TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: February 10, 2026

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

As we move through February 2026, increasingly sophisticated hostile activities continue to expand the cyber threat landscape. Traditional defence models are proving inadequate as adversaries exploit structural weaknesses across deeply interconnected digital ecosystems. To preserve resilience and strategic advantage, organisations must strengthen core security foundations, implement layered defences, and integrate anticipatory intelligence across their architectures.

In this high-stakes environment, Tata Communications' Cyber Threat Intelligence report becomes indispensable. Published weekly, the report provides 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 — protecting critical operations globally before disruption takes hold.

TATA COMMUNICATIONS

MedusaLocker variant Karma targets Windows systems across corporate sectors

The Karma (MedusaLocker) ransomware has emerged as a notable enterprise-focused threat, targeting Windows environments across sectors including BFSI, manufacturing, healthcare, and professional services. The strain encrypts files with hybrid RSA and AES cryptography, appending a ".KARMA" extension, and delivers an HTML ransom note asserting both encryption and data theft. Operators impose strict 72-hour deadlines, escalate demands, and threaten public disclosure to coerce payment.

First observed in underground threat forums, Karma leverages phishing and compromised access to achieve network-wide impact and reinforce extortion messaging by modifying desktop elements. The operation offers limited proof decryption and escalates fees after deadlines, with no public decryptor available. This reflects a mature extortion framework now contributing to rising ransomware pressure on organisations with weak incident-response and backup strategies.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Manufacturing, BFSI
REGION	North America, Europe, APAC	**APPLICATION**	Windows

Source - https://www.cyfirma.com/news/weekly-intelligence-report-16-january-2026/

TATA COMMUNICATIONS

Advanced Gopher Strike espionage weaponises GitHub and Golang malware tools

Threat analysts have identified two coordinated APT campaigns, “Gopher Strike” and “Sheet Attack”, targeting Indian government organisations, beginning in September 2025. Both operations leverage spear-phishing PDF lures containing malicious ISO payloads that only activate on Indian Windows systems, demonstrating geo-fencing and evasion measures. Custom Golang-based loaders and backdoors—GOGITTER, GITSHELLPAD and GOSHELL—are used to establish persistence and C2 channels.

The campaigns abuse legitimate cloud platforms and private GitHub repositories for command-and-control, masking malicious activity within trusted services while ultimately deploying tailored Cobalt Strike Beacons. Such techniques reflect advanced cloud exploitation and selective victim filtering, signalling sustained, targeted cyber espionage with refined tradecraft. Security teams should prioritise the detection of anomalous cloud service use and novel tooling to mitigate these sophisticated threats.

ATTACK TYPE	Malware	**SECTOR**	Software Development, Cryptocurrency
REGION	Global	**APPLICATION**	Apple Mac OS, VS Code

Source - https://www.zscaler.com/blogs/security-research/apt-attacks-target-indian-government-using-gogitter-gitshellpad-and-goshell

TATA COMMUNICATIONS

GlassWorm campaign abuses open VSX platform in supply chain infiltration

A sophisticated supply-chain attack compromised developer credentials on the Open VSX extension registry, enabling threat actors to publish malicious updates to four widely used extensions. Hidden GlassWorm loaders executed runtime-decrypted payloads that harvest credentials, browser data, and cryptocurrency wallet information. Security teams removed the poisoned versions and revoked access tokens, highlighting the risk of trusted identity abuse in software ecosystems.

GlassWorm's loader employs advanced evasion techniques, including locale-based profiling and Solana blockchain hooks to fetch command-and-control details, complicating detection and mitigation. The attack underscores the need for continuous monitoring of third-party plugins and robust authentication hygiene for developer accounts. Organisations are urged to audit installed extensions, rotate credentials, and implement enhanced supply-chain controls to reduce exposure.

ATTACK TYPE	Social engineering, Ransomware, Malware	**SECTOR**	Financial services, Business
REGION	Russia	**APPLICATION**	Microsoft Windows Defender, Windows, PowerShell

Source - https://socket.dev/blog/glassworm-loader-hits-open-vsx-via-suspected-developer-account-compromise

TATA COMMUNICATIONS

Chollima ecosystem splits into specialised cryptocurrency and espionage units

Recent threat analysis confirms that what was previously tracked as a single DPRK-aligned cyber actor, LABYRINTH CHOLLIMA, has formally evolved into three distinct adversaries with dedicated missions, tradecraft and malware toolsets. GOLDEN CHOLLIMA and PRESSURE CHOLLIMA now operate independently of the core group, leveraging specialised capabilities to pursue strategic and financially motivated objectives within the global cyber threat landscape.

GOLDEN and PRESSURE CHOLLIMA prioritise cryptocurrency and fintech targeting, conducting persistent and high-value theft operations, while core LABYRINTH CHOLLIMA continues focused espionage against defence, manufacturing, logistics and industrial sectors. Despite independent operations, shared infrastructure and tactical DNA underscore coordinated DPRK resource allocation. Organisations exposed to digital assets and critical systems must heighten vigilance.

ATTACK TYPE	Malware	**SECTOR**	Financial services, Manufacturing, Aerospace, Defence Industry, Cryptocurrency
REGION	Europe, Canada, India, South Korea, United States	**APPLICATION**	Apple Mac OS, Windows, Linux

Source - https://www.crowdstrike.com/en-us/blog/labyrinth-chollima-evolves-into-three-adversaries/

TATA COMMUNICATIONS

UK and US education sectors under siege from custom Interlock ransomware toolchain

The Interlock ransomware group continues to escalate assaults on primarily UK and US education organisations, leveraging a unique self-developed toolkit rather than a Ransomware-as-a-Service model, researchers report. Initial intrusion via a MintLoader infection progressed through NodeSnakeRAT and Interlock RAT implants, enabling persistence, credential theft, lateral movement, and data exfiltration before final ransomware deployment, underscoring the threat's sophistication.

Fortinet analysts highlight abuse of legitimate utilities such as ScreenConnect and AzCopy, and exploitation of a zero-day anti-cheat driver to disable defences, as part of Interlock's evolving tradecraft. Such techniques demonstrate the actor's capability to bypass traditional detection and control measures, reinforcing the need for proactive threat hunting, hardened access controls and integrated threat intelligence across security ecosystems.

ATTACK TYPE	Ransomware	**SECTOR**	Education
REGION	North America, United Kingdom, United States	**APPLICATION**	Windows, Node JS, PowerShell, ScreenConnect

Source - https://www.fortinet.com/blog/threat-research/interlock-ransomware-new-techniques-same-old-tricks

TATA COMMUNICATIONS

ShinyHunters vishing campaign compromises cloud SaaS platforms for data theft

Researchers report a significant expansion in ShinyHunters-aligned extortion activity, tracked under UNC6661, UNC6671 and UNC6240, against cloud SaaS and identity providers. The campaign leverages sophisticated voice phishing and victim-branded credential harvesting sites to steal both SSO credentials and MFA codes. Once access is gained, attackers exfiltrate sensitive data from SaaS platforms for extortion, with harassment and DDoS pressure tactics also observed.

Unlike traditional software exploits, this activity relies on social engineering to compromise organisations' identity systems, exploiting human trust to bypass authentication defences. Targeted platforms include Okta, Microsoft 365, SharePoint and Salesforce, illustrating broad coverage and opportunistic data theft for ransom. Security experts urge accelerated adoption of phishing-resistant MFA and comprehensive user awareness training to mitigate further compromise and financial fallout.

ATTACK TYPE	Phishing, Malware, Cyberespionage	**SECTOR**	Healthcare, IT, Government, Transportation, Education, E-commerce, BFSI, Airlines, Manufacturing, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Apple Mac OS, Windows, Linux, Slack, Okta, Salesforce

Source - https://cloud.google.com/blog/topics/threat-intelligence/expansion-shinyhunters-saas-data-theft

TATA COMMUNICATIONS

UAT-8099 operators intensify BadIIS deployment through compromised servers

Researchers have documented sustained intrusion activity by the threat actor UAT-8099 targeting vulnerable Internet Information Services (IIS) servers across Asia from late 2025 into early 2026, with a pronounced concentration in Thailand and Vietnam. Cisco Talos confirms significant operational overlap with the WEBJACK campaign and notes the use of web shells, PowerShell, and remote-control tools such as GotoHTTP to establish persistent access.

Analysts report that UAT-8099 has evolved its toolkit to deploy region-specific BadIIS malware variants, embedding geographic logic with tailored file extensions, dynamic page handling and localised HTML templates to drive search engine optimisation (SEO) fraud. A Linux BadIIS variant with proxy, injection and SEO fraud modes further underscores the actor's focus on stealthy, long-term monetisation-oriented compromises in affected territories.

ATTACK TYPE	Malware	**SECTOR**	Government, Business
REGION	India, Japan, Pakistan, Thailand, Vietnam	**APPLICATION**	Microsoft Internet Information Services (IIS), Windows, Linux

Source - https://blog.talosintelligence.com/uat-8099-new-persistence-mechanisms-and-regional-focus/

TATA COMMUNICATIONS

AI-assisted malware campaign exploits cloud services for command and control

Cybersecurity researchers have disclosed an advanced persistent threat campaign targeting Indian government entities, exploiting three bespoke backdoors — SHEETCREEP, FIREPOWER and MAILCREEP — since late 2025. The operation uses weaponised PDFs and LNK files to deliver malware that abuses trusted cloud services such as Google Sheets, Firebase and Microsoft Graph API for covert command-and-control. Evidence points to generative-AI-assisted malware development and a Pakistan-linked APT36 affiliate.

Analysis shows this campaign conducts multi-stage payload deployment with hands-on-keyboard activity and sophisticated evasion, blending malicious C2 traffic with legitimate SaaS channels to avoid detection. MAILCREEP manipulates mailboxes via Microsoft's Graph API, while FIREPOWER and SHEETCREEP leverage Firebase and Google Sheets, respectively. Researcher assesses with medium confidence that these operations reflect an evolved Pakistan-linked threat actor aligned with APT36's historical targeting.

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

Source - https://www.zscaler.com/blogs/security-research/apt-attacks-target-indian-government-using-sheetcreep-firepower-and

TATA COMMUNICATIONS

Tax-themed phishing surge delivers XWorm through spoofed government portals

A significant surge in phishing campaigns impersonating India's Income Tax Department has been detected, with threat actors distributing highly convincing emails and counterfeit tax portals to deceive recipients. These lures deliver the XWorm remote access trojan, enabling credential theft, system reconnaissance, keylogging and unauthorised data exfiltration. CERT-In has flagged the activity as high-risk, urging heightened vigilance and robust email defences.

The malicious operations exploit spear-phishing, masquerading and user execution vectors to compromise individuals and organisations, posing a significant risk to financial and personal information. Phishing messages often promise refunds or urgent action to entice clicks, while spoofed domains closely resemble the official tax portal. CERT-In recommends reporting suspicious communications to their official website and strictly avoiding password, OTP or banking detail disclosure.

ATTACK TYPE	Phishing, Malware	**SECTOR**	Financial services, Government, Business
REGION	India	**APPLICATION**	Apple Mac OS, Windows, Linux

Source - CERT-In Advisory reference

TATA COMMUNICATIONS

HoneyMyte enhances malware toolkit targeting government and corporate networks

Cybersecurity researchers report that HoneyMyte, also known as Mustang Panda or Bronze President, has significantly upgraded its CoolClient backdoor, deploying enhanced variants in ongoing espionage campaigns across Asia and Europe. The updated CoolClient leverages DLL sideloading to execute malicious payloads alongside scripts for reconnaissance and data theft, with variants actively harvesting credentials and exfiltrating sensitive information from targeted systems, especially within the government sector.

Analysts note the threat actor's use of multiple browser credential stealer variants targeting Chrome, Edge and other Chromium-based browsers, combined with modular plugins and custom scripts to capture system information and documents. Campaign telemetry shows concentrated activity in Myanmar, Malaysia, Mongolia, Thailand and Russia, underscoring a sustained focus on strategic espionage against public sector networks in Southeast Asia.

ATTACK TYPE	Malware, Cyberespionage	**SECTOR**	Government
REGION	Russia, Malaysia, Mongolia, Myanmar (Burma), Pakistan, Thailand	**APPLICATION**	Microsoft Edge, Mozilla Firefox, Windows, Google Chrome, FileZilla

Source - https://securelist.com/honeymyte-kernel-mode-rootkit/118590/

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