TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: February 3, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As 2026 gets underway, the cyber threat landscape is expanding, shaped by increasingly sophisticated and persistent hostile activity observed throughout 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.

TATA COMMUNICATIONS

Deceptive MonetaStealer malware targets macOS while posing as Windows file

Security researchers have identified MonetaStealer, a newly emerging macOS information-stealing threat that's disguised as a Windows executable to mislead users. Detected on 6 January 2026, the PyInstaller-compiled Mach-O binary unpacks a concealed Python payload that evades basic scanners and maintains a zero-detection rate on VirusTotal. Early code analysis suggests heavy reliance on AI-generated logic and limited maturity.

Once executed on macOS, MonetaStealer actively harvests high-value data, including Chrome passwords, cookies, history, cryptocurrency wallets, Wi-Fi credentials, SSH keys, clipboard contents, and financial documents, staging results locally before exfiltrating via a Telegram bot infrastructure. It lacks persistence and anti-analysis safeguards, indicating rapid development, but its comprehensive targeting of sensitive assets highlights an urgent need for vigilant threat monitoring and defensive controls.

ATTACK TYPE	Malware	**SECTOR**	Financial services, Cryptocurrency
REGION	Global	**APPLICATION**	Apple Mac OS, Google Chrome OS, Google Chrome

Source - https://the-sequence.com/monetastealer-threat

INTRODUCTION | EARLY-STAGE MACOS MONETASTEALER DISGUISED AS WINDOWS EXECUTABLE | AKIRA TARGETS VPN CREDENTIALS AND VIRTUAL INFRASTRUCTURE GLOBALLY | SOCIAL ENGINEERING CAMPAIGN DELIVERS RANSOMWARE AND RAT | DUPEHIKE CAMPAIGN LEVERAGES POWERSHELL TO DEPLOY CUSTOM MALWARE | DEVELOPER-FOCUSED CAMPAIGN EXPLOITS VISUAL STUDIO CODE FOR INITIAL ACCESS | CRYPTOMINING MALWARE DISTRIBUTED VIA FAKE PYTHON LIBRARY ON PYPI | ATTACKERS HIJACK LEGITIMATE CODE LINTING TOOLS TO DISTRIBUTE MULTISTAGE MALWARE | EVELYN STEALER CAMPAIGN WEAPONISE VISUAL STUDIO CODE EXTENSIONS | MALICIOUS EXTENSIONS TARGET HR AND ERP PLATFORMS FOR CREDENTIAL THEFT | APT OPERATORS ABUSE ADVERTISING CLICK INFRASTRUCTURE TO DISTRIBUTE MALWARE

TATA COMMUNICATIONS

Akira RaaS operators exploit VPN weaknesses for multisystem extortion campaigns

Akira continues to rank among the most active ransomware-as-a-service (RaaS) groups, responsible for approximately 14.8 per cent of reported global incidents in mid-January 2026 and trailing only Qilin in prevalence. Emerging in March 2023, the group's double-extortion campaigns have driven sustained high-volume victimisation across sectors, with lifetime ransom proceeds now exceeding US $244 million and ongoing leak-site disclosures.

Analysis shows that Akira's operations leverage compromised VPN credentials and exploited vulnerabilities, enabling access to Windows, Linux, ESXi, and Nutanix AHV environments. Believed to include former Conti affiliates, the group's mature tradecraft adapts rapidly, exploiting edge-device flaws such as SonicWall SSL-VPN weaknesses to expand impact. Recent activity includes posting 15 + new victims on its Tor-based leak site.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Construction, Government, Education, Energy, Business, Retailer and Distributor
REGION	Global	**APPLICATION**	Cisco Adaptive Security Appliance (ASA), VMWare ESXi, Windows, Linux, Fortinet VPN, Veeam

Source - https://redpiranha.net/news/threat-intelligence-report-january-13-january-19-2026

TATA COMMUNICATIONS

Remote access tool deployed via social engineering leads to ransomware infection

Sicarii, an emergent Ransomware-as-a-Service (RaaS) operation first observed in late 2025, has drawn attention for its unusual ideological branding. Unlike typical financially motivated ransomware groups, Sicarii openly incorporates Israeli and Jewish symbols in its identity. However, most underground communications occur in fluent Russian, while Hebrew content appears non-native, indicating performative signalling rather than credible ideological alignment.

Technical analysis shows Sicarii's malware includes functional ransomware features such as AES-GCM encryption, extensive data exfiltration, and exploitation attempts against exposed services, including Fortinet vulnerabilities such as CVE-2025-64446. The operation also uses geo-fencing to avoid Israeli systems and exhibits early-stage tradecraft with centralised control and inconsistent victim narratives, suggesting experimentation over maturity within the broader ransomware ecosystem.

ATTACK TYPE	Social engineering, Ransomware, Malware	**SECTOR**	Financial services, Business
REGION	Russia	**APPLICATION**	Microsoft Windows Defender, Windows, PowerShell

Source - https://www.fortinet.com/blog/threat-research/inside-a-multi-stage-windows-malware-campaign

TATA COMMUNICATIONS

Spear-phishing operation deploys custom loader to establish C2 communications

Operation DupeHike (tracked as UNG0902) is an active cyber-espionage campaign targeting Russian corporate HR, payroll, and administrative staff via spear-phishing ZIP attachments named to mimic employee bonus documents. Malicious LNK files launch PowerShell in hidden mode to fetch a bespoke C++ loader dubbed DUPERUNNER, which conducts process enumeration and thread injection to deploy the in-memory AdaptixC2 beacon.

Once executed, the AdaptixC2 beacon establishes encrypted HTTP-based command-and-control communications with attacker infrastructure, enabling remote commands and potential data exfiltration. DupeHike operators leverage realistic bonus policy decoys tied to Russian corporate workflows to evade defences, illustrating elevated tactics and bespoke tooling. Cybersecurity specialists warn that this multi-stage attack underscores the need for heightened phishing vigilance and defensive controls.

ATTACK TYPE	Social engineering, Phishing, Cyberespionage	**SECTOR**	BFSI, Business, IT Services and Consulting, Staffing and Recruiting
REGION	Russia	**APPLICATION**	Windows

Source - https://www.seqrite.com/blog/operation-dupehike-ung0902-targets-russian-employees-with-duperunner-and-adaptixc2/

TATA COMMUNICATIONS

Visual Studio Code exploited in evolved social engineering recruitment campaign

Researchers have identified a refined phase of the DPRK-linked “Contagious Interview” campaign that weaponises Microsoft Visual Studio Code to deliver malware via trusted workflows. Attackers lure victims with trojanised GitHub and GitLab repositories, which trigger malicious tasks.json execution once the IDE trust prompt is accepted, fetching obfuscated JavaScript from remote infrastructure. This technique embeds a persistent backdoor, enabling remote execution and continuous command-and-control beaconing.

Threat analysis shows this evolution targets developer environments by abusing legitimate Visual Studio Code configuration files to execute Node.js payloads that persist beyond IDE closure. The backdoor harvests host identifiers, maintains frequent C2 communication, and dynamically executes attacker instructions. Security teams are urged to validate third-party repositories rigorously and tighten trust settings to mitigate these advanced supply-chain-style attacks.

ATTACK TYPE	Malware	**SECTOR**	IT, Software Development
REGION	Global	**APPLICATION**	Apple Mac OS, Microsoft Visual Studio, Windows, VS Code, Node.js

Source - https://www.jamf.com/blog/threat-actors-expand-abuse-of-visual-studio-code/

TATA COMMUNICATIONS

PyPI supply chain attack delivers cryptominer through fake library package

Security researchers have identified a malicious PyPI package, sympy-dev, impersonating the widely used SymPy library to distribute cryptomining malware. Published on 17 January 2026 under multiple versions (1.2.3–1.2.6), the deceptive package mirrored SymPy's branding and description to increase accidental installs and surpassed 1,000 downloads in its first day, signalling rapid exposure in development and CI environments.

Analysis shows each release embeds a concealed Python loader that fetches and executes Linux ELF payloads directly in memory using Linux memfd_create and /proc/self/fd, reducing on-disk artefacts. Once triggered, this mechanism retrieves XMRig cryptomining binaries from attacker-controlled infrastructure, turning compromised developer machines and systems into covert miners. The package remained live on PyPI as researchers petitioned for its removal.

ATTACK TYPE	Malware, Supply Chain	**SECTOR**	Education, IT Services and Consulting, Software Development
REGION	Global	**APPLICATION**	Python

Source - https://socket.dev/blog/pypi-package-impersonates-sympy-to-deliver-cryptomining-malware?utm_medium=feed

TATA COMMUNICATIONS

Compromised NPM packages deliver Scavenger malware to developer workstations

A recent supply chain attack hijacked popular npm linter packages, most notably eslint-config-prettier, following a targeted device-code phishing campaign that compromised a maintainer's npm credentials. Unauthorised malicious versions were also published directly to the npm registry without any corresponding GitHub commits, exposing thousands of dependent projects and magnifying risk across the JavaScript ecosystem. Analysts also warn of upstream software supply chain dangers.

Technical analysis reveals the tainted installers include a Windows-only DLL loader invoked via rundll32.exe that deploys Scavenger malware. This payload uses layered anti-analysis methods and encrypted command-and-control traffic before delivering a second-stage infostealer targeting Chromium data and other artefacts on infected machines. Developers are urged to audit dependencies and strengthen credential and supply chain defences immediately.

ATTACK TYPE	Malware, Supply Chain	**SECTOR**	IT, Software Development
REGION	Global	**APPLICATION**	Chromium, Windows, Node Packager Manager (NPM)

Source - https://c-b.io/Install+Linters%2C+Get+Malware+-+DevSecOps+Speedrun+Edition

TATA COMMUNICATIONS

Evelyn Stealer targets developers through weaponised code editor extensions

The Evelyn Stealer campaign weaponises Visual Studio Code extensions to target software developers, delivering a sophisticated multistage information-stealer via trusted development tooling. Installation of trojanised extensions drops a malicious Lightshot DLL, which sideloads and launches hidden payloads before injecting the Evelyn Stealer into legitimate Windows processes. Once active, it harvests credentials, browser and system data, and cryptocurrency wallets.

Research shows that the Evelyn Stealer demonstrates advanced evasion techniques, including encrypted payload stages and process hollowing, allowing attackers to blend into developer workflows and evade detection. Stolen data is compressed and exfiltrated via FTP to attacker-controlled infrastructure. The campaign underscores the rising abuse of developer ecosystems as attack vectors and the need for stringent extension vetting and endpoint security.

ATTACK TYPE	Malware, Supply Chain	**SECTOR**	IT Services and Consulting, Software Development, Cryptocurrency
REGION	Global	**APPLICATION**	Mozilla Firefox, VS Code

Source - https://www.trendmicro.com/en_us/research/26/a/analysis-of-the-evelyn-stealer-campaign.html

TATA COMMUNICATIONS

Fake productivity extensions enable widespread enterprise platform session theft

Researchers have uncovered a coordinated campaign of five malicious Chrome extensions targeting enterprise HR and ERP platforms, including Workday, NetSuite, and SuccessFactors. Disguised as productivity or security tools, the extensions collectively steal authentication tokens, manipulate browser APIs, and obstruct incident-response interfaces to facilitate session hijacking. More than 2,300 users were impacted as the threat actors exploited cookie exfiltration, DOM manipulation, and token injection techniques.

Threat research indicates four extensions were published under the name databycloud1104 and one under softwareaccess, yet all share identical infrastructure and code patterns, suggesting a single coordinated operation. Key variants block access to administrative security controls and implement bidirectional cookie injection for full account takeover without credentials. The campaign remains under investigation, and takedown requests have been submitted to Google.

ATTACK TYPE	Malware	**SECTOR**	Business, IT Services and Consulting, Retailer and Distributor
REGION	Global	**APPLICATION**	Google Chrome OS, SAP Enterprise Resource Planning (ERP), Google Chrome

Source - https://socket.dev/blog/5-malicious-chrome-extensions-enable-session-hijacking

TATA COMMUNICATIONS

Konni threat group deploys EndRAT using advertising redirection social engineering

Operation Poseidon, attributed to the North Korea-linked Konni APT, exploits Google and Naver advertising infrastructures to deliver the EndRAT malware via spear-phishing, masking malicious redirection URLs as legitimate adverts. Malicious ZIP attachments contain LNK shortcuts and trigger AutoIt scripts disguised as PDFs, loading malware in memory. Security experts warn that this methodology underscores advanced evasion, camouflage, and reuse of established infrastructure.

Research and allied analysts note that Poseidon's sophistication includes hidden padding in phishing emails to defeat AI-based filters and compromised WordPress hosts serving payloads. The campaign reflects an evolution in Konni's tactics and expanded targeting beyond traditional sectors, aiming for deeper, persistent access. Organisations are therefore urged to strengthen phishing defences and closely monitor such deceptive ad-linked threats.

ATTACK TYPE	Malware, Cyberespionage	**SECTOR**	Financial services, Government
REGION	South Korea	**APPLICATION**	WordPress, Windows

Source - https://research.checkpoint.com/2026/konni-targets-developers-with-ai-malware/

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