TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: JANUARY 13, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As 2026 begins, the cyber threat landscape is intensifying, driven by increasingly sophisticated hostile activities. Traditional defence models are proving inadequate as threats continue to exploit the structural vulnerabilities of highly interconnected digital ecosystems. To maintain resilience and strategic advantage, organisations must strengthen foundational security frameworks, deploy multi-layered defences, and embed anticipatory intelligence throughout their architectures.

In this high-stakes environment, Tata Communications' Cyber Threat Intelligence report becomes indispensable. Published weekly, the report delivers an incisive analysis of emerging attack campaigns, evolving adversarial tactics, and sector-specific exposures. By translating intelligence into immediate defensive action, security teams can anticipate, prepare for, and neutralise threats proactively — safeguarding critical operations before disruption takes hold.

TATA COMMUNICATIONS

COOSEAGROUP leverages encryption and anonymised communication channels

Threat researchers have identified a new ransomware strain, **COOSEAGROUP**, predominantly active in Windows environments across the Asia-Pacific region. The malware encrypts files, appending a unique identifier and the ".Cooseagroup" extension, and generates a Chinese-language ransom note titled README.TXT demanding payment for decryption. The note also warns of sensitive data exposure and pressures victims with time-based escalation tactics.

The COOSEAGROUP ransom note instructs victims to contact attackers via the anonymised Session messenger and discourages third-party assistance, asserting that manual decryption attempts may irreversibly damage files. Researchers note that removal of the malware halts further encryption but offers no recovery, underscoring the imperative of secure backups. No free decryptor is currently available yet.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Tourism, Manufacturing, IT, Government, Energy, E-Commerce, BFSI, Aviation, Broadcast Media Production, Retailer, Telecommunications
REGION	APAC	**APPLICATION**	Windows

Source - https://www.cyfirma.com/news/weekly-intelligence-report-26-december-2025/

TATA COMMUNICATIONS

Emerging Kazu ransomware executes high-impact breaches using stolen credentials

Kazu is an emerging ransomware and data-extortion group first observed in mid-2025, quickly gaining traction as a threat actor against government, healthcare, financial services and public sector targets globally. The group's operations leverage a double-extortion model, exfiltrating significant volumes of sensitive data before deploying ransomware linked technically to LockBit variants to encrypt victim systems.

According to threat intelligence, Kazu exploits exposed remote services, unpatched web applications, stolen credentials and phishing to gain initial access, often via loaders such as SmokeLoader. Once inside, operators collect and compress extensive datasets, publish proof on a Tor leak site and negotiate ransoms through encrypted channels, threatening public disclosure to pressure victims into payment.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Financial services, Government
REGION	North America, Middle East, Europe, Africa, South Asia, East Asia, Latin America	**APPLICATION**	VMWare ESXi, Windows, Linux

Source - https://redpiranha.net/news/threat-intelligence-report-december-9-december-15-2025

TATA COMMUNICATIONS

Active LockBit campaign deploys multi-stage attacks across global enterprise targets

LockBit 5.0 remains one of the most active ransomware-as-a-service threats, employing a structured attack lifecycle that includes initial access, lateral movement, privilege escalation, and ransomware deployment. Its architecture disables backup and protection services and excludes critical system components to maximise impact. The variant leverages ChaCha20-Poly1305 encryption with X25519 and BLAKE2b key exchange, rendering local recovery infeasible.

Beyond encryption, LockBit 5.0 has expanded its global extortion model through a dedicated data leak site that lists compromised organisations and reinforces threats of public exposure. Security analysts note its cross-platform capabilities targeting Windows, Linux and ESXi environments, alongside advanced obfuscation and anti-analysis tactics that complicate detection and forensic response.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, IT, Business
REGION	Global	**APPLICATION**	Windows

Source - https://asec.ahnlab.com/ko/91834/

TATA COMMUNICATIONS

RondoDoX botnet weaponises React2Shell in sustained IoT and web attacks

Security researchers uncovered a sustained nine-month RondoDoX botnet campaign by analysing exposed command-and-control logs documenting activity from March to December 2025. The threat actors progressed from initial manual reconnaissance to automated, hourly exploitation of vulnerable web applications and IoT devices. The campaign leveraged over ten Rondo malware variants and six active C2 servers to expand botnet reach.

In December 2025, following public disclosure of the critical React2Shell vulnerability in Next.js Server Actions, operators rapidly weaponised this flaw for unauthenticated remote code execution. New C2 infrastructure deployed payloads including Mirai variants, cryptominers, and persistence frameworks on compromised hosts. The aggressive exploitation wave underscores heightened risk to internet-facing applications and embedded systems absent timely patching.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, Manufacturing, IT, Government, Transportation, Energy, E-Commerce, BFSI, Airline, Retailer and Distributor, Telecommunications
REGION	Global	**APPLICATION**	WordPress, Drupal, Oracle WebLogic , Next.js, React, Apache Struts 2

Source - https://www.cloudsek.com/blog/rondodox-botnet-weaponizes-react2shell

TATA COMMUNICATIONS

Authenticated WhatsApp sessions exploited to propagate Astaroth banking trojan

A sophisticated multi-stage malware campaign abuses authenticated WhatsApp Web sessions to propagate the Astaroth (Guildma) implant via automated messaging. The operation begins with a Python-based SORVEPOTEL worm that hijacks active WhatsApp Web sessions using Selenium and ChromeDriver, harvesting contacts and sending high-trust lure messages. Victim interaction with the lure triggers a complex execution chain delivered wholly in memory.

Upon execution of the malicious VBS file, parallel loaders deploy additional components, including an MSI installer that unpacks an AutoIt loader, which decrypts and decompresses the final Astaroth payload. This memory-resident implant establishes IMAP-based command-and-control and lightweight HTTP telemetry, enabling stealthy backdoor access and resilient propagation. The campaign leverages trusted communications and living-off-the-land binaries to evade detection.

ATTACK TYPE	Social engineering, Malware	**SECTOR**	Financial services, BFSI, Cryptocurrency
REGION	Brazil, Latin America	**APPLICATION**	Windows, Google Chrome, WhatsApp

Source - https://blackpointcyber.com/blog/whatsapp-worm-sorvepotel-astaroth-malware/

TATA COMMUNICATIONS

Fake employee evaluations deliver malware enabling remote system surveillance

Security researchers have identified an active phishing campaign distributing Guloader malware via emails impersonating internal communications on October 2025 employee performance reviews. The messages reference potential layoffs to coerce recipients into opening a malicious RAR attachment whose file extension is concealed, increasing the likelihood of execution. This social-engineering tactic aims to lure recipients into engaging with the payload.

Analysis reveals the attachment contains an NSIS-compiled executable that loads shellcode from a Google Drive URL directly into memory, avoiding disk-based detection, and subsequently deploys the Remcos remote access trojan. Once executed, Remcos enables threat actors to perform remote command execution, capture keystrokes, screenshots, webcam and microphone feeds, and harvest browser credentials, underscoring significant post-compromise risks.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, Financial services, Manufacturing, IT, Government, Transportation, Education, Energy, Retailer and Distributor, Telecommunications
REGION	Global	**APPLICATION**	Windows

Source - https://asec.ahnlab.com/ko/91798/

TATA COMMUNICATIONS

DarkSpectre’s multi-year campaign uses trusted extensions for surveillance and fraud

DarkSpectre is a sophisticated and well-resourced Chinese threat actor behind at least three interconnected browser extension campaigns that have infected over 8.8 million users across Chrome, Edge, Firefox and Opera. Koi Security’s research links ShadyPanda and GhostPoster with a newly disclosed Zoom Stealer operation, underscoring long-term surveillance, affiliate fraud and stealthy payload delivery embedded within extensions that appear legitimate to end users.

ShadyPanda’s mass-scale extensions have operated for years before activating malicious behaviour, harvesting search and personal data, while GhostPoster uses steganographic techniques to conceal JavaScript within image assets. The Zoom Stealer campaign silently exfiltrates corporate meeting intelligence from more than 28 conferencing platforms, illustrating DarkSpectre’s strategic evolution from consumer-focused fraud to large-scale corporate espionage and persistent surveillance.

ATTACK TYPE	Malware	**SECTOR**	Financial services, IT, Business, Cryptocurrency
REGION	Global	**APPLICATION**	Microsoft Edge, Google Chrome OS, Mozilla Firefox, Opera Browser, Google Chrome

Source - https://www.koi.ai/blog/darkspectre-unmasking-the-threat-actor-behind-7-8-million-infected-browsers

TATA COMMUNICATIONS

VVS stealer exploits PyArmor obfuscation to compromise Discord accounts globally

VVS Stealer, a Python-based infostealer actively sold on Telegram since April 2025, targets Discord users by exfiltrating account tokens and sensitive credentials. Packaged with PyInstaller, the malware is heavily obfuscated using PyArmor in BCC mode to evade static analysis and detection. Researchers report it hijacks active Discord sessions by injecting malicious JavaScript into the Electron runtime.

Upon execution, VVS Stealer not only steals Discord-related tokens and credentials but also harvests browser-stored data, including cookies, passwords and history. The malware persists by installing itself in Windows startup folders, displays fake error messages to conceal activity, and exfiltrates data via Discord webhooks. Analysts highlight growing abuse of obfuscation tools in commodity malware aimed at popular platforms.

ATTACK TYPE	Malware	**SECTOR**	IT, Gaming industry, Software Development, Social Media
REGION	Global	**APPLICATION**	Python, Windows, DISCORD

Source - https://unit42.paloaltonetworks.com/vvs-stealer/

TATA COMMUNICATIONS

PHALT#BLYX campaign leverages Windows utilities to deliver DCRat trojan stealthily

The multi-stage PHALT#BLYX malware campaign exploits social engineering and trusted system tools to compromise the hospitality sector, beginning with phishing emails purporting to be Booking.com reservation alerts. Victims encounter fake CAPTCHA prompts followed by a simulated Blue Screen of Death that pressures them into executing malicious PowerShell commands, which silently retrieve and compile malware via the legitimate MSBuild utility.

Once executed, the infection chain disables Windows Defender and establishes persistence, ultimately deploying a customised DCRat remote access Trojan capable of process hollowing, credential harvesting and secondary payload delivery. Indicators such as embedded Russian-language artefacts, Euro-denominated lures and prior threat actor behaviour link this activity to Russian-associated operators. Security experts warn that such “ClickFix” tactics highlight the rising sophistication of malware delivery.

ATTACK TYPE	Malware	**SECTOR**	Tourism
REGION	Europe	**APPLICATION**	Microsoft Windows Defender, Windows, PowerShell

Source - https://www.securonix.com/blog/analyzing-phaltblyx-how-fake-bsods-and-trusted-build-tools-are-used-to-construct-a-malware-infection/

TATA COMMUNICATIONS

Intellexa spyware targets mobile platforms using advanced zero-day vulnerabilities

Intellexa, the operator of the Predator spyware platform, continues to exploit advanced zero-day vulnerabilities despite sanctions and heightened scrutiny by international security researchers. According to Google's Threat Intelligence Group analysis, at least 15 distinct zero-days across Android, iOS and Chrome have been linked to Intellexa since 2021. These include remote code execution, sandbox escape and privilege escalation flaws, all patched by vendors following disclosure.

The sustained exploitation of these vulnerabilities enables covert delivery and execution of sophisticated spyware against high-value mobile targets. Evidence suggests Intellexa both develops and acquires exploit chain components from external parties, maintaining operational capability. Such techniques pose systemic risk to mobile-centric enterprises and emphasise the need for rapid patching and robust threat intelligence integration within corporate security practices.

ATTACK TYPE	Vulnerability, Malware	**SECTOR**	Healthcare, Manufacturing, Construction, IT, Government, Journalism, Energy, Business, BFSI, Aviation, Retailer, Telecommunications
REGION	Global	**APPLICATION**	Android, Apple IOS, Google Chrome OS, Google Chrome

Source - https://cloud.google.com/blog/topics/threat-intelligence/intellexa-zero-day-exploits-continue

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