TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: March 3, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As we enter March 2026, increasingly sophisticated hostile activities are escalating the cyber threat. Traditional defence models are proving inadequate as adversaries exploit the structural weaknesses of deeply interconnected digital ecosystems. Organisations must strengthen core security foundations, implement layered defences, and integrate anticipatory intelligence across their architectures to preserve resilience and strategic advantage.

In this high-stakes environment, the Tata Communications Cyber Threat Intelligence report becomes indispensable. Published weekly, the report delivers incisive analysis of emerging attack campaigns, evolving adversary tactics, and sector-specific exposures. By converting intelligence into immediate defensive action, security teams can anticipate, prepare for, and neutralise threats proactively to protect critical operations globally before disruption.

TATA COMMUNICATIONS

UNC3886 exploits zero-day flaw in telecommunications networks via proxies

A coordinated cyber campaign attributed to a China-linked APT group, UNC3886, recently leveraged Operational Relay Box (ORB) networks to target Singapore's telecommunications sector, exploiting a zero-day vulnerability to bypass perimeter firewalls and deploying rootkits to maintain covert access. Telecoms infrastructure owned by Singtel, StarHub, M1 and SIMBA Telecom was probed, with limited network-related data exfiltrated and advanced evasion tactics observed.

Investigations revealed ORB nodes composed of compromised IoT devices, SOHO routers and VPS relays masking attacker origin and complicating attribution, with NetFlow analysis linking relay traffic to major ISPs in Singapore. Singapore's Cyber Security Agency mounted Operation CYBER GUARDIAN, combining government and industry defence efforts to evict the threat and reinforce resilience against persistent, stealthy intrusion activity.

ATTACK TYPE	Cyberespionage	**SECTOR**	Internet service provider, Telecommunications
REGION	Singapore	**APPLICATION**	D-Link, ASUS Routers

Source - https://cloud.google.com/blog/topics/threat-intelligence/unc1069-targets-cryptocurrency-ai-social-engineering/

GhostSocks leverages SOCKS5 and LummaC2 through proxy traffic globally

GhostSocks is a Golang-based SOCKS5 backconnect proxy malware marketed through a Malware-as-a-Service model and closely tied to LummaC2, the prolific information stealer. First surfaced on Russian-language forums in 2023, its reach expanded to English-speaking criminal communities in 2024. By leveraging compromised systems as residential proxies, threat actors can mask malicious traffic, evading IP-based protections deployed by financial institutions and other high-value sectors.

The Lumma–GhostSocks nexus exemplifies modern malware commodification, with automatic provisioning and discounted access for Lumma licence holders, enhancing post-infection exploitation. GhostSocks employs sophisticated obfuscation, relay-based C2 communications and auxiliary backdoor capabilities, including arbitrary command execution and credential modification. Cybersecurity teams are urged to monitor associated infrastructure indicators and block malicious proxies to mitigate this persistent threat.

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

Source - https://infrawatch.com/blog/ghostsocks-lummas-partner-in-proxy#blogpost

TATA COMMUNICATIONS

Double extortion ransomware, Termite spreads laterally through file transfer software

Termite ransomware, identified as a dangerous Babuk-derived double-extortion threat, is increasingly targeting organisations worldwide by exploiting phishing vectors, stolen credentials and vulnerabilities in managed file-transfer software such as Cleo solutions. Once inside, it encrypts data, deletes recovery artefacts, and spreads laterally across network shares, maximising disruption and operational impact.

After a successful compromise, Termite exfiltrates sensitive information before encryption, leveraging darknet leak portals to intensify ransom pressure and negotiate payments in cryptocurrency. With campaigns already observed across multiple sectors and regions, its operational similarities to other major ransomware ecosystems highlight a growing risk to enterprises facing coordinated data theft, service disruption and long-term exposure. Cybersecurity teams must prioritise layered defences and threat hunting.

ATTACK TYPE	Vulnerability, Cyberespionage	**SECTOR**	IT, Business
REGION	Global	**APPLICATION**	Windows, SmarterTools, SmarterMail

Source - CERT-In reference

Spear-phishing MacroMaze campaign abuses webhook for payload delivery

Operation MacroMaze, a recent APT28 campaign active from September 2025 to January 2026, has been observed targeting organisations across Western and Central Europe through macro-enabled spear-phishing documents that abuse legitimate webhook services for command-and-control and exfiltration. Researchers report multiple macro variants with evolving evasion techniques, including UI manipulation and automated script execution, seeking to maintain low visibility through ephemeral infrastructure and rigorous artefact cleanup.

The campaign's tradecraft blends simple tooling with strategic sophistication: malicious Word macros drop VBScript, CMD, batch and HTML components to establish persistence via scheduled tasks and exfiltrate data through auto-submitting forms in browser contexts. By leveraging widely used webhook platforms and lightweight scripts, APT28 complicates detection and underscores the need for heightened macro policies, traffic monitoring and proactive threat intelligence integration.

ATTACK TYPE	Cyberespionage	**SECTOR**	Government
REGION	Europe	**APPLICATION**	Microsoft Edge, Windows, MS Word

Source - https://lab52.io/blog/operation-macromaze-new-apt28-campaign-using-basic-tooling-and-legit-infrastructure/

TATA COMMUNICATIONS

Activists targeted with advanced CRESCENTHARVEST RAT using DLL sideloading

Researchers have identified a cyber-espionage campaign named CRESCENTHARVEST that exploits ongoing Iran protest narratives to target Farsi-speaking supporters with sophisticated malware. The operation delivers malicious shortcut files disguised as protest-related media and authentic Farsi reports, weaponising DLL sideloading via a signed Google binary. Once executed, the payload establishes persistence, steals credentials and Telegram data, logs keystrokes and communicates with a structured C2 infrastructure.

Threat intelligence indicates CRESCENTHARVEST is likely aligned with Iranian-linked actors focused on long-term surveillance of activists, dissidents and diaspora communities. By leveraging social-engineered lures tied to geopolitical events, the campaign bypasses conventional defences and harvests sensitive information for sustained espionage rather than short-term disruption. Organisations and individuals at risk are urged to heighten vigilance and strengthen endpoint defences against similar targeted intrusions.

ATTACK TYPE	Social engineering, Malware	**SECTOR**	Broadcast Media Production and Distribution, Social Media
REGION	Iran	**APPLICATION**	Google Chrome OS, Windows, Google Chrome, Telegram

Source - https://www.acronis.com/en/tru/posts/crescentharvest-iranian-protestors-and-dissidents-targeted-in-cyberespionage-campaign/

TATA COMMUNICATIONS

Compromised GrayCharlie WordPress campaign delivers NetSupport RAT at scale

Cybersecurity intelligence reveals that the GrayCharlie threat cluster, overlapping with SmartApeSG, continues large-scale compromises of WordPress sites by injecting malicious JavaScript that redirects visitors to deceptive browser update and ClickFix lures. These tactics deliver NetSupport RAT, later augmented by Stealc and SectopRAT payloads via multi-stage loaders. Recorded Future analysts note recurring hosting footprints and clustered TLS fingerprints, underscoring the operation's scale and persistence.

The campaign's infrastructure, predominantly hosted on MivoCloud and HZ Hosting Ltd, has also been linked to suspected supply-chain compromises affecting numerous U.S. law firm WordPress sites through shared IT providers, amplifying risk to professional services. Once deployed, GrayCharlie maintains stealthy remote access, harvests credentials and enables follow-on payloads. Defenders are urged to apply updated detection rules, block malicious IPs and domains, and harden web platforms.

ATTACK TYPE	Malware	**SECTOR**	Legal services, Business
REGION	USA	**APPLICATION**	WordPress, Windows

Source - https://www.recordedfuture.com/research/graycharlie-hijacks-law-firm-sites-suspected-supply-chain-attack

Phishing campaign delivers surveillance framework via tax impersonation

Researchers have identified a sophisticated cyber-espionage campaign exploiting phishing emails that impersonate the Income Tax Department of India to target residents. The multi-stage attack chain uses DLL sideloading, anti-debugging, encrypted shellcode and privilege escalation to deliver Blackmoon malware. By leveraging COM-based UAC bypass, process masquerading and persistent service installation, the operation enables stealthy access, resilient endpoint control and extensive monitoring.

Analysis reveals the final payload utilises SyncFuture Terminal Security Management (TSM), a legitimate Chinese remote management platform repurposed as an espionage framework. This provides attackers with deep surveillance capabilities, including remote monitoring, file access logging and user activity exfiltration. The campaign's blend of anti-analysis evasion and abuse of trusted software underscores growing advanced persistent threats focused on long-term intelligence gathering.

ATTACK TYPE	Malware, Cyberespionage	**SECTOR**	IT, Government, Business
REGION	India	**APPLICATION**	Windows

Source - https://www.esentire.com/blog/weaponized-in-china-deployed-in-india-the-syncfuture-espionage-targeted-campaign

TATA COMMUNICATIONS

First Gen-AI-driven Android malware PromptSpy exploits generative models

Security researchers have identified PromptSpy, the first Android malware to integrate generative AI directly into its execution flow, marking a significant evolution in mobile threats. The strain leverages Google's Gemini model to interpret real-time UI data and generate dynamic instructions that maintain persistence across devices. Delivered via fake banking-themed droppers, it abuses Accessibility Services to resist removal and capture sensitive device activity.

Once installed, PromptSpy deploys an embedded Virtual Network Computing module that grants attackers remote control, enabling lockscreen credential theft, screen recording and gesture capture. The malware's use of AI-assisted interface manipulation enhances adaptability across varied Android UIs while evasion techniques, such as overlay-based uninstall blocking, underscore the increasing sophistication of GenAI-assisted mobile threats. ESET's discovery signals a concerning shift in cyber risks.

ATTACK TYPE	Malware, Mobile	**SECTOR**	Financial services
REGION	Argentina	**APPLICATION**	Android

Source - https://www.welivesecurity.com/en/eset-research/promptspy-ushers-in-era-android-threats-using-genai/

TATA COMMUNICATIONS

Critical CVE-2026-1731 flaw in BeyondTrust software actively exploited globally

CVE-2026-1731 is a critical pre-authentication remote code execution flaw in BeyondTrust Remote Support and Privileged Remote Access software, assigned a CVSS score of 9.9 and now listed in CISA's Known Exploited Vulnerabilities (KEV) catalogue, mandating urgent remediation for federal and private sectors. Active in-the-wild exploitation has been observed within hours of public disclosure, underscoring the need for immediate patching.

Threat actors are weaponising the vulnerability via the WebSocket-exposed thin-scc-wrapper component to execute OS commands without authentication, enabling web shell deployment, account creation, command-and-control infrastructure, backdoor implants such as VShell and SparkRAT backdoors, lateral movement and data exfiltration across sectors globally. Self-hosted deployments without the latest updates or network segmentation controls remain at the highest risk.

ATTACK TYPE	Vulnerability, Malware	**SECTOR**	Healthcare, BFSI, Legal services, IT, Retail and Distribution
REGION	Australia, Canada, France, Germany, USA	**APPLICATION**	Apple Mac OS, Windows, Linux, BeyondTrust Privileged Remote Access

Source - https://unit42.paloaltonetworks.com/beyondtrust-cve-2026-1731/

TATA COMMUNICATIONS

ClickFix CAPTCHA Campaign enables malware infection via DLL sideloading

A forensic investigation into a major Polish organisation's breach reveals how a Fake CAPTCHA (ClickFix) campaign initiated a complex attack chain. Deceived users were lured into executing a malicious PowerShell command via the Windows Run dialogue, triggering DLL sideloading and deployment of the Latrodectus and Supper malware families. This social-engineering vector enabled reconnaissance, C2 communication and persistence mechanisms.

Analysts found that the initial payload downloaded obfuscated modules masquerading under legitimate Windows binaries, with DLL side-loading enabling latent execution across the environment. Subsequent Supper components established scheduled task persistence and encrypted command-and-control links, facilitating lateral movement and data exfiltration. The case underscores that even a single compromised click via opportunistic fake CAPTCHA delivery can precipitate enterprise-wide compromise.

ATTACK TYPE	Social engineering, Malware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Poland	**APPLICATION**	Windows, PowerShell

Source - https://cert.pl/en/posts/2026/02/fake-captcha-in-action/

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