TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: March 31, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As March 2026 draws to a close, the cyber threat landscape is escalating, 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 anticipatory intelligence across their architectures.

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

Trojanised packages distribute CanisterWorm across developer ecosystem platforms

Security researchers have identified a sophisticated supply chain attack spanning the Trivy and npm ecosystems, driven by the CanisterWorm malware. The campaign originated from a compromised publisher account, enabling attackers to distribute trojanised packages at scale. At least 29 npm packages were affected, embedding a covert backdoor designed to establish persistent access and evade conventional detection mechanisms.

The malware exhibits worm-like propagation, leveraging compromised credentials to autonomously publish infected versions of additional packages. Its command-and-control infrastructure utilises decentralised hosting, complicating takedown efforts and attribution. This incident reflects a broader escalation in software supply chain threats, where automated propagation and credential harvesting are increasingly used to amplify impact across developer environments and enterprise systems.

ATTACK TYPE	Malware, Supply Chain	**SECTOR**	IT
REGION	Global	**APPLICATION**	Apple Mac OS, Docker, Kubernetes, Windows, Linux, Microsoft Azure, Node Package Manager (npm), AWS, GitHub

Source - https://socket.dev/blog/canisterworm-npm-publisher-compromise-deploys-backdoor-across-29-packages

TATA COMMUNICATIONS

Messaging platform abused to deliver malware targeting dissidents and journalists

The FBI has issued a FLASH alert warning of cyber operations linked to Iran's Ministry of Intelligence and Security (MOIS), which are leveraging Telegram as command-and-control infrastructure to distribute malware globally. The campaign primarily targets dissidents, journalists, and opposition groups, enabling intelligence collection, data leaks, and reputational harm through covert surveillance and intrusion activities.

Threat actors employ sophisticated social engineering, impersonating trusted contacts, or technical support to deliver multi-stage malware disguised as legitimate applications. Once deployed, the malware establishes persistent access via Telegram-based bots, enabling remote control, screen capture, and data exfiltration. Linked to groups such as Handala Hack and Homeland Justice, the activity underpins broader espionage and influence operations.

ATTACK TYPE	Social engineering, Malware, Cyber espionage	**SECTOR**	Government, Journalism, Defence, Broadcast Media Production and Distribution
REGION	Global	**APPLICATION**	Windows, Telegram

Source - https://www.ibm.com/think/x-force/slopoly-start-ai-enhanced-ransomware-attacks

TATA COMMUNICATIONS

Hastalamuerte deploys Gentlemen ransomware via firewall flaws and EDR evasion

The Gentlemen ransomware group, operated by threat actor Hastalamuerte, emerged in mid-2025 following a split from the Qilin RaaS ecosystem, rapidly evolving into a structured affiliate-driven operation. Leveraging a large inventory of compromised FortiGate devices and exploiting CVE-2024-55591 authentication bypass vulnerabilities, the group gains initial access alongside brute-forced VPN credentials, enabling scalable intrusion pathways across global enterprise environments.

The group employs advanced tradecraft, including BYOVD techniques to disable endpoint protections at the kernel level, automated lateral movement via scripting frameworks, and AI-assisted tooling to optimise attack execution. Combined with double extortion tactics and cross-platform targeting, these capabilities enable high-impact campaigns, reflecting the broader shift towards professionalised, modular ransomware operations designed for scale, persistence, and operational efficiency.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Cisco Adaptive Security Appliance (ASA), Fortinet FortiClient SSL VPN, Oracle E-business Intelligence, VMware ESXi, Windows, SonicWall VPN Client, Veeam, FortiOS, FortiGate Firewall

Source - https://www.ic3.gov/CSA/2026/260320.pdf

TATA COMMUNICATIONS

Modular MaaS ACRStealer employs evasion methods to steal browser credentials

ACRStealer, a Malware-as-a-Service (MaaS) infostealer, is being actively deployed via HijackLoader, reflecting its evolution into a modular and widely accessible threat. Recent analysis shows it leverages low-level system calls and WoW64 transitions to evade user-mode monitoring, bypassing conventional API-based detection and reinforcing its stealth in modern endpoint environments.

Its infrastructure enables layered TCP/TLS command-and-control communication, adaptive transmission methods, and integration into gaming-centric infection chains. Distributed through malvertising and compromised download platforms, the malware targets credentials, cookies, and platform-specific tokens, while supporting secondary payload execution via PowerShell and process injection, underscoring a scalable and continuously refined data exfiltration ecosystem.

ATTACK TYPE	Malware	**SECTOR**	Gaming, Business
REGION	Germany, Mongolia, the United States	**APPLICATION**	Windows

Source - https://blog.gdatasoftware.com/2026/03/38385-acr-stealer-infrastructure

TATA COMMUNICATIONS

DarkSword zero-day iOS flaws exploited in commercial spyware campaigns

DarkSword is a sophisticated full-chain iOS exploit identified by Google's Threat Intelligence Group, leveraging multiple zero-day vulnerabilities to silently compromise devices and escalate privileges to full system access. Active since November 2025, it has been deployed by state-linked actors and commercial spyware vendors in targeted campaigns across Saudi Arabia, Turkey, Malaysia, and Ukraine, highlighting a growing convergence between nation-state and commercial surveillance ecosystems.

The framework operates through modular malware families — GHOSTBLADE, GHOSTKNIFE and GHOSTSABER — enabling capabilities ranging from credential harvesting and file enumeration to remote code execution and large-scale data exfiltration. Researchers note its "fileless" and rapid-execution design reduces forensic traces, accelerating intelligence collection. Although Apple has issued patches and blocked malicious domains, the continued exploitation of unpatched devices underscores persistent spyware proliferation risks.

ATTACK TYPE	Social engineering, Cyber espionage	**SECTOR**	Government
REGION	Malaysia, Saudi Arabia, Turkey, Ukraine	**APPLICATION**	Apple iOS, Apple Safari

Source - https://cloud.google.com/blog/topics/threat-intelligence/darksword-ios-exploit-chain

TATA COMMUNICATIONS

Cisco FMC zero-day exploited by Interlock operators before public disclosure

An ongoing Interlock ransomware campaign has been identified exploiting CVE-2026-20131 in Cisco Secure Firewall Management Center. The flaw, a critical remote code execution vulnerability caused by insecure de-serialisation, enables unauthenticated attackers to execute arbitrary Java code with root privileges on affected devices. Threat intelligence confirms exploitation began on 26 January 2026, significantly preceding Cisco's public disclosure.

Analysis of a misconfigured staging server exposed the group's full operational toolkit, revealing a highly coordinated, multi-stage intrusion chain. This included custom remote access trojans, reconnaissance scripts, proxy infrastructure and fileless web shells, alongside techniques supporting persistence and evasion. The campaign demonstrates a shift towards edge-device compromise and double-extortion tactics, with enterprise firewalls serving as initial access vectors.

ATTACK TYPE	Vulnerability, Ransomware	**SECTOR**	Healthcare, Manufacturing, Construction, Government, Education
REGION	Global	**APPLICATION**	Cisco Secure Firewall, Cisco FMC, Cisco Security Cloud Control (SCC) Firewall Management

Source - https://aws.amazon.com/blogs/security/amazon-threat-intelligence-teams-identify-interlock-ransomware-campaign-targeting-enterprise-firewalls/

TATA COMMUNICATIONS

NPM repository deploys Cipher infostealer disguised as a legitimate executor tool

Malicious packages discovered within the npm ecosystem were found distributing a Windows executable disguised as a “Solara” executor via external hosting links, evading initial antivirus detection due to low signature recognition. Subsequent behavioural analysis revealed anomalous execution patterns, prompting deeper inspection of the payload delivery chain and its staged deployment mechanisms.

Further investigation identified the payload as Cipher Infostealer, leveraging obfuscated JavaScript alongside Python-based components and Discord injection techniques to harvest sensitive data, including browser credentials and cryptocurrency wallets. The campaign underscores evolving supply chain threats, combining multi-stage execution, stealth persistence, and advanced evasion tactics targeting both developers and end users.

ATTACK TYPE	Cybercrime, Malware, Supply Chain	**SECTOR**	Software Development
REGION	Global	**APPLICATION**	Chromium, Python, Windows, Node Package Manager (npm), Discord

Source - https://research.jfrog.com/post/solara-cipher-npm/

TATA COMMUNICATIONS

Stored XSS attack enables GhostMail session hijacking and large-scale data theft

A targeted phishing campaign, dubbed Operation GhostMail, has exploited a stored cross-site scripting vulnerability (CVE-2025-66376) in Zimbra Collaboration Suite to compromise a Ukrainian government agency. Delivered via a socially engineered internship email, the attack embeds obfuscated JavaScript within the HTML body, executing automatically when viewed in a vulnerable webmail client, without requiring user interaction.

Once executed, the browser-based payload harvests credentials, session tokens, and two-factor authentication recovery codes, while enabling persistent access through app-specific passwords and API abuse. Data, including up to 90 days of mailbox content, is exfiltrated over DNS and HTTPS channels. The tradecraft and targeting align with tactics previously attributed to Russian state-sponsored APT28 activity.

ATTACK TYPE	Phishing, Malware, Cyber espionage, APT	**SECTOR**	Government
REGION	Ukraine	**APPLICATION**	Zimbra Collaboration

Source - https://www.seqrite.com/blog/operation-ghostmail-zimbra-xss-russian-apt-ukraine/

Threat actors deploy Warlock ransomware using tunnelling and driver abuse

Researchers have observed the Warlock ransomware group, also tracked as Water Manual, significantly refining its intrusion life cycle to enhance persistence, lateral movement, and defence evasion across enterprise environments. The campaign primarily targets unpatched, internet-facing Microsoft SharePoint servers, exploiting authentication and remote code execution flaws to gain initial access and deploy web shells for sustained footholds.

Post-compromise activity demonstrates a highly orchestrated attack chain, combining Cobalt Strike beacons, credential harvesting, and Active Directory abuse to achieve domain-wide control. Adversaries leverage multiple tunnelling tools, including Cloudflare and VS Code tunnels, while employing BYOVD techniques with vulnerable drivers to disable security controls. Data exfiltration via Rclone precedes ransomware deployment through Group Policy mechanisms.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Manufacturing, Government, Education
REGION	Russia, the UK, Germany, the United States	**APPLICATION**	Microsoft SharePoint Server, Windows, VS Code, PowerShell

Source - https://www.trendmicro.com/en_us/research/26/c/dissecting-a-warlock-attack.html

TATA COMMUNICATIONS

SearchStrike campaign exploits fake GitHub repositories for Node.js malware

CERT-In has identified an ongoing malware campaign, Operation SearchStrike, that specifically targets IT administrators and developers by impersonating widely trusted Microsoft and Sysinternals utilities. Threat actors leverage search engine optimisation techniques to elevate malicious GitHub repositories, creating a false sense of legitimacy and prompting users to download trojanised MSI installers disguised as genuine tools.

Once executed, these installers deploy Node.js-based malware designed to establish persistence within compromised environments and evade detection. The campaign's distinguishing feature lies in its use of Ethereum smart contracts to conceal command-and-control instructions, enabling covert communication and remote access while blending malicious traffic with legitimate blockchain activity, thereby complicating traditional security monitoring and response efforts.

ATTACK TYPE	Supply Chain	**SECTOR**	IT Services and Consulting
REGION	Global	**APPLICATION**	Microsoft Sysinternals, Windows, Node.js, GitHub

Source - CERT-In

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