TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: September 29, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As September 2026 draws to a close, the cyber threat landscape remains as relentless as ever, with threat actors orchestrating increasingly sophisticated and tightly coordinated campaigns across deeply interconnected digital environments. Conventional defence models are struggling to keep pace as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now hinges on organisations reinforcing foundational security controls, adopting layered defence strategies, and weaving forward-looking intelligence throughout every layer of their operational frameworks.

In this fast-evolving environment, the Tata Communications Cyber Threat Intelligence report remains an indispensable resource for security practitioners. Published weekly, it offers sharp, timely analysis of emerging threat campaigns, evolving attacker methodologies, and sector-specific risk exposures. By translating intelligence into practical defence guidance, it equips security teams to anticipate, counter, and contain threats with confidence — safeguarding the continuity of critical operations at scale.

TATA COMMUNICATIONS

Hybrid Mantax Otax application steals OTPs encrypts files and hijacks devices remotely

Researchers have uncovered Mantax Otax, a hybrid Android malware strain that fuses ransomware, spyware, credential theft and remote device control into a single infection. Distributed as sideloaded APKs through third-party file-sharing services and phishing lures, it abuses Device Administrator and Accessibility Services to seize near-total control of the compromised device once a victim grants permissions.

The malware harvests SMS messages, one-time passwords, contacts, call logs, browser history, files and messaging data, while capturing screens and photographs. On Android 9 and earlier it encrypts files and demands payment; a newer variant adds WebSocket communication, application blocking, touch interception and disruptive overlays. Users are urged to avoid sideloading apps and install only from trusted sources.

ATTACK TYPE	Ransomware, Emerging Threats	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Indonesia	**APPLICATION**	Android, Telegram, WhatsApp

Source - https://zimperium.com/blog/mantax-otax-indonesian-mobile-ransomware-with-spyware-integration

TATA COMMUNICATIONS

Massive Oracle CSPU addresses databases middleware and business application flaws

Oracle has released its September 2026 Critical Security Patch Update, addressing 673 vulnerabilities across 17 product families. The release spans Database Server, E-Business Suite, Fusion Middleware, Java SE, PeopleSoft, Siebel CRM, Supply Chain and Virtualization, among others. The volume marks a notable decline from recent months, following 943 vulnerabilities patched in August and 1,449 in July 2026.

More than 100 of the flaws are rated critical, while over 240 can be exploited remotely without authentication. E-Business Suite and Fusion Middleware received the largest batches of patches. Oracle warns that attackers have already compromised organisations that failed to apply previously released updates, and strongly urges customers to remain on supported versions and patch without delay.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Oracle Database, Oracle PeopleSoft Enterprise, Oracle Siebel CRM, Oracle Virtualization, Oracle WebLogic Server, Oracle Java SE, Oracle E-Business Suite, Oracle Hyperion

Source - https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-oracle-products-could-allow-for-arbitrary-code-execution_2026-097

TATA COMMUNICATIONS

Operation RapidRust APT36 targets government and defence networks with RUSTYSHADE

In August 2026, security analysts observed Operation RapidRust, a campaign attributed to the advanced threat actor APT36 targeting government and defence organisations. The operation introduced RUSTYSHADE, a Rust-based Windows backdoor; RUSTYMOVE, a removable-media propagation tool designed to reach air-gapped networks; and the PSNATCH and BASHNATCH file stealers, which exfiltrate sensitive data from Windows and Linux systems respectively.

RUSTYSHADE abuses attacker-controlled private GitHub repositories for encrypted command-and-control and data exfiltration, using AES-256-GCM to conceal its traffic. The group staged payloads on Backblaze cloud storage and registered typosquatted domains impersonating Indian media outlets to deliver PowerShell scripts. Reconnaissance and network mapping supported lateral movement. Organisations are urged to monitor removable-media usage and restrict unnecessary outbound connections to cloud services.

ATTACK TYPE	Malware, Cyber-espionage	**SECTOR**	Government, Defence
REGION	India, Afghanistan	**APPLICATION**	Windows, Linux, Microsoft OneDrive, PowerShell, GitHub

Source - https://gbhackers.com/apt36-malware-campaign/

TATA COMMUNICATIONS

CISA flags actively exploited Linux kernel flaws to KEV catalog for urgent federal patching

The US Cybersecurity and Infrastructure Security Agency has added three Linux kernel vulnerabilities to its Known Exploited Vulnerabilities catalogue following evidence of active exploitation. Tracked as CVE-2025-39682 (CVSS 9.8), CVE-2025-39964 (CVSS 7.8) and CVE-2026-53266 (CVSS 8.8), the flaws affect the kernel's TLS receive path, the AF_ALG cryptographic socket interface and the ebtables SNAT address-rewrite path respectively.

Depending on the component and configuration, the flaws can enable kernel memory corruption, denial-of-service or potential privilege escalation, with local access typically required. Red Hat and researchers have confirmed public or known exploits for all three. CISA set a three-day remediation deadline for federal agencies under Directive 26-04; all organisations are urged to deploy the fixed kernel releases immediately.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Linux

Source - https://securityonline.info/linux-kernel-vulnerabilities-exploited/

TATA COMMUNICATIONS

Mustang Panda targets government and energy sectors with Toneshell and Havencode

IBM X-Force, working with Deception.Pro, has captured live activity from ITG27 — the China-aligned espionage group widely tracked as Mustang Panda — inside simulated enterprise environments mimicking an electric-grid operator and a government body. The operators, unaware of the trap, deployed a previously undiscovered VNC-capable backdoor named Havencode, extending an earlier campaign against India's government and energy sectors.

Initial access relied on geopolitically themed spearphishing lures delivering Claimloader and the Toneshell backdoor. Once inside, operators conducted system reconnaissance, credential-related activity, interactive desktop browsing and document collection, before creating archives and exfiltrating data via an attacker-controlled SFTP server. Organisations are advised to scrutinise archive-based lures, monitor for hidden VNC sessions and hunt for the published indicators of compromise.

ATTACK TYPE	Cyber-espionage
REGION	North America, Middle East, Europe, Africa, India, South Asia, East Asia
SECTOR	Government, Energy/Power, Renewable Energy
APPLICATION	Microsoft Edge, Microsoft Visual Studio, KeePass, Mozilla Firefox, Mozilla Thunderbird, Windows, Google Chrome, Zoho WorkDrive

Source - https://www.ibm.com/think/x-force/trapping-a-mustang-panda

TATA COMMUNICATIONS

Stealthy BambooToken abuses MQTT C2 and DLL to control enterprise systems covertly

Researchers have detailed BambooToken, a previously undocumented cross-platform malware framework active since at least February 2023 and observed as recently as July 2026. Targeting Windows and Linux systems, it has steadily evolved from an early PowerShell stager and direct HTTP-based command-and-control into a modular framework relaying tasking through brokered MQTT communications, a lightweight IoT protocol.

On Windows, the malware sideloads a rogue DLL into the legitimately signed Tendyron OnKey process, enabling host discovery and modular command handling while blending with trusted activity. Routing traffic through Cloudflare-proxied domains and multiple MQTT nodes, it compromised roughly a dozen enterprises across Asia and South America. Organisations are urged to monitor for anomalous MQTT traffic and unexpected DLL loads.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, BFSI, Legal Services, Hospitality, IT, Cryptocurrency
REGION	South America, Singapore, Asia, Argentina, Cambodia, Chile, China, Lithuania, Malaysia, Vietnam, South Asia, Hong Kong	**APPLICATION**	Windows, Linux, MikroTik Router

Source - https://thehackernews.com/2026/09/bambootoken-malware-uses-mqtt-to.html

TATA COMMUNICATIONS

Unpatched FortiGate flaw exploited to plant post-exploitation PivotC2 FortiGate RAT

Threat Research Unit has observed active exploitation of CVE-2025-25249, a critical heap-based buffer overflow in the FortiOS and FortiSwitchManager cw_acd daemon. Carrying a CVSS score of 9.8, the flaw allows unauthenticated attackers to execute arbitrary code via crafted CAPWAP packets. Successful exploitation deploys PivotC2, a bespoke Node.js remote access trojan built specifically for post-exploitation on compromised FortiGate firewalls.

PivotC2 establishes TLS-based command-and-control and provides interactive shell access, traffic tunnelling, network discovery and configuration harvesting, effectively turning the firewall into a pivot into internal networks. Researchers report more than 30,000 IP addresses scanned and 178 confirmed infections, with data exfiltration observed in two full intrusions. Organisations are urged to patch affected FortiOS versions and hunt for compromise immediately.

ATTACK TYPE	Cybercrime, Malware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	UK, Chile, Colombia, United States	**APPLICATION**	Microsoft Edge, Microsoft Exchange Server, Fortinet FortiGate, Fortiswitch Manager, Node.js, Google Chrome, FortiOS

Source - https://socradar.io/blog/cve-2025-25249-pivotc2-fortigate-rat/

TATA COMMUNICATIONS

KREMLIN force-installs browser extensions to steal credentials from Chrome and Edge

Security Labs has documented REF9334, a banking malware operation active since May 2025 across seven campaigns. Its KREMLIN toolkit combines JavaScript loaders, PowerShell, Node.js, RunPE, DLL sideloading and malicious browser extensions. Notably, the operators abuse Ethereum smart contracts as dead-drop resolvers, dynamically updating command-and-control endpoints and payload locations without altering the malware, making their infrastructure far harder to dismantle.

The malicious extension installs itself in Chrome and Edge by manipulating Secure Preferences and regenerating the integrity checks that would normally flag unauthorised changes, so the browser loads it as though the user approved it. It harvests credentials, cookies, storage, screenshots and keystrokes before exfiltrating the data. Organisations should enforce extension allowlisting and monitor for unauthorised browser profile modifications.

ATTACK TYPE	Malware	**SECTOR**	BFSI
REGION	Brazil	**APPLICATION**	Microsoft Edge, Chromium, Windows, Google Chrome, WhatsApp

Source - https://www.elastic.co/security-labs/threat-command/malicious-browser-extension-kremlin-banking-malware

TATA COMMUNICATIONS

New REVSTEALER infostealer targets gamers and crypto holders through fake software

Elastic Security Labs is tracking REVSTEALER, an emerging Windows infostealer sold commercially since early 2026 that has gained rapid momentum. Distributed largely through social engineering, it reaches victims via hijacked YouTube channels advertising fake game cheats and mod menus, and by masquerading as legitimate applications. The malware harvests browser credentials, cookies, cryptocurrency wallets, gaming accounts and sensitive local data.

To evade defences, REVSTEALER employs a weighted sandbox scoring system, VMProtect packing and an App-Bound Encryption bypass, streaming stolen data straight from memory before deleting itself. It uses Polygon blockchain dead drops for resilient command-and-control and can deploy modules enabling proxying, cryptocurrency theft and mining. Organisations are urged to warn users against pirated software and unofficial gaming tools.

ATTACK TYPE	Malware, Emerging Threats	**SECTOR**	Gaming Industry, Social Media, Cryptocurrency
REGION	Global	**APPLICATION**	Windows

Source - https://www.elastic.co/security-labs/threat-command/revstealer-credential-harvesting-infostealer

TATA COMMUNICATIONS

Mirai-style KATARU IoT malware combines public Linux LPE exploits and DDoS capabilities

Researchers have identified KATARU, a Mirai-style IoT malware that compromises internet-exposed devices through Telnet credential brute forcing before downloading an ARM payload. Once running, the malware attempts to escalate privileges by making /etc/passwd writable, then falls back on multiple publicly available Linux local privilege-escalation exploits to seize full root control of the compromised device.

Departing from typical Mirai variants, KATARU uses an encrypted X25519 and ChaCha20-Poly1305 command channel, and supports TCP, UDP, ICMP, HTTP, QUIC and DNS floods alongside broad persistence and anti-analysis checks. Architecture-mismatched exploit code and reused cryptographic test values suggest hasty, poorly validated assembly. Organisations should disable Telnet, replace default credentials, patch firmware and segment IoT networks.

ATTACK TYPE	Malware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications, Software Development
REGION	Vietnam	**APPLICATION**	Android, OpenVPN, Linux

Source - https://cyberpress.org/linux-exploits-create-botnets/

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