TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: February 24, 2026

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

As we advance through February 2026, 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, 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 — protecting critical operations globally before disruption takes hold.

TATA COMMUNICATIONS

Cryptocurrency sector faces AI-driven phishing and credential harvesting campaign

Security researchers report that UNC1069, a financially motivated threat actor linked to North Korea, is targeting cryptocurrency and decentralised finance organisations through AI-enhanced social engineering. The campaign leverages compromised Telegram accounts and fake Zoom meetings to deliver malware on macOS and Windows systems. The group has shifted its focus towards Web3 firms and related financial services entities since at least 2023.

The intrusion chain deploys multiple malware families, including WAVESHAPER, HYPERCALL, SUGARLOADER, SILENCELIFT, DEEPBREATH and CHROMEPUSH, to establish persistence and exfiltrate sensitive data. These tools harvest credentials, browser cookies and messaging data, enabling cryptocurrency theft and supporting further identity-based social engineering campaigns. Researchers note the activity reflects a targeted data-harvesting strategy with dual financial and operational objectives.

ATTACK TYPE	Social engineering	**SECTOR**	IT, Financial services, Investment Management, Software Development, Cryptocurrency
REGION	Global	**APPLICATION**	Microsoft Edge, Windows, Zoom Meetings, Google Chrome, Telegram, Zoom

Source - https://cloud.google.com/blog/topics/threat-intelligence/unc1069-targets-cryptocurrency-ai-social-engineering/

Green Blood ransomware targets organisations with Golang-based malware

The Green Blood Group represents a technically mature ransomware operation, leveraging a Golang-based payload with ChaCha8 encryption optimised for high-throughput file processing. Its architecture supports parallelised encryption across multiple drives while fingerprinting infected systems to enable targeted ransom tracking. Analysts note the malware's structured key management and exclusion logic, indicating deliberate engineering to maximise operational stability while denying access to critical data.

Beyond encryption, the group employs multi-vector initial access techniques, including phishing, exploited vulnerabilities, compromised websites, and trojanised software, with a geographic focus on regions with less mature incident response capabilities. Pre-encryption data exfiltration underpins its double-extortion model, with claims of large-scale data theft reinforcing coercive leverage through Tor-based leak infrastructure and staged disclosure tactics designed to pressure victims into payment negotiations.

ATTACK TYPE	Ransomware	**SECTOR**	Manufacturing, Government, Business
REGION	Belgium, Colombia, Egypt, Senegal	**APPLICATION**	Windows

Source - https://redpiranha.net/news/threat-intelligence-report-february-3-february-9-2026

Storm-2603 exploits SmarterMail security flaws to stage Warlock ransomware

Security researchers have confirmed that the China-linked threat actor Storm-2603 is actively exploiting the SmarterTools SmarterMail vulnerability CVE-2026-23760 to prepare Warlock ransomware attacks. The flaw enables unauthenticated password resets, allowing adversaries to gain administrative control. Storm-2603 then chains this access with abuse of SmarterMail's Volume Mount feature to escalate privileges and execute arbitrary commands at the operating system level.

Following initial compromise, the attackers deploy legitimate tools such as Velociraptor via Windows Installer packages to establish persistence and command-and-control, blending malicious activity with routine administrative operations. Researchers also observed parallel probing for CVE-2026-24423, highlighting multi-vector targeting of internet-facing email servers. The campaign underscores the rapid weaponisation of newly disclosed vulnerabilities and the need for immediate patching and network isolation.

ATTACK TYPE	Vulnerability, Cyberespionage	**SECTOR**	IT, Business
REGION	Global	**APPLICATION**	Windows, SmarterTools SmarterMail

Source - https://reliaquest.com/blog/threat-spotlight-storm-2603-exploits-CVE-2026-23760-to-stage-warlock-ransomware/

INTRODUCTION
THREAT ACTOR UNC1069 EXPLOITS AI TO FACILITATE CRYPTO CREDENTIAL THEFT
NEW RANSOMWARE DEPLOYS PROFESSIONAL TOOLING FOR SYSTEMATIC DATA EXTORTION
SMARTERMAIL FLAWS EXPLOITED FOR AUTHENTICATION BYPASS AND MALWARE STAGING
ADVANCED MUDDLED LIBRA LEVERAGES VMWARE VIRTUALISATION INFRASTRUCTURE
RECRUITMENT FRAUD DEPLOYS REMOTE ACCESS TOOLS VIA OPEN-SOURCE PACKAGE
APPLICATION UPDATES WEAPONISED TO DELIVER CHRYSALIS BACKDOORS GLOBALLY
THREAT ACTORS EXPLOIT LANGUAGE MODELS FOR SOCIAL ENGINEERING ATTACKS
FAKE SOFTWARE SITES DELIVER MULTISTAGE LOADER WITH EVASION CAPABILITIES
CLICKFIX EXPLOITS FAKE REPOSITORIES TO DEPLOY MACOS STEALER MALWARE
ZERO-DAY VULNERABILITY IN CHROME CSS ENGINE UNDER ACTIVE EXPLOITATION

TATA COMMUNICATIONS

Muddled Libra abuses VMware vSphere for credential dumping and exfiltration

Researchers investigating a September 2025 intrusion uncovered a rogue virtual machine created by the Muddled Libra threat group after it compromised a VMware vSphere environment, providing rare forensic visibility into its tactics and tooling. Analysis showed the attackers rapidly established a beachhead, downloaded stolen certificates, created SSH tunnels for command-and-control, and performed Active Directory reconnaissance before probing sensitive Snowflake datasets for potential exfiltration paths.

The findings reinforce Muddled Libra's preference for living-off-the-land techniques, abusing legitimate services and administrative utilities rather than deploying overt malware, and pivoting laterally through compromised identities. Researchers observed attempts to exfiltrate Outlook data via S3 uploads and extensive browsing of internal VMware hosts, highlighting the continued criticality of identity compromise and cloud data repositories as attack surfaces.

ATTACK TYPE	Social engineering, Cyberespionage	**SECTOR**	BFSI, IT, Business, Hospitality, Retailer and Distributor, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Active Directory Services, Microsoft Outlook, VMware vSphere Server, Windows, Microsoft Office 365, Microsoft Azure

Source - https://unit42.paloaltonetworks.com/muddled-libra-ops-playbook/

Malicious Graphalgo packages distributed via npm and PyPI target developers

Researchers have identified a new branch of the Graphalgo fake recruitment campaign, attributed to a North Korea-linked threat actor and active since May 2025. The operation targets JavaScript and Python developers in the cryptocurrency ecosystem through fabricated job opportunities, GitHub coding assignments and malicious dependencies distributed via npm and PyPI, exploiting trust in open-source development workflows.

The campaign uses modular infrastructure, staged malware delivery and token-authenticated command-and-control channels to deploy a multi-language remote access trojan. This malware enables remote command execution, system persistence and reconnaissance of cryptocurrency wallets, underscoring the growing risk of supply-chain attacks that leverage social engineering and compromised package repositories to infiltrate developer environments.

ATTACK TYPE	Social engineering, Malware	**SECTOR**	IT, Software Development, Cryptocurrency
REGION	Global	**APPLICATION**	Python, Windows, Node Packager Manager (NPM), Python Package Index (PyPI, Github)

Source - https://www.reversinglabs.com/blog/fake-recruiter-campaign-crypto-devs

Lotus Blossom hijacks Notepad++ updates in trusted supply chain campaign

Security researchers disclosed that state-linked Lotus Blossom actors compromised the official Notepad++ hosting environment in 2025, intercepting update traffic and selectively redirecting victims to attacker-controlled servers. The campaign primarily affected government, telecoms and critical infrastructure organisations in Southeast Asia, with further activity observed in Europe, the US and South America, underscoring the software's strategic role for administrators and developers.

Investigators identified dual infection chains using malicious installers, including Lua-based script execution delivering Cobalt Strike beacons and DLL sideloading that deployed the Chrysalis backdoor with sophisticated evasion features. The attackers leveraged weaknesses in older update mechanisms to gain persistent access, signalling a shift towards stealthy intelligence collection via trusted software supply chains rather than overt disruption.

ATTACK TYPE	Vulnerability, Malware, Cyberespionage	**SECTOR**	BFSI, Manufacturing, IT, Government, Telecommunications, Software Development
REGION	Europe, United States, South Asia, East Asia	**APPLICATION**	Windows, Notepad ++

Source - https://unit42.paloaltonetworks.com/notepad-infrastructure-compromise/

HONESTCUE and COINBAIT abuse AI APIs for reconnaissance and attacks

Adversarial exploitation of artificial intelligence expanded across the cyber-attack lifecycle in late 2025, with actors using LLMs to accelerate reconnaissance, target profiling and highly tailored phishing campaigns. Attempts to extract proprietary model capabilities and clone reasoning processes were also observed, alongside growing interest in autonomous “agentic” systems. These activities improved attacker productivity rather than introducing fundamentally new offensive capabilities.

Threat actors further experimented with AI-integrated malware, including proof-of-concept tooling such as HONESTCUE, which leveraged generative AI APIs to dynamically generate malicious code and evade detection. Underground ecosystems increasingly relied on jailbroken models and commercial APIs to scale operations, signalling a maturing criminal marketplace. While no breakthrough techniques emerged, the trajectory suggests accelerating operational efficiency and evolving adversary tradecraft.

ATTACK TYPE	Social engineering, Phishing, Malware	**SECTOR**	Healthcare, BFSI, Manufacturing, IT, Government, Transportation, Education, Energy, Retailer and Distributor, Telecommunications, Cryptocurrency
REGION	Global	**APPLICATION**	Apple Mac OS, Windows, DISCORD

Source - https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use/

TATA COMMUNICATIONS

OysterLoader leverages steganography for covert payload distribution operations

OysterLoader, also known as Broomstick and CleanUp, is a sophisticated multi-stage C++ malware loader primarily distributed via spoofed websites impersonating legitimate IT tools such as PuTTY and WinSCP. Linked to Rhysida ransomware operations, it functions as an initial access vector to deploy follow-on payloads, including infostealers and ransomware, highlighting the growing industrialisation of malware delivery campaigns.

Security researchers note that OysterLoader employs layered obfuscation techniques, including staged shellcode, custom LZMA decompression, API hammering and steganographic payload delivery, to evade detection and complicate analysis. It also uses evolving command-and-control infrastructure with customised Base64 encoding and rotating endpoints, enabling resilient communications and persistence across compromised environments despite ongoing defensive efforts by security vendors.

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

Source - https://blog.sekoia.io/oysterloader-unmasked-the-multi-stage-evasion-loader/

Fake GitHub repositories distribute macOS infostealers through commands

Threat analysts reported an active ClickFix campaign using fake GitHub repositories impersonating well-known technology brands to lure users into executing malicious terminal commands. Victims are redirected through staged GitHub-themed pages that fingerprint devices, collect telemetry, and selectively deliver macOS payloads. The technique shifts execution decisions to users, creating a scalable initial-access vector for infostealer operations.

Analysis shows the campaign deploying MacSync and the newer SHub Stealer v2.0, which harvests credentials, browser artefacts, cryptocurrency wallets and sensitive files, with SHub adding persistence, remote command execution and encrypted beaconing. Researchers observed dynamic evasion, infrastructure rotation and campaign analytics, signalling a mature infostealer ecosystem expanding beyond developers towards broader enterprise data theft at scale and ongoing.

ATTACK TYPE	Malware	**SECTOR**	IT, Software Development, Cryptocurrency
REGION	Global	**APPLICATION**	Apple Mac OS, Chromium, GitHub

Source - https://securitylabs.datadoghq.com/articles/tech-impersonators-clickfix-and-macos-infostealers/

TATA COMMUNICATIONS

Chrome users urged to patch actively exploited CSS vulnerability immediately

Google has issued an emergency security update for Chrome to address CVE-2026-2441, a high-severity zero-day vulnerability in the browser's CSS engine that is being actively exploited in the wild. The flaw, caused by a use-after-free memory corruption issue, could allow attackers to execute arbitrary code via malicious webpages, significantly increasing enterprise endpoint risk.

The vulnerability affects Chrome on Windows, macOS and Linux, with patches released through the stable channel to mitigate exposure. Google confirmed exploitation activity and urged users to update immediately to supported versions, as the issue resides in a core rendering component used across modern websites. Organisations are advised to prioritise patch deployment and verify browser versions across all managed devices.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, BFSI, Manufacturing, IT, Government, Transportation, Education, Energy, Retailer and Distributor, Telecommunications
REGION	Global	**APPLICATION**	Google Chrome OS, Google Chrome

Source - https://securityonline.info/critical-alert-chrome-zero-day-cve-2026-2441-exploited-in-the-wild/

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