TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: March 10, 2026

THREAT INTELLIGENCE ADVISORY REPORT

As we enter 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.

INTRODUCTION
THE GENTLEMEN CAMPAIGN COMBINES BYOVD AND FORTIGATE FOR DOUBLE EXTORTION
SINOBI THREAT ACTOR DEPLOYS RANSOMWARE WITH DOUBLE EXTORTION LEAK SITES
WORM MALWARE TARGETS NPM TO COMPROMISE CI PIPELINES AND WORKFLOWS
ANDROID TROJAN SURXRAT INTEGRATING LARGE AI MODULES AS MAAS
MULTISTAGE ATTACK USES EXAM LURES TO INSTALL SURVEILLANCE AND EXFILTRATION TOOLS
SAFEPAY OPERATORS CONDUCT SYSTEMATIC ENTERPRISE INTRUSIONS FOR DATA THEFT
REGIONAL CYBER ACTIVITY INTENSIFIES WITH COORDINATED HACKTIVIST MOBILISATION
AURASTEALER MALWARE USES CLOUDFLARE INFRASTRUCTURE FOR OPERATIONAL SECURITY
SUPPLY CHAIN COMPROMISED WITH STEGABIN CREDENTIAL THEFT MALWARE VIA NPM
NEW RAT LOWERS BARRIERS FOR ENTERPRISE-TARGETED DOUBLE EXTORTION CAMPAIGNS

Gentlemen ransomware uses network exploitation with data theft for access

The Gentlemen ransomware operation, first identified in mid-2025, employs a double extortion strategy to maximise leverage against victims by both encrypting systems and exfiltrating sensitive data. The threat actor exploits internet-facing services, notably FortiGate firewall admin panels and VPN interfaces, often leveraging compromised administrative credentials to gain initial access into enterprise environments. Its Tor-based data leak site enhances negotiation pressure.

Post-compromise activity by The Gentlemen is highly methodical, with systematic Active Directory reconnaissance and lateral movement using legitimate administrative tools such as PsExec, PuTTY and RDP. Defence evasion techniques include BYOVD-style loading of vulnerable drivers and disabling of security agents. Before deploying cross-platform ransomware, the group stages data collection and secure exfiltration over encrypted channels to support its extortion model.

ATTACK TYPE	Ransomware	SECTOR	IT, Healthcare, BFSI, Legal, Manufacturing, Construction, Transportation, Education, Energy, Business, Real Estate, Hospitality, Retailer and Distributor
REGION	Australia, Canada, India, Japan, UK, Brazil, France, Mexico, South Africa, Thailand, Turkey, UAE, United States	APPLICATION	VMware ESXi, Windows, Linux, FortiGate Firewall

Source - https://redpiranha.net/news/threat-intelligence-report-february-10-february-16-2026

INTRODUCTION | THE GENTLEMEN CAMPAIGN COMBINES BYOVD AND FORTIGATE FOR DOUBLE EXTORTION | SINOBI THREAT ACTOR DEPLOYS RANSOMWARE WITH DOUBLE EXTORTION LEAK SITES | WORM MALWARE TARGETS NPM TO COMPROMISE CI PIPELINES AND WORKFLOWS | ANDROID TROJAN SURXRAT INTEGRATING LARGE AI MODULES AS MAAS | MULTISTAGE ATTACK USES EXAM LURES TO INSTALL SURVEILLANCE AND EXFILTRATION TOOLS | SAFEPAY OPERATORS CONDUCT SYSTEMATIC ENTERPRISE INTRUSIONS FOR DATA THEFT | REGIONAL CYBER ACTIVITY INTENSIFIES WITH COORDINATED HACKTIVIST MOBILISATION | AURASTEALER MALWARE USES CLOUDFLARE INFRASTRUCTURE FOR OPERATIONAL SECURITY | SUPPLY CHAIN COMPROMISED WITH STEGABIN CREDENTIAL THEFT MALWARE VIA NPM | NEW RAT LOWERS BARRIERS FOR ENTERPRISE-TARGETED DOUBLE EXTORTION CAMPAIGNS

Sinobi ransomware leverages credential abuse and data exfiltration techniques

Sinobi is a Ransomware-as-a-Service (RaaS) group that surfaced in mid-2025, widely assessed as a rebrand or successor of the Lynx and INC ransomware families due to notable code overlaps and shared tooling. The operation uses compromised credentials, VPN/RDP access, and public-facing vulnerability exploits to infiltrate networks, escalate privileges and evade defences before executing data exfiltration and encryption.

Once inside, Sinobi affiliates stage sensitive data exfiltration using legitimate utilities such as Rclone, then deploy high-speed encryption across systems. Victims receive ransom notes with Tor-hosted leak-site links as part of a double extortion strategy, threatening publication unless payment demands are met. Medium-to-large organisations in manufacturing, healthcare, financial services and education are frequently targeted.

ATTACK TYPE	Ransomware	SECTOR	Healthcare, BFSI, Manufacturing, Education
REGION	Australia, Canada, UK, United States	APPLICATION	Windows, SonicWall

Source - https://socradar.io/blog/dark-web-profile-sinobi-ransomware/

Shai-Hulud-like worm malware spreads via npm typosquatting to inject backdoors

Researchers have identified SANDWORM_MODE, an active npm supply-chain worm spreading through typosquatted packages and a weaponised GitHub Action. The campaign infects developer environments and CI pipelines, harvesting credentials such as npm tokens, SSH keys and environment variables while injecting malicious workflows into repositories to enable automated lateral propagation across the software ecosystem.

The malware demonstrates an emerging tactic of targeting AI-assisted development environments. It deploys a rogue MCP server that integrates with coding assistants, enabling prompt injection and covert extraction of LLM API keys and other secrets. Data exfiltration occurs via HTTPS endpoints, GitHub APIs and DNS tunnelling, allowing attackers to sustain large-scale compromise across repositories and software supply chains.

ATTACK TYPE	Malware, Supply Chain	SECTOR	IT and Software Development
REGION	Global	APPLICATION	VS Code, Node Packager Manager (NPM), GitHub

Source - https://socket.dev/blog/sandworm-mode-npm-worm-ai-toolchain-poisoning?utm_medium=feed

INTRODUCTION | THE GENTLEMEN CAMPAIGN COMBINES BYOVD AND FORTIGATE FOR DOUBLE EXTORTION | SINOBI THREAT ACTOR DEPLOYS RANSOMWARE WITH DOUBLE EXTORTION LEAK SITES | WORM MALWARE TARGETS NPM TO COMPROMISE CI PIPELINES AND WORKFLOWS | ANDROID TROJAN SURXRAT INTEGRATING LARGE AI MODULES AS MAAS | MULTISTAGE ATTACK USES EXAM LURES TO INSTALL SURVEILLANCE AND EXFILTRATION TOOLS | SAFEPAY OPERATORS CONDUCT SYSTEMATIC ENTERPRISE INTRUSIONS FOR DATA THEFT | REGIONAL CYBER ACTIVITY INTENSIFIES WITH COORDINATED HACKTIVIST MOBILISATION | AURASTEALER MALWARE USES CLOUDFLARE INFRASTRUCTURE FOR OPERATIONAL SECURITY | SUPPLY CHAIN COMPROMISED WITH STEGABIN CREDENTIAL THEFT MALWARE VIA NPM | NEW RAT LOWERS BARRIERS FOR ENTERPRISE-TARGETED DOUBLE EXTORTION CAMPAIGNS

MaaS platform deploys Android SURXRAT with LLM module for experiments

SURXRAT is an evolving Android Remote Access Trojan distributed through a Telegram-based malware-as-a-service ecosystem under the SURXRAT V5 branding. Derived from ArsinkRAT code, it enables affiliates to generate customised malware builds while operators maintain central infrastructure. The malware supports extensive surveillance and remote-control functions, harvesting SMS messages, contacts, call logs, device details and other sensitive information for fraud and espionage activities.

Recent variants also demonstrate experimental capabilities, including the conditional download of a large language model exceeding 23 GB from public repositories such as Hugging Face. Researchers believe this unusual feature may enable AI-assisted automation, performance degradation to mask malicious activity, or new monetisation models. Combined with Firebase-based command-and-control and ransomware-style screen locking, SURXRAT reflects growing sophistication in Android malware ecosystems.

ATTACK TYPE	Malware, Mobile	SECTOR	BFSI
REGION	Europe	APPLICATION	Android

Source - https://cyble.com/blog/surxrat-downloads-large-llm-module-from-hugging-face/

APT36 campaign delivers stealth RAT using exam-themed phishing documents

Threat analysts have uncovered a targeted cyber espionage campaign attributed to Transparent Tribe (APT36), which distributes a malicious ZIP archive disguised as examination documents to lure victims. The archive delivers a deceptive LNK shortcut and a macro-enabled PowerPoint add-in that initiate a staged infection chain using hidden directories, batch scripts and macro-based payload reconstruction.

Once executed, the malware establishes persistence through registry modifications and hard links while communicating with command-and-control infrastructure via direct TCP channels. The operation ultimately deploys a .NET-based remote access trojan enabling surveillance, system discovery and data exfiltration. Researchers note the campaign reflects Transparent Tribe’s evolving tradecraft targeting the Indian government and strategic entities for intelligence collection.

ATTACK TYPE	Malware, Cyberespionage, APT	SECTOR	Government, Defence Industry
REGION	India	APPLICATION	Microsoft PowerPoint, Windows

Source - https://www.cyfirma.com/research/apt36-multi-vector-execution-malware-campaign-targeting-indian-government-entities/

SafePay deploys advanced encryption following extensive network reconnaissance

Researchers have identified SafePay ransomware, a centralised double-extortion operation active since late 2024 and increasingly targeting enterprises across regions, including the United States, Germany, the United Kingdom, Japan, and Australia. Unlike ransomware-as-a-service models, the group operates through a tightly controlled infrastructure, enabling consistent tactics and rapid execution while maintaining strict control over negotiations and ransom operations.

Initial access is commonly achieved through exposed VPN gateways, RDP services or other remote entry points using compromised credentials. After gaining access, operators conduct network discovery, move laterally and exfiltrate sensitive data before deploying a DLL-based encryptor that uses ChaCha20 and X25519 cryptography, appending ".safepay" extensions while disabling recovery mechanisms.

ATTACK TYPE	Ransomware	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.cyfirma.com/news/weekly-intelligence-report-27-february-2026/

INTRODUCTION | THE GENTLEMEN CAMPAIGN COMBINES BYOVD AND FORTIGATE FOR DOUBLE EXTORTION | SINOBI THREAT ACTOR DEPLOYS RANSOMWARE WITH DOUBLE EXTORTION LEAK SITES | WORM MALWARE TARGETS NPM TO COMPROMISE CI PIPELINES AND WORKFLOWS | ANDROID TROJAN SURXRAT INTEGRATING LARGE AI MODULES AS MAAS | MULTISTAGE ATTACK USES EXAM LURES TO INSTALL SURVEILLANCE AND EXFILTRATION TOOLS | SAFEPAY OPERATORS CONDUCT SYSTEMATIC ENTERPRISE INTRUSIONS FOR DATA THEFT | REGIONAL CYBER ACTIVITY INTENSIFIES WITH COORDINATED HACKTIVIST MOBILISATION | AURASTEALER MALWARE USES CLOUDFLARE INFRASTRUCTURE FOR OPERATIONAL SECURITY | SUPPLY CHAIN COMPROMISED WITH STEGABIN CREDENTIAL THEFT MALWARE VIA NPM | NEW RAT LOWERS BARRIERS FOR ENTERPRISE-TARGETED DOUBLE EXTORTION CAMPAIGNS

Ideologically motivated hacktivist activity surges amid regional military tensions

Amid escalating military tensions between Iran, Israel and the United States under Operation Epic Fury, cyber operations have intensified alongside kinetic activity, fuelling a surge in ideologically driven hacktivism across the Middle East. Analysts report that dozens of groups rapidly mobilised online, launching distributed denial-of-service attacks, website defacements and coordinated propaganda campaigns targeting countries perceived as supporting Israeli or U.S. actions.

Most active collectives currently promote pro-Iran or pro-Palestine narratives, focusing attacks on government institutions, financial services, telecommunications providers and energy infrastructure across the region. Although many claims remain unverified and largely disruption-oriented, the scale of coordinated messaging and targeting of critical sectors highlights growing geopolitical cyber risk and the potential for escalation beyond regional networks.

NOTE: The CTI Team has not independently verified all attack claims

ATTACK TYPE	Hacktivism, DDoS	SECTOR	Healthcare, BFSI, IT, Government, Transportation, Education, Energy, Aviation, Automobile, Broadcast Media, Telecommunications, Logistics, Social Media
REGION	Middle East, Asia, Bahrain, Iran, Iraq, Israel, Jordan, Kuwait, Qatar, UAE, United States, Dubai	APPLICATION	Apple Mac OS, Windows, Linux, Generic

Source - CTI Team Internal Research

Emerging AuraStealer employs Cloudflare protection and anti-analysis methods

Following the 2025 disruption of the Lumma Stealer infrastructure, the infostealer ecosystem has shifted as threat actors seek new malware-as-a-service (MaaS) alternatives. One emerging contender is AuraStealer, first advertised on Russian-language cybercrime forums in July 2025. Marketed as a Lumma successor, it targets browser data, cryptocurrency wallets and two-factor authentication tokens, reflecting growing criminal demand for credential-harvesting tools.

AuraStealer employs Cloudflare-fronted command-and-control infrastructure, AES-encrypted communications and process injection techniques designed to bypass security controls such as Anti-Browser Exploitation (ABE). Analysts have identified dozens of shifting C2 domains alongside extensive anti-analysis and debugging evasion mechanisms. Recent campaigns distribute the malware through TikTok-based ClickFix chains, where users are tricked into executing malicious PowerShell commands that deploy the infostealer.

ATTACK TYPE	Social engineering, Malware	SECTOR	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retailer and Distributor, Telecommunications
REGION	Global	APPLICATION	Chromium, OpenVPN, Windows, Telegram, Discord

Source - https://www.intrinsec.com/wp-content/uploads/2026/02/TLP-CLEAR-AuraStealer-EN.pdf

StegaBin attack deploys an infostealer hidden via Pastebin steganographic methods

Cybersecurity researchers have uncovered a coordinated supply-chain campaign involving 26 malicious npm packages distributing a multi-stage credential-stealing framework known as StegaBin. The packages execute hidden install scripts that retrieve staged payloads and deploy a nine-module infostealer and remote access trojan designed to harvest sensitive data from developer workstations and development environments.

The malware employs steganography-based “dead-drop” resolvers hosted on Pastebin to conceal command-and-control infrastructure, dynamically decoding attacker domains before retrieving payloads from Vercel-hosted servers. Once deployed, the toolkit targets VSCode configurations, Git repositories, SSH keys, browser credentials and cryptocurrency wallets, reflecting tradecraft associated with the FAMOUS CHOLLIMA cluster linked to Lazarus Group operations.

ATTACK TYPE	Supply Chain	SECTOR	IT Services and Consulting, Software Development, Cryptocurrency
REGION	Global	APPLICATION	Apple Mac OS, Microsoft Edge, Mozilla Firefox, Windows, Linux, VS Code, Google Chrome, Node Packager Manager (NPM)

Source - https://socket.dev/blog/stegabin-26-malicious-npm-packages-use-pastebin-steganography?utm_medium=feed

Steaelite RAT facilitates automated data exfiltration and encryption attacks

A newly identified remote access trojan, Steaelite, has been circulating across underground cybercrime forums since November 2025, marketed as a “fully undetectable” tool targeting Windows 10 and 11 systems. Delivered through a browser-based management panel, the malware enables attackers to conduct credential theft, live surveillance and remote command execution from a single interface.

Researchers note that Steaelite streamlines double-extortion operations by merging data exfiltration and ransomware deployment capabilities into one platform. Once a compromised device connects, the malware automatically harvests stored browser credentials, cookies and session tokens before operator interaction. This automation reduces technical barriers, enabling even lower-skilled actors to orchestrate enterprise-targeted ransomware campaigns more efficiently.

ATTACK TYPE	Malware	SECTOR	BFSI, IT Services and Consulting, Cryptocurrency
REGION	Global	APPLICATION	Microsoft Windows 10, Windows 11

Source - https://gbhackers.com/steaelite-rat/

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.