TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: January 20, 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 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 predictive 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.

INTRODUCTION

EMERGING CRAZYHUNTER CAMPAIGN SPREADS THROUGH AD AND BYPASSES SECURITY

AUTHENTICATED REMOTE CODE EXECUTION FLAW HITS N8N PLATFORM

BANKING MALWARE ASTAROTH EXPLOITS WHATSAPP WEB FOR RAPID PROPAGATION

RISING RIPPER RANSOMWARE DEMONSTRATES RAPID ENCRYPTION AND EXFILTRATION

SPEARPHISHING CAMPAIGN LEVERAGES RUSTYWATER FOR STEALTHY INTRUSION

BQTLOCK RANSOMWARE DEPLOYS HYBRID ENCRYPTION TO DEMAND MONERO

BLUEDELTA CYBER GROUP HARVESTS CREDENTIALS VIA SPOOFED LOGIN PORTALS

NEW VECT RANSOMWARE OPERATION TARGETS ENTERPRISE SYSTEMS AT SCALE

AI-ASSISTED PHISHING EXPLOITS VPN DOWNLOADS TO CAPTURE CREDENTIALS

THREAT ACTORS WEAPONISE CVE-2025-55182 AS SERVER-BREACHING ENTRY POINT

TATA COMMUNICATIONS

CrazyHunter ransomware exploits Active Directory and BYOVD-driven network

CrazyHunter ransomware has emerged as a rapidly evolving Go-based threat derived from the Prince ransomware family and now shows advanced Active Directory compromise, lateral propagation, and defence evasion capabilities. It primarily targets Taiwanese critical sectors, especially healthcare, exploiting weak domain credentials and lateral movement via SharpGPOAbuse, with multiple confirmed institutions compromised and sensitive data publicised on a leak site.

The campaign deploys sophisticated techniques, including Bring-Your-Own-Vulnerable-Driver (BYOVD) attacks using a signed Zemana driver to escalate privileges and neutralise security defences. Once inside, the malware spreads broadly via abused Group Policy Objects and encrypts network resources using hybrid ChaCha20-ECIES encryption, coercing victims with ransom demands and reputational pressure, underscoring the urgency for enhanced threat detection and proactive cyber defences.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare
REGION	Taiwan	**APPLICATION**	Windows

Source - https://www.trellix.com/blogs/research/the-ghost-in-the-machine-crazyhunters-stealth-tactics/

n8n workflow automation platform exposed to critical authenticated RCE

A critical authenticated Remote Code Execution vulnerability (CVE-2026-21877) has been reported in the n8n workflow automation platform, affecting versions >= 0.123.0 and < 1.121.3, including both self-hosted and n8n Cloud environments. Under certain conditions, authenticated users can trigger arbitrary code execution via unsafe file write operations, potentially leading to full system compromise. The issue is resolved in version 1.121.3.

Security researchers emphasise immediate updates to mitigate this maximum-severity (CVSS 10.0) flaw that leverages the Git node and other file interaction points. Organisational risk includes control of workflows, unauthorised access to credentials, and disruption of automated processes. If upgrading to 1.121.3 is not feasible, administrators should disable the Git node and restrict untrusted access as a temporary defence.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Financial services, Manufacturing, IT, Government, Transportation, Education, Energy, Telecommunications
REGION	Global	**APPLICATION**	Apple Mac OS, Windows, Linux, n8n

Source - https://github.com/n8n-io/n8n/security/advisories/GHSA-v364-rw7m-3263

Astaroth malware spreads via WhatsApp web campaign for credential theft

The Astaroth banking malware has resurfaced in the Boto-Cor-de-Rosa campaign, exploiting WhatsApp Web as a worm-like propagation vector to target Brazilian users. Delivered via malicious ZIP archives containing an obfuscated Visual Basic downloader, the attack installs both the Delphi-based banking Trojan and a Python-written WhatsApp spreader that harvests contacts and auto-forwards infected files to perpetuate infection.

Once executed on a Windows system, Astaroth's dual modules operate in parallel: one silently monitors web browsing to capture banking credentials, the other automatically disseminates malicious ZIP files to all harvested contacts, creating a self-sustaining infection loop. Researchers note the campaign leverages region-specific social engineering and multilingual components, underscoring evolving tactics and the continued threat to users dependent on trusted messaging platforms.

ATTACK TYPE	Social engineering, Malware	**SECTOR**	BFSI
REGION	Brazil	**APPLICATION**	Python, WhatsApp

Source - https://www.acronis.com/en/tru/posts/boto-cor-de-rosa-campaign-reveals-astaroth-whatsapp-based-worm-activity-in-brazil/

TATA COMMUNICATIONS

Emerging Ripper ransomware operation targets Windows with double extortion

Researchers uncovered Ripper ransomware during underground forum monitoring as part of threat discovery operations, identifying it as a Windows-targeting malware that encrypts data using both AES and RSA and appends a ".ripper12" extension to compromised files. Ripper also alters desktop visuals and delivers a READ_NOTE.html ransom note threatening data exfiltration and public exposure to enforce double extortion.

According to the intelligence reports, Ripper exhibits advanced persistence mechanisms and post-compromise behaviour, including scheduled task manipulation and credential capture techniques. Its operators provide proof-of-decryption and impose time-bound payment demands, suggesting emerging sophistication. CYFIRMA assesses Ripper as an evolving operation that may expand targeting, deployment efficiency and sustained threat presence within the ransomware ecosystem.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, IT, Government, Military, Business, BFSI, Airlines, Retailer and Distributor, Telecommunications
REGION	Global	**APPLICATION**	Windows

Source - https://www.cyfirma.com/news/weekly-intelligence-report-09-january-2026/

TATA COMMUNICATIONS

Muddy Water APT group deploys Rust-based implants in spearphishing campaign

Threat analysts have identified a targeted spearphishing campaign attributed to the Muddy Water APT group actively exploiting diplomatic, maritime, financial and telecommunications organisations across the Middle East. Attackers employ icon-spoofed emails and macro-enabled Microsoft Word documents to deliver a Rust-based implant, dubbed RustyWater, indicating a marked shift from legacy PowerShell tooling toward modern, structured remote access capabilities.

Once deployed, RustyWater establishes persistence via Windows registry modifications, leverages asynchronous HTTP command-and-control and incorporates anti-analysis and modular post-compromise functionality, enabling tailored capability expansion. This evolution reflects Muddy Water's adoption of stealthier, low-noise remote access tooling that complicates forensic analysis and detection, underscoring heightened risk to critical infrastructure and the need for robust defensive measures within affected sectors.

ATTACK TYPE	Malware, Cyber espionage	**SECTOR**	Financial services, Government, Telecommunications
REGION	Middle East, Turkmenistan, United Arab Emirates	**APPLICATION**	Microsoft Word, Windows

Source - https://www.cloudsek.com/blog/reborn-in-rust-muddywater-evolves-tooling-with-rustywater-Implant

TATA COMMUNICATIONS

Hybrid BQTLock ransomware leveraging hybrid encryption and data leak pressure

BQTLock is a ransomware-as-a-service (RaaS) strain first observed in mid-2025 that rapidly broadened its reach from the Middle East to global victims, according to threat intelligence reporting. It uses robust AES-256 and RSA-4096 hybrid encryption, appends the ".bqtlock" extension to compromised files, and employs a strict double-extortion model with data leak threats and escalating deadlines to pressure payment.

The group demands Monero payments via tiered "wave" pricing and combines ideological messaging with financial incentives, though researchers assess profit as the primary driver. Confirmed 2025 victims span US, European and Middle Eastern organisations, including education, healthcare and SMEs. BQTLock's ongoing operations into 2026 underscore its technical evolution and persistent threat to sectors with weaker security, as documented in the December–January intelligence report.

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

Source - https://redpiranha.net/news/threat-intelligence-report-december-30-2025-january-5-2026

TATA COMMUNICATIONS

Credential harvesting campaign by BlueDelta leverages PDFs and infrastructure

Between February and September 2025, cybersecurity researchers observed a series of targeted credential harvesting campaigns by BlueDelta, a threat group linked to Russia's GRU. The operations used spoofed Microsoft Outlook Web Access (OWA), Google and Sophos VPN login portals to deceive users and collect credentials before redirecting them to legitimate websites. The campaigns abused free hosting, tunnelling and link-shortening services such as Webhook[.]site, InfinityFree, Byet Internet Services and ngrok to host malicious content and exfiltrate stolen data. Several lures included legitimate PDF documents to improve credibility and evade automated defences.

Analysis indicates that BlueDelta's targeting was deliberate and intelligence-driven, focusing on researchers and institutions in Türkiye and Europe with ties to energy, nuclear research, defence cooperation, and government communication networks. BlueDelta's continued refinement of credential-theft tradecraft suggests an ongoing interest in harvesting credentials from high-value organisations, maintaining low-cost infrastructure to support Russian strategic priorities and espionage objectives.

ATTACK TYPE	Malware, Phishing	**SECTOR**	IT, Government, Education, Defence and Space Manufacturing, International Trade and Development, Renewable Energy
REGION	Europe, North Macedonia, Turkey, Uzbekistan	**APPLICATION**	Microsoft Outlook, Google OAuth, Sophos VPN

Source - https://www.recordedfuture.com/research/gru-linked-bluedelta-evolves-credential-harvesting

TATA COMMUNICATIONS

Vect ransomware exploits enterprise systems with high automation and impact

Vect has been identified in early January 2026 as a new Ransomware-as-a-Service operation delivering a custom C++ ransomware strain with cross-platform targeting of Windows, Linux and VMware ESXi environments. Its use of the high-speed ChaCha20-Poly1305 encryption and Safe Mode boot manipulation to bypass defences, combined with automated lateral movement via SMB and WinRM, highlights significant technical sophistication and rapid enterprise impact.

Operating a strict double-extortion model, Vect leverages TOR-only infrastructure, Monero payments and a professional affiliate ecosystem with tiered commissions, negotiation portals and public leak sites. Initial activity has affected organisations in Brazil and South Africa across education and manufacturing, suggesting experienced operators behind the campaign.

ATTACK TYPE	Malware	**SECTOR**	Manufacturing, Education
REGION	Brazil, South Africa	**APPLICATION**	VMWare ESXi, Windows, Linux

Source - https://redpiranha.net/news/threat-intelligence-report-january-6-january-12-2026

TATA COMMUNICATIONS

SEO-driven Fortinet VPN campaign steals credentials via fake download portals

A sophisticated phishing campaign is exploiting search engine optimisation and AI-generated search summaries to impersonate Fortinet's official VPN download portal, researchers report. Threat actors host initial content on GitHub Pages to leverage platform trust and artificially elevate search rankings, then redirect users from major search engines to a cloned Fortinet site.

The multi-stage attack flow selectively redirects human visitors from search results to evade automated security scans, while harvesting login details via a deceptive modal that mimics Fortinet's interface. Organisations and remote workers should verify URLs and block known malicious domains such as vpn-fortinet[.]github[.]io and fortinet-vpn[.]com, reinforcing that legitimate downloads rarely require pre-authentication before installer access.

ATTACK TYPE	Phishing	**SECTOR**	IT
REGION	Global	**APPLICATION**	Fortinet FortiClient SSL VPN, Fortinet VPN, Fortinet

Source - https://cybersecuritynews.com/fake-fortinet-sites/

TATA COMMUNICATIONS

React2shell (CVE-2025-55182) flaw leveraged for automated ransomware deployment

Researchers have confirmed exploitation of the critical React2Shell vulnerability (CVE-2025-55182) as an initial access vector for ransomware, marking a shift from prior reports of backdoors and cryptomining to direct cyber-extortion attacks. In a recently investigated case, a financially motivated actor gained unauthenticated access to a corporate web server and deployed Weaxor ransomware in under one minute, underscoring automation and urgency to patch vulnerable React Server Components.

Researchers have confirmed exploitation of the critical React2Shell vulnerability (CVE-2025-55182) as an initial access vector for ransomware, marking a shift from prior reports of backdoors and cryptomining to direct cyber-extortion attacks. In a recently investigated case, a financially motivated actor gained unauthenticated access to a corporate web server and deployed Weaxor ransomware in under one minute, underscoring automation and urgency to patch vulnerable React Server Components.

ATTACK TYPE	Vulnerability, Malware	**SECTOR**	IT and Software Development
REGION	Global	**APPLICATION**	Apple Mac OS, Windows, Linux, Next.js, React

Source - https://www.s-rminform.com/latest-thinking/react2shell-used-as-initial-access-vector-for-weaxor-ransomware-deployment

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