TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: May 12, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As May 2026 progresses, the cyber threat landscape continues to intensify, driven by increasingly advanced and coordinated adversarial activity. Conventional defence models are struggling to keep pace as threat actors exploit systemic vulnerabilities across highly interconnected digital environments. Sustaining resilience and competitive advantage now requires organisations to reinforce foundational security, adopt layered defence strategies, and embed forward-looking intelligence into their operational frameworks.

In this high-risk environment, the Tata Communications Cyber Threat Intelligence report serves as a critical resource. Issued weekly, it delivers incisive analysis of emerging threat campaigns, evolving attacker methodologies, and sector-specific risk exposures. By translating intelligence into actionable defence measures, security teams are better equipped to anticipate, respond to, and mitigate threats, ensuring continuity of critical operations at scale.

TATA COMMUNICATIONS

OilRig uses multi-stage steganography to conceal malicious command infrastructure

APT34, also tracked as OilRig and APT-C-49, has launched a sophisticated multi-stage phishing campaign using protest-themed lures to deploy a modular, fileless malware chain. Malicious Excel macros trigger local C# loader compilation, while staged payloads retrieved from GitHub and Google Drive enable stealthy execution, persistence, and extraction of encrypted configuration using LSB steganography.

The campaign abused trusted cloud platforms and Telegram Bot API infrastructure for encrypted command-and-control communications, enabling dynamic module delivery, remote execution, and covert espionage activity. Researchers note the malware operates primarily in memory, reducing forensic traces and complicating detection. The activity reflects a broader evolution towards cloud-enabled, stealth-focused intrusion frameworks targeting government, finance, energy, and telecommunications sectors.

ATTACK TYPE	Social engineering, Phishing, Cyber-espionage, APT	**SECTOR**	Government, Energy, BFSI, Telecommunications
REGION	Middle East, Europe, Asia, the United States	**APPLICATION**	Microsoft Excel, Windows, Google Drive, GitHub

Source - https://gbhackers.com/oilrig-hides-c2-config/

TATA COMMUNICATIONS

Banking Trojan Anatsa exploits financial institutions via Play Store distribution

A malicious document reader application on the Google Play Store was found distributing the Anatsa banking trojan to more than 10,000 users before removal. Disguised as a legitimate utility, the application employed a staged dropper mechanism to bypass marketplace security checks, later retrieving malicious payloads remotely and silently deploying malware onto compromised Android devices.

Once active, Anatsa abused accessibility permissions to intercept SMS messages, overlay banking applications, and harvest financial credentials from targeted users. Researchers identified advanced evasion capabilities, including sandbox detection, runtime payload execution, and steganography-style code concealment. The latest variants reportedly target 831 financial institutions globally, underscoring escalating risks across mobile banking ecosystems and official application marketplaces.

ATTACK TYPE	Malware, Mobile	**SECTOR**	BFSI, Cryptocurrency
REGION	Global	**APPLICATION**	Android

Source - https://www.cyberaccord.com/fake-document-reader-on-google-play-with-10k-downloads-installing-anatsa-malware/

TATA COMMUNICATIONS

TeamPCP weaponised SAP tools to harvest credentials across CI/CD pipelines

A supply chain compromise affecting SAP CAP npm packages has introduced malicious preinstall scripts designed to execute automatically during package installation. The campaign targeted widely used packages, including mbt and multiple @cap-js modules, downloading a Bun runtime to deploy obfuscated payloads capable of harvesting credentials, cloud tokens, and sensitive developer environment information.

Researchers identified strong overlaps with previously observed TeamPCP activity, including the abuse of trusted platforms, automated propagation methods, and advanced obfuscation techniques to evade detection. Stolen data, including GitHub, npm, and system secrets, was exfiltrated through attacker-controlled repositories, significantly increasing risks across SAP cloud development pipelines, CI/CD infrastructure, and enterprise software supply chains.

ATTACK TYPE	Malware, Supply Chain	**SECTOR**	IT, Software Development
REGION	Global	**APPLICATION**	Apple macOS, SAP, Windows, Linux, Node Packager Manager (npm), GitHub

Source - https://socket.dev/blog/sap-cap-npm-packages-supply-chain-attack#Indicators-of-Compromise

TATA COMMUNICATIONS

GlassWorm campaign exploits VSX sleeper extensions to deploy malware implants

A new phase of the GlassWorm campaign has emerged across the Open VSX ecosystem, where researchers identified 73 cloned extensions operating as sleeper implants. Initially published as benign packages mimicking legitimate developer tools, several were later weaponised through malicious updates that introduced transitive dependencies, obfuscated loaders, and externally hosted payload retrieval mechanisms.

Recent activation waves indicate a highly automated deployment pipeline, with coordinated updates pushing malicious extension packs within minutes across multiple publisher accounts. Researchers observed the use of GitHub-hosted VSIX payloads, native binaries, and runtime obfuscation techniques to evade detection while enabling stealthy compromise of developer environments, software repositories, and interconnected supply chain ecosystems.

ATTACK TYPE	Supply Chain	**SECTOR**	IT, Software Development
REGION	Global	**APPLICATION**	Apple macOS, Windows, Linux, VS Code, Cursor IDE

Source - https://socket.dev/blog/73-open-vsx-sleeper-extensions-glassworm?utm_medium=feed

TATA COMMUNICATIONS

VECT 2.0 ransomware critical error renders encrypted data permanently unrecoverable

VECT 2.0 is an emerging multi-platform ransomware targeting Windows, Linux, and VMware ESXi environments through an affiliate-driven RaaS model linked to TeamPCP supply chain operations. Researchers discovered a critical flaw in its ChaCha20-IETF encryption implementation, where incorrect nonce handling permanently destroys files larger than 128 KB, rendering recovery impossible even after ransom payment.

The ransomware employs shared code across all platform variants, enabling consistent destructive behaviour against enterprise assets, including virtual machine disks, databases, backups, and business documents. Despite marketing itself as a sophisticated ransomware framework with advanced encryption and anti-analysis capabilities, researchers identified multiple engineering flaws and ineffective features, effectively transforming VECT 2.0 into a destructive data wiper masquerading as ransomware.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail, Telecommunications, Software Development
REGION	Global	**APPLICATION**	VMWare ESXi, Windows, Linux

Source - https://research.checkpoint.com/2026/vect-ransomware-by-design-wiper-by-accident/

TATA COMMUNICATIONS

SLOTAGENT RAT deploys encrypted and post-exploitation capabilities for espionage

Researchers analysing a suspicious ZIP archive uploaded earlier this year identified SLOTAGENT, a previously undocumented remote access trojan employing a layered execution chain to evade detection. The malware uses API hashing, RC4 and XOR encryption, reflective DLL loading, and in-memory execution techniques to conceal functionality and complicate forensic analysis during targeted intrusions against enterprise environments.

SLOTAGENT establishes custom TCP-based command-and-control communications using structured JSON-like exchanges and supports extensive post-exploitation capabilities, including remote shell access, file transfers, screenshot capture, process memory dumping, and Beacon Object File execution. Researchers also observed anti-forensic functionality such as timestomping and encrypted configuration handling, reflecting increasingly stealth-focused malware engineering designed to sustain persistent access and data exfiltration.

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

Source - https://gbhackers.com/slotagent-malware-hides-api/

TATA COMMUNICATIONS

HeartlessSoul targets aviation sector with JavaScript RAT and GIS data theft

The HeartlessSoul threat group is conducting targeted cyber operations against aviation, industrial, and government organisations using phishing attachments, malvertising campaigns, and trojanised software installers. The intrusion chain deploys PowerShell loaders, Node.js components, and a JavaScript-based remote access trojan to establish persistence, exfiltrate sensitive data, and support long-term surveillance across compromised enterprise environments.

Researchers observed the campaign abusing trusted cloud platforms and Solana Name Service infrastructure to resolve command-and-control servers dynamically, complicating attribution and takedown efforts. The malware also collects geospatial intelligence and operational metadata from infected systems. Infrastructure overlaps with previously identified GOFFEE activity suggest coordinated operations and an increasingly sophisticated approach to stealth, resilience, and cross-sector targeting.

ATTACK TYPE	APT	**SECTOR**	Government, Aviation
REGION	Russia	**APPLICATION**	Microsoft Edge, Microsoft Outlook, ChromeOS, Windows, Node.js, Google Chrome, Microsoft Edge, PowerShell, Telegram

Source - https://advisory.eventussecurity.com/advisory/heartlesssoul-campaign-targeting-aviation-sector-via-email-attachments/

TATA COMMUNICATIONS

cPanel flaw exploitation enables access for SORRY ransomware and Mirai botnets

CERT-In has warned that CVE-2026-41940, a critical authentication bypass flaw in cPanel and WHM, is being exploited extensively through CRLF injection attacks targeting exposed management interfaces. Successful exploitation enables unauthenticated attackers to gain root-level administrative access, compromise hosted websites and databases, and execute malicious payloads across vulnerable hosting environments without requiring valid credentials or user interaction.

Researchers have linked ongoing exploitation campaigns to Mirai botnet variants and the “SORRY” ransomware, which encrypts compromised files using a “.sorry” extension and disrupts server operations. Security analysts report automated scanning and exploitation activity affecting thousands of internet-facing systems globally, with attackers leveraging compromised infrastructure for malware deployment, persistence, credential theft, and broader propagation across hosting ecosystems.

ATTACK TYPE	**Vulnerability, Cybercrime, Ransomware, Malware, DDoS**	**SECTOR**	**IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail, Telecommunications**
REGION	**Global**	**APPLICATION**	**Linux, cPanel and WHM (WebHost Manager)**

Source - CERT-IN Research

TATA COMMUNICATIONS

SHADOW-EARTH-053 leverages ProxyLogon flaws for persistent espionage compromise

SHADOW-EARTH-053 is a China-aligned cyberespionage group targeting government, defence, transportation, and critical infrastructure organisations through exploitation of unpatched Microsoft Exchange and IIS vulnerabilities, particularly the ProxyLogon chain. Following initial compromise, attackers deploy GODZILLA web shells and ShadowPad malware via DLL sideloading, enabling covert persistence, reconnaissance, mailbox access, and credential theft across affected enterprise environments globally.

Researchers observed the group using tunnelling utilities, including GOST and Wstunnel, alongside credential-harvesting tools such as Mimikatz and custom dumping utilities to support lateral movement and prolonged access. Overlapping victimology and shared tooling with SHADOW-EARTH-054 suggest parallel exploitation of exposed infrastructure rather than coordinated operations, reinforcing persistent risks posed by legacy internet-facing services lacking timely patch management.

ATTACK TYPE	Vulnerability, Malware, APT	**SECTOR**	Government, Transportation, Defence Industry, IT Services and Consulting
REGION	Europe, South Asia, East Asia	**APPLICATION**	Microsoft Active Directory Services, Microsoft Exchange Server, Microsoft Internet Information Services (IIS), Windows

Source - https://socprime.com/active-threats/shadow-earth-053-targets-exchange-servers-in-asia/

TATA COMMUNICATIONS

Advanced Silver Fox APT deploy ABCDoor through geofenced phishing operations

A Silver Fox APT campaign active between December 2025 and January 2026 used phishing emails impersonating tax authorities to distribute a modified RustSL loader targeting organisations across industrial, consulting, retail, and transportation sectors. The malware employed geofencing, virtual machine detection, and obfuscated payload delivery to evade analysis while expanding operations into additional regional targets.

The multi-stage infection chain deployed ValleyRAT, which subsequently installed a newly identified Python-based backdoor, ABCDoor, enabling remote access, file manipulation, screenshot capture, and credential theft. Researchers also observed Phantom Persistence techniques designed to survive reboots by disguising malicious execution as legitimate software updates, reflecting increasingly sophisticated persistence and stealth capabilities within evolving espionage-driven campaigns.

ATTACK TYPE	Phishing, Malware	**SECTOR**	Manufacturing, Transportation, Consultancy, Retail and Distribution
REGION	Russia, India, Japan, Cambodia, Indonesia, South Africa	**APPLICATION**	Python, Windows, Node.js

Source - https://securelist.com/silver-fox-tax-notification-campaign/119575/

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