TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: March 17, 2026

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

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

In this high-stakes environment, the Tata Communications Cyber Threat Intelligence report becomes indispensable. Published weekly, the report delivers 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 to protect critical operations globally before disruption.

TATA COMMUNICATIONS

Handala RedWanted uses cyber intrusions with open-source intelligence gathering

The Handala RedWanted platform represents a coordinated cyber-enabled influence operation attributed to Iran's Ministry of Intelligence and Security (MOIS). Launched in October 2025, the portal systematically publishes dossiers on Israeli intelligence officers, military personnel and defence industry staff, combining breached datasets, open-source intelligence and alleged intercepts to expose personal identities and operational affiliations.

Beyond exposure campaigns, RedWanted introduces a bounty model that incentivises contributors to submit real-time location intelligence on listed individuals. Rewards reportedly reaching $50,000 signal an escalation from traditional hack-and-leak activity to hybrid psychological operations. Analysts note the approach converts stolen cyber data into intimidation campaigns capable of amplifying strategic pressure and potential physical threat risks.

ATTACK TYPE	Hacktivism, Cyberespionage	**SECTOR**	IT, Military, Aerospace, Defence Industry
REGION	Middle East, Israel	**APPLICATION**	Apple Mac OS, Windows, Linux

Source - https://falconfeeds.io/blogs/handala-redwanted-platform-the-convergence-of-doxxing-psychological-warfare-and-kinetic-threat-facilitation

TATA COMMUNICATIONS

Malicious GitHub project ShoeVista distributes a remote access trojan to developers

Security researchers have identified a sophisticated campaign linked to a North Korean state-sponsored APT group distributing the DEV#POPPER remote access trojan and OmniStealer infostealer via a weaponised GitHub repository named “ShoeVista.” Disguised as an eCommerce project, the repository contains obfuscated code that activates when developers clone and execute the application, initiating a covert multi-stage malware deployment chain.

The infection chain deploys a Node.js-based backdoor that retrieves additional payloads from remote infrastructure and even blockchain transaction data before establishing command-and-control communication. Once active, the malware harvests environment variables, browser data, cryptocurrency wallets, API keys and developer credentials across macOS, Windows and Linux systems, highlighting the growing risk of supply-chain compromise through malicious open-source repositories.

ATTACK TYPE	Supply Chain	**SECTOR**	Waste disposal, Energy, Software Development, Cryptocurrency
REGION	Global	**APPLICATION**	Apple Mac OS, Microsoft Edge, Mozilla Firefox, Opera Browser, Windows, Linux, VS Code, Google Chrome, GitHub, Discord

Source - https://www.esentire.com/blog/north-korean-apt-malware-analysis-dev-popper-rat-and-omnistealer-everyday-im-shufflin

TATA COMMUNICATIONS

MuddyWater leverages RDP access and DLL Side-Loading for malware installation

Researchers identified an intrusion attributed to the Iranian-linked MuddyWater advanced persistent threat targeting an Israeli organisation. The compromise began with unauthorised Remote Desktop Protocol access, after which the attacker conducted reconnaissance and established SSH reverse tunnels to maintain covert remote connectivity with external infrastructure while exploring the compromised environment.

The threat actor later deployed malware through DLL sideloading, executing the legitimate Fortemedia FMAPP.exe application to load a malicious FMAPP.dll that initiated command-and-control communication. Subsequent activity included system enumeration, verification of C2 connectivity, and persistence attempts via PowerShell sessions, indicating hands-on-keyboard intrusion before defenders detected and contained the operation.

ATTACK TYPE	Cyberespionage	**SECTOR**	IT, Government, Defence Industry
REGION	Israel	**APPLICATION**	Windows, OpenSSH, PowerShell

Source - https://www.huntress.com/blog/muddywater-attack-chain

TATA COMMUNICATIONS

Vibeware espionage leverages cloud services to conceal malicious command traffic

Recent research has linked a new cyber-espionage campaign to APT36, also known as Transparent Tribe, highlighting the group's shift toward AI-assisted malware development referred to as "Vibeware." This approach prioritises volume over sophistication, producing large numbers of disposable implants in niche languages such as Nim, Zig, Crystal, Rust and Go to evade traditional detection mechanisms.

Initial compromise typically begins with phishing emails containing weaponised LNK shortcut files that execute PowerShell loaders to retrieve additional payloads. These implants enable persistence, credential theft and data exfiltration while communicating with command-and-control infrastructure hosted on legitimate cloud services, including Slack, Discord, Google Sheets, Supabase and Firebase, helping malicious traffic blend into routine network activity.

ATTACK TYPE	Social engineering, Phishing, Malware, Cyberespionage, APT	**SECTOR**	Government, Military, Defence and Space Manufacturing
REGION	India, Afghanistan	**APPLICATION**	Microsoft Edge, Windows, Google Chrome, Google Drive, Slack, Discord

Source - https://businessinsights.bitdefender.com/apt36-nightmare-vibeware

TATA COMMUNICATIONS

Payload ransomware threat combines file encryption with exfiltration capabilities

Security monitoring has identified the emergence of Payload Ransomware, a Windows-focused threat that encrypts files using the ChaCha20 algorithm and appends the ".payload" extension to affected data. After execution, the malware deploys a ransom note instructing victims to initiate negotiations through an anonymised portal, warning that files will remain inaccessible without the attacker-provided decryption key.

The malware also employs a double-extortion strategy, combining file encryption with data theft to pressure victims into payment. Before encryption, it disables security controls, deletes shadow copies, clears event logs, and terminates backup services to hinder recovery. Observed campaigns have primarily targeted organisations in Mexico and Egypt, particularly within the real estate and retail sectors.

ATTACK TYPE	Ransomware	**SECTOR**	Real Estate, Retailer and Distributor
REGION	Egypt, Mexico	**APPLICATION**	Windows

Source - https://www.cyfirma.com/news/weekly-intelligence-report-05-march-2026/

TATA COMMUNICATIONS

State-backed Seedworm group compromises multiple sectors amid rising tensions

Iranian threat group Seedworm, also tracked as MuddyWater, Temp Zagros and Static Kitten, has maintained covert access to several U.S. networks since early February 2026, with activity persisting after recent U.S. and Israeli strikes on Iran. Investigations indicate suspicious intrusions affecting a U.S. bank, an airport, a defence-sector software supplier with operations in Israel, and multiple NGOs across North America.

Researchers also identified new malware used in the campaign, including a Deno-based backdoor dubbed Dindoor and a Python implant known as Fakeset. Both were digitally signed using certificates linked to earlier Seedworm activity. In one incident, attackers attempted to exfiltrate corporate backups via Rclone to a cloud storage bucket, highlighting ongoing espionage-oriented intrusion techniques commonly used by the group.

ATTACK TYPE	Cyberespionage	**SECTOR**	Education, Automobile, IT Services and Consulting, Software Development
REGION	Australia, Canada, Japan, UK, Belgium, Germany, Italy, New Zealand, United States	**APPLICATION**	Windows

Source - https://www.security.com/threat-intelligence/iran-cyber-threat-activity-us

TATA COMMUNICATIONS

UAT-9244 APT compromises telecom infrastructure using custom malware families

Threat activity attributed to UAT-9244, a China-linked advanced persistent threat actor associated with the FamousSparrow cluster, has targeted telecommunications providers across South America since 2024. Researchers report compromises affecting Windows, Linux and network edge devices through a toolkit of new malware implants designed to establish persistent access within critical communications infrastructure and enable long-term espionage operations.

The campaign deploys three malware families — TernDoor, PeerTime and BruteEntry — to expand and sustain intrusions. TernDoor, delivered through DLL side-loading, provides remote command execution and system manipulation, while the PeerTime backdoor uses BitTorrent-based peer-to-peer command-and-control. Meanwhile, BruteEntry converts compromised edge devices into scanning nodes targeting services such as SSH, PostgreSQL and Apache Tomcat.

ATTACK TYPE	Malware	**SECTOR**	Telecommunications
REGION	South America	**APPLICATION**	PostgreSQL, Windows, Linux, Apache Tomcat

Source - https://blog.talosintelligence.com/uat-9244/

TATA COMMUNICATIONS

RedAlert campaign distributes trojanised emergency notification app via SMS

Researchers have uncovered the RedAlert mobile spyware campaign distributing a trojanised version of Israel's official Home Front Command "Red Alert" emergency alert application via SMS phishing messages. The malicious link prompts users to sideload an Android APK outside official stores, closely replicating the legitimate interface while covertly harvesting SMS messages, contact lists, call logs, and precise GPS location data from infected devices.

Technical analysis indicates the malware employs advanced evasion techniques, including signature spoofing, reflection-based cloaking, and dynamic payload loading to bypass Android security controls. The multi-stage infection chain executes obfuscated DEX payloads that continuously exfiltrate harvested data through HTTP POST requests to attacker-controlled infrastructure, enabling surveillance, location tracking, and potential interception of SMS-based two-factor authentication.

ATTACK TYPE	Malware	**SECTOR**	Government, Defence Industry
REGION	Middle East, Israel	**APPLICATION**	Android

Source - https://www.cloudsek.com/blog/redalert-trojan-campaign-fake-emergency-alert-app-spread-via-sms-spoofing-israeli-home-front-command

TATA COMMUNICATIONS

Zerobot targets exploiting automation platform alongside traditional IoT devices

Security researchers have identified active exploitation of CVE-2025-7544 in Tenda AC1206 routers and CVE-2025-68613 in the n8n workflow automation platform as part of a Mirai-derived Zerobot campaign. Detected in January 2026 via global honeypot telemetry, attackers leveraged public proof-of-concept exploits to compromise exposed systems and deliver malware across internet-facing devices and automation services.

Once exploitation succeeds, the malware deploys a shell script that retrieves the zerobotv9 payload using utilities such as wget, curl, tftp and ftpget, with additional socket-based methods to ensure execution across multiple CPU architectures. The campaign's targeting of n8n—an enterprise workflow automation platform—signals a notable shift beyond traditional IoT devices toward enterprise integration and automation environments.

ATTACK TYPE	Vulnerability, Malware	**SECTOR**	IT Services and Consulting, Software Development
REGION	Global	**APPLICATION**	Tenda Router, n8n

Source - https://www.akamai.com/blog/security-research/zerobot-malware-targets-n8n-automation-platform

TATA COMMUNICATIONS

Mass VPN probing suggests attackers are preparing credential-compromising campaigns

Researchers have identified a large-scale reconnaissance campaign targeting SonicWall SonicOS infrastructure between 22 and 25 February 2026, recording 84,142 coordinated scanning sessions originating from 4,305 IP addresses across 20 autonomous systems. The activity largely focused on SSL VPN enumeration, with 92% of probes querying a single API endpoint to determine whether exposed VPN services were accessible.

Notably, approximately 32% of traffic was delivered via a commercial proxy network operating in short, controlled bursts, suggesting deliberate attempts to evade detection. While exploitation activity remained minimal, researchers assessed the reconnaissance as preparatory. SonicWall VPN access has previously enabled ransomware groups such as Akira and Fog to infiltrate corporate networks, indicating potential credential-based attacks may follow.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Tourism, BFSI, Manufacturing, IT, Government, Energy, Business, Aviation, Retailer and Distributor, Telecommunications
REGION	Global	**APPLICATION**	SonicWall SMA, SonicWall SRA (Secure Remote Access), SonicWall Firewall, SonicWall VPN Client

Source - https://securityonline.info/massive-sonicwall-reconnaissance-campaign-signals-imminent-ransomware-strikes/

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