proxies should block unauthorised connections to Firebase or similar hosting services. User training is critical, particularly for executives and finance staff, to help them identify social engineering tactics. Email filters should be tuned to detect and quarantine content with CAPTCHAs or fake branding, and DNS traffic should be analysed for indicators of compromise. As attackers weaponise legitimate tools, behavioural monitoring becomes a frontline defence.

ATTACK TYPE	Ransomware	**SECTOR**	Energy, BFSI, Mining, Investment Management
REGION	Singapore, Canada, UK, Brazil, Egypt, France, South Korea, Norway, Saudi Arabia, South Africa, Switzerland	**APPLICATION**	Windows

Source - https://www.trellix.com/blogs/research/cfo-spear-phishing-netbird-attack/

Rust-based AsyncRAT variant signals growing shift in malware development

Security researchers have identified a new AsyncRAT variant rewritten in Rust, reflecting a broader trend of malware authors adopting modern programming languages for stealth and cross-platform capabilities. While the Rust version retains core functions like plugin support, persistence mechanisms, and C2 communication, it is currently in a limited stage of development. The rewrite complicates reverse engineering and improves evasion of traditional signature-based detection, raising concern over future variants as the malware matures.

Organisations should expand their detection strategies to account for malware compiled in non-traditional languages like Rust or Go. Threat hunting teams should search for new binary signatures and use static/dynamic analysis tools capable of parsing Rust binaries. Endpoint defences should flag newly introduced executables, especially those mimicking known RAT behaviours or establishing encrypted outbound connections. Application behaviour analysis and anomaly detection have become increasingly important as threats move away from easily identifiable codebases. Proactively hunting for test-stage malware gives defenders a rare opportunity to develop detections before mass deployment. Security teams should also monitor for command-and-control domains linked to emerging Rust-based threats.

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

Source - https://www.gdatasoftware.com/blog/2025/05/38207-asyncrat-rust

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