TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: January 27, 2026

TATA

THREAT INTELLIGENCE ADVISORY REPORT

As 2026 gets underway, the cyber threat landscape is expanding, shaped by increasingly sophisticated and persistent hostile activity observed through January. Traditional defence models are falling short as adversaries systematically exploit structural weaknesses across deeply interconnected digital ecosystems. To preserve resilience and strategic advantage, organisations must reinforce core security foundations, deploy layered defences, and embed 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.

Hacktivist activity surges with increased defacement and disruption campaigns

During January 2026, India’s cyber threat environment saw a sustained escalation in hacktivist-driven operations, with multiple collectives issuing overt claims of anti-India campaigns and naming targeted digital assets. These activities were accompanied by a marked rise in website defacements and service disruptions across government, education, healthcare and BFSI sectors. This pattern reflects a visibility-focused threat profile prioritising narrative impact over technical complexity.

Threat analysts reported that coordinated distributed denial-of-service actions and defacement incidents were leveraged to amplify psychological impact, undermining confidence in public and private digital infrastructure. Such hacktivist campaigns, often tied to geopolitical narratives and social discourse, compounded pressure on organisations to enhance defensive posture and incident readiness. Sector-wide resilience gaps have become more evident as January’s activity intensified.

ATTACK TYPE	Vulnerability, Hacktivism, Breaches, DDoS, Cyberespionage	SECTOR	Healthcare, Manufacturing, IT, Government, Education, Defence Industry, BFSI, Broadcast Media Production, Retailer and Distributor, Telecommunications
REGION	India	APPLICATION	Apple Mac OS, Android, iOS, Windows, Linux

Source - CTI Team Internal Research

LOTUSLITE backdoor delivered through geopolitically themed lures in targeted campaign

Security researchers have disclosed a targeted espionage campaign against U.S. government and policy entities, exploiting geopolitical tensions with Venezuela to entice victims with a politically themed ZIP archive. The malicious file leverages DLL sideloading to deploy a custom backdoor, LOTUSLITE, capable of remote command execution, file operations, data exfiltration and persistent access via the Windows Registry.

Analyst units have attributed the operation with moderate confidence to the China-linked Mustang Panda group, noting infrastructure and tradecraft overlaps with previous campaigns. The spear-phishing delivery method reflects a growing trend of using current political events as lures against high-value targets. Though technically unsophisticated, the focused targeting underscores ongoing strategic cyber-espionage risks.

ATTACK TYPE	Malware, Cyberespionage	SECTOR	Government
REGION	United States	APPLICATION	Windows

Source - https://www.acronis.com/en/tru/posts/lotuslite-targeted-espionage-leveraging-geopolitical-themes/

Sicarii ransomware emerges with ideological branding and immature tradecraft

Sicarii, a previously unidentified RaaS operation first detected in late 2025, has attracted attention for its overt Israeli and Jewish branding, incorporating Hebrew text and historical symbols uncommon in financially motivated ransomware campaigns. However, research notes that underground communications are predominantly in Russian, and Hebrew content appears non-native, raising questions about the authenticity of the group's claimed identity.

Technical analysis reveals that Sicarii's malware executes geo-fencing to avoid Israeli systems and employs typical extortion capabilities such as AES-GCM encryption and credential harvesting, yet the operation exhibits early-stage tooling and inconsistent victim narratives. These behavioural anomalies and linguistic discrepancies suggest performative identity signalling rather than mature ideological motivation, leaving attribution inconclusive as of mid-January 2026.

ATTACK TYPE	Ransomware	SECTOR	Manufacturing, Business, Social Media
REGION	Middle East, Europe	APPLICATION	Windows, Fortinet

Source - https://research.checkpoint.com/2026/sicarii-ransomware-truth-vs-myth/

Cisco gateway flaw enables unauthenticated remote command execution attacks

Cisco has disclosed an active attack campaign exploiting CVE-2025-20393, a critical vulnerability (CVSS 10.0) in AsyncOS-powered Cisco Secure Email Gateway and Secure Email and Web Manager appliances that expose the Spam Quarantine feature to the internet. The flaw enables unauthenticated remote command execution with root privileges, permitting full appliance takeover. Cisco warns organisations to urgently assess exposure and apply mitigations.

Cisco researchers attribute observed intrusions to UAT-8837, a China-nexus advanced persistent threat actor targeting critical infrastructure sectors in North America, deploying persistence mechanisms post-compromise. Affected environments have seen root-level control established and tooling installed to maintain access. As of mid-January, Cisco has released patches; immediate upgrades and configuration reviews are required to remove implanted artefacts and prevent further exploitation.

ATTACK TYPE	Vulnerability, Malware	SECTOR	IT, Government, Energy, Business, Telecommunications
REGION	Global	APPLICATION	Cisco Email Security Appliance, Cisco AsyncOS, Cisco Secure Email, Cisco Web Manager

Source - https://blog.talosintelligence.com/uat-8837/

Emerging DeadLock group decentralised blockchain to rotate proxy infrastructure

DeadLock is a low-profile ransomware family first identified in July 2025, drawing attention in mid-January after researchers confirmed its abuse of Polygon smart contracts. Rather than traditional infrastructure, the group stores and rotates proxy server addresses on the blockchain, complicating attribution and takedown efforts while enabling resilient command-and-control communications observed across limited but targeted victim environments globally.

Analysis shows DeadLock operates without a public leak site or affiliate programme, relying instead on stealth and decentralisation. Investigators observed evolving ransom notes, unverified data theft claims, and AnyDesk-facilitated access. A PowerShell-based toolset is used for service disruption, while smart contracts are queried dynamically to retrieve proxy URLs supporting a Session-based HTML interface during active campaigns.

ATTACK TYPE	Ransomware	SECTOR	Healthcare, Tourism, E-Commerce, Manufacturing, Construction, IT, Government, Education, Energy, BFSI, Airlines, Retailer, Telecommunications
REGION	Global	APPLICATION	AnyDesk, Windows, PowerShell

Source - https://www.group-ib.com/blog/deadlock-ransomware-polygon-smart-contracts/

INTRODUCTION

SUSTAINED HACKTIVIST ACTIVITY TARGETS CRITICAL INFRASTRUCTURE AND PUBLIC SERVICES

LOTUSLITE USES DIPLOMATIC LURES TO DEPLOY PERSISTENT BACKDOOR IMPLANT

SICARII RANSOMWARE SURFACES TO TARGET ENTERPRISES WITH IDEOLOGICAL POSITIONING

CRITICAL CISCO VULNERABILITY EXPLOITED TO GAIN FULL APPLIANCE CONTROL REMOTELY

DEADLOCK EXPLOITS SMART CONTRACTS TO MAINTAIN COVERT COMMUNICATION CHANNELS

REMOTE CODE EXECUTION VULNERABILITY IN FORTISIEM EXPLOITED AFTER POC EMERGES

MOBILE BANKING TROJAN DEVIXOR EVOLVES INTO MULTIFUNCTIONAL THREAT

PYTHON MALWARE TARGETS WINDOWS USERS FOR CONTINUOUS DATA EXFILTRATION

PHISHING CAMPAIGN USES CLOUDFLARE SERVICES TO MASK ASYNCRAT DISTRIBUTION

PLUGGYAPE DEPLOY PYTHON BACKDOOR THROUGH FAKE CHARITABLE FOUNDATION LURE

FortiSIEM RCE flaw under active exploitation as PoC emerges for CVE-2025-64155

Fortinet has disclosed and patched a critical FortiSIEM vulnerability, CVE-2025-64155, rated 9.4/9.8 on the CVSS scale, that permits unauthenticated remote code execution via crafted TCP requests to the phMonitor service on port 7900. The flaw impacts Super and Worker nodes across several FortiSIEM versions and enables argument injection, arbitrary file writes and privilege escalation to root. A public PoC has been released.

Organisations are urged to apply Fortinet's security updates immediately, as active exploitation has been observed in the wild and attackers can leverage the flaw to compromise enterprise monitoring infrastructure. Interim mitigation includes restricting access to the vulnerable phMonitor port. The disclosure and rapid exploit publication underscore ongoing threat actor interest in high-impact vulnerabilities.

ATTACK TYPE	Vulnerability	SECTOR	Healthcare, Manufacturing, IT, Government, Military, Business, BFSI, Aviation, Retailer and Distributor, Telecommunications
REGION	Global	APPLICATION	Fortinet , FortiSIEM

Source - https://thehackernews.com/2026/01/fortinet-fixes-critical-fortisiem-flaw.html

deVixor Android RAT leverages phishing to steal credentials and deploy ransomware

The deVixor Android banking RAT continues to evolve as a multifaceted threat, with the analysis of over 700 malicious APK samples since October 2025 confirming large-scale campaigns targeting Iranian users via phishing sites masquerading as automotive businesses. Beyond SMS harvesting, recent variants now encompass credential theft, persistent surveillance and remote control, organised through Telegram bots and Firebase-based command infrastructure.

Recent technical findings highlight deVixor's expanded capabilities in harvesting financial data from SMS and WebView-based JavaScript injection, along with a remotely triggered ransomware module that locks devices and demands cryptocurrency payments. The malware's regional focus on Iranian banks, domestic payment services and cryptocurrency platforms underscores deliberate targeting, with ongoing feature updates and evasion techniques reinforcing its status as an active, scalable criminal operation.

ATTACK TYPE	Malware	SECTOR	IT, BFSI, Government, Automobile, Retailer and Distributor, Cryptocurrency
REGION	Iran	APPLICATION	Android

Source - https://cyble.com/blog/devixor-an-evolving-android-banking-rat-with-ransomware-capabilities-targeting-iran/

Surveillance malware SolyxImmortal exfiltrates sensitive data through platform abuse

Emerging in January 2026, the SolyxImmortal information-stealing malware has been analysed as a stealth-focused threat that persistently surveils compromised Windows systems without destructive behaviour. Written in Python and delivered as a standalone script, it establishes persistence via AppData replication and registry autorun, harvesting credentials from Chromium-based browsers, sensitive documents, keystrokes and screenshots before exfiltrating data using hardcoded Discord webhooks.

Analysts note SolyxImmortal leverages legitimate APIs and trusted third-party infrastructure to evade detection, operating entirely in the user space and avoiding overt anomalies common to high-profile malware. Continuous monitoring targets high-value user actions, with routine screenshots and batched keystroke capture sent to dedicated webhook channels. Its design suggests reuse by mid-tier actors and underscores growing commodity malware risks in early 2026.

ATTACK TYPE	Malware	SECTOR	IT, Healthcare, BFSI, Manufacturing, Government, Education, Energy, Retailer and Distributor, Telecommunications
REGION	Global	APPLICATION	Chromium, Python, Windows, DISCORD

Source - https://www.cyfirma.com/research/solyximmortal-python-malware-analysis/

AsyncRAT delivered through Cloudflare tunnels and Python injection techniques

Analysts have identified a sophisticated multi-stage AsyncRAT campaign abusing Cloudflare's free-tier TryCloudflare tunnels to host malicious WebDAV servers, effectively concealing command-and-control infrastructure behind trusted services. The attack initiates with Dropbox-delivered phishing emails containing double-extension shortcut files that download multi-stage scripts. These fetch further components, display decoy PDFs, and progressively build a full Python environment on victim systems.

Within the compromise chain, adversaries use the Python environment to perform APC-based injection into explorer.exe and establish persistence through Startup scripts, leveraging living-off-the-land techniques such as Windows Script Host and PowerShell to evade detection. By hiding malicious activity within Cloudflare traffic, often whitelisted by enterprise defences, this campaign significantly complicates detection and response.

ATTACK TYPE	Malware	SECTOR	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retailer and Distributor, Telecommunications
REGION	Global	APPLICATION	Microsoft Edge, Microsoft Outlook, Python, Windows, PowerShell

Source - https://www.trendmicro.com/en_us/research/26/a/analyzing-a-a-multi-stage-asyncrat-campaign-via-mdr.html

PLUGGYAPE backdoor targets defence personnel via messenger social engineering

Between October and December 2025, Ukraine’s CERT-UA, alongside the Armed Forces Cyber Incident Response Team, investigated a series of highly targeted cyberattacks against members of the Ukrainian Defence Forces. Adversaries used social engineering to impersonate charitable foundations on messaging platforms, distributing password-protected archives with deceptive extensions such as .docx, .pif, and .pdf.exe to deliver the Python-based PLUGGYAPE backdoor. Activity is attributed with medium confidence to Void Blizzard (UAC-0190).

Analysis of later campaign variants revealed enhanced technical sophistication, including MQTT support, anti-analysis routines, and indirect command-and-control discovery via public paste services such as Pastebin and rentry, encoded to evade detection. Investigators noted threat actors leveraged legitimate Ukrainian mobile numbers and local language communications to increase credibility. The evolution of PLUGGYAPE underscores persistently adaptive tactics against military targets amid the ongoing conflict.

ATTACK TYPE	Malware	**SECTOR**	Government, Military, Defence Industry
REGION	Ukraine	**APPLICATION**	Windows

Source - https://cert.gov.ua/article/6286942

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

All content is provided AS IS and for information purposes only. Tata Communications does not make any representations or warranties of any kind, including completeness, adequacy or accuracy of such information and disclaims all liability in connection with the use of this information. The information contained herein should not be construed as a substitute for professional advice.