TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: February 17, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As we move through February 2026, the cyber threat landscape is intensifying, 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 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

Emerging Nova ransomware leverages Rust encryption safe mode evasion

Nova, formerly RALord, is an emerging ransomware-as-a-service (RaaS) group that rebranded in 2025 and has since expanded its global footprint, targeting sectors such as healthcare, education, IT services, media, construction, and agriculture. The group operates a double-extortion model – encrypting files while exfiltrating sensitive data – and publishes victim profiles on Tor-based leak portals to amplify extortion pressure.

Nova affiliates use credential theft, vulnerability exploitation, and AI-driven spear-phishing to gain initial access, then deploy Rust-based encryptors to evade detection and accelerate encryption across Windows, Linux, and virtualised environments. The group systematically disables security tools and destroys backups to inhibit recovery, underscoring the growing sophistication and operational maturity of commercialised ransomware ecosystems targeting enterprises worldwide.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Healthcare, Entertainment, Construction, Education, Hospitality
REGION	Europe, Canada, the UK, the US, APAC	**APPLICATION**	VMWare ESXi, Windows

Source - https://redpiranha.net/news/threat-intelligence-report-january-20-january-26-2026

TATA COMMUNICATIONS

WinRAR (CVE-2025-8088) path traversal flaw enables malware persistence

Widespread exploitation of CVE-2025-8088 highlights the persistent risk posed by unpatched software. The high-severity WinRAR path traversal vulnerability enables adversaries to drop malicious files into sensitive system directories, including the Windows Startup folder, ensuring persistence. Threat Intelligence group reports sustained abuse by state-sponsored actors and cybercriminals, with campaigns observed across defence, technology, and finance sectors.

Attackers commonly embed payloads within Alternate Data Streams (ADS) in seemingly benign archives, allowing malware to execute automatically after reboot. Observed payloads include espionage frameworks, remote access trojans, and credential-stealing tools, underscoring the vulnerability's dual exploitation – espionage and financial gain. Despite patches released in July 2025, continued exploitation reflects slow patch adoption and persistent user exposure.

ATTACK TYPE	Phishing, Malware	**SECTOR**	IT, Government, Military, BFSI, Defence and Space Manufacturing, Hospitality
REGION	Brazil, China, Indonesia, Ukraine	**APPLICATION**	Windows, Google Chrome, Telegram

Source - https://cloud.google.com/blog/topics/threat-intelligence/exploiting-critical-winrar-vulnerability/

Supply chain attack deploys Chrysalis backdoor via compromised updates

Investigators found the compromise stemmed from a hijacked Notepad++ update infrastructure, allowing attackers to selectively redirect update requests to malicious servers without altering the application's source code. Active between mid-2025 and December 2025, the campaign demonstrated precise supply chain targeting, suggesting an intelligence-driven operation targeting organisations strategically rather than infecting indiscriminately. The approach underscores systemic risks in trusted software distribution channels.

Technical analysis indicates Chrysalis provided remote command execution, file transfer, system enumeration, and stealthy persistence using encrypted command-and-control communications that mimicked legitimate traffic. The implant's design leveraged extensive obfuscation and trusted binary abuse to evade detection, highlighting evolving APT tradecraft. Researchers assessed Lotus Blossom ATP group as China-linked and active against government and critical infrastructure sectors across Asia and Central America.

ATTACK TYPE	Malware, Cyber espionage, Supply Chain	**SECTOR**	Government, Journalism, Aviation, Broadcast Media Production and Distribution, Defence and Space Manufacturing, Telecommunications
REGION	South Asia, Central America	**APPLICATION**	Windows, Notepad++

Source - https://www.rapid7.com/blog/post/tr-chrysalis-backdoor-dive-into-lotus-blossoms-toolkit/

TATA COMMUNICATIONS

Custom .NET Loader distributes malware using the RunPE mechanism worldwide

PhantomVAI is a highly obfuscated .NET loader observed in large-scale, global phishing operations, primarily delivering information stealers and remote-access trojans. Built on a modified RunPE utility known as Mandark, it injects payloads into Windows using process hollowing and virtual machine detection. Security researchers link its widespread use to multiple threat actors operating under a loader-as-a-service (LaaS) model.

The loader typically masquerades as Microsoft.Win32.TaskScheduler.dll, abusing legitimate, open-source projects to evade detection and blend into enterprise environments. PhantomVAI campaigns deploy malware families such as Remcos, XWorm, AsyncRAT, DarkCloud, and SmokeLoader, often distributed via diverse phishing lures. Researchers note persistent evolution and increasing sample volume, indicating sustained criminal adoption across regions and sectors.

ATTACK TYPE	Malware	**SECTOR**	Government, Business
REGION	Europe, Canada, India, South Korea, the United States	**APPLICATION**	Windows

Source - https://www.intrinsec.com/wp-content/uploads/2026/01/TLP-CLEAR-20260130-PhantomVAI_Loader.pdf

TATA COMMUNICATIONS

Neusploit campaign deploys MiniDoor stealer via weaponised document exploit

In Operation Neusploit, researchers attributed a multi-stage intrusion campaign to Russia-linked APT28, which weaponised CVE-2026-21509 via crafted RTF files to target Central and Eastern Europe. The activity was observed in January 2026, with lures tailored in local languages and server-side filtering used to selectively deliver payloads to intended victims. Microsoft issued an out-of-band patch amid active exploitation.

Following exploitation, the attack chain deployed MiniDoor to exfiltrate Outlook emails and PixyNetLoader to establish persistence through COM hijacking and staged payload delivery. Threat actors embedded encrypted components within PNG files and leveraged Filen API-based command-and-control, while executing Covenant Grunt implants entirely in memory using CLR hosting. These techniques significantly reduced on-disk artefacts and detection opportunities.

ATTACK TYPE	Cyber espionage	**SECTOR**	Government
REGION	Romania, Slovakia, Ukraine	**APPLICATION**	Microsoft Outlook, Windows, Microsoft Office 365

Source - https://www.zscaler.com/blogs/security-research/apt28-leverages-cve-2026-21509-operation-neusploit

TATA COMMUNICATIONS

Cloud-native Arsink malware deploys surveillance across infected devices

Arsink is a cloud-native Android Remote Access Trojan that enables persistent surveillance and full device control, exploiting trusted cloud platforms to evade detection. Threat actors distribute malicious APKs disguised as legitimate or “premium” apps via Telegram, Discord, and file-sharing services, relying on social engineering rather than technical exploits. Once installed, the malware harvests sensitive data and maintains covert access at scale.

Researchers identified over 1,200 distinct Arsink samples and 317 command-and-control endpoints, with approximately 45,000 infected IP addresses across 143 countries. The campaign leverages Google Apps Script, Firebase, Google Drive, and Telegram for resilient command-and-control and data exfiltration, enabling rapid variant development and infrastructure rotation. This modular architecture underlines the campaign’s opportunistic nature and capacity for ongoing evolution.

ATTACK TYPE	Malware, Mobile	**SECTOR**	Telecommunications
REGION	Global	**APPLICATION**	Android

Source - https://zimperium.com/blog/the-rise-of-arsink-rat

TATA COMMUNICATIONS

Metro4Shell attacks compromise React Native development server infrastructure

Threat actors are actively exploiting CVE-2025-11953, a critical command injection flaw in the React Native Metro development server, to gain unauthorised remote code execution. The vulnerability arises when Metro binds to external network interfaces and exposes vulnerable endpoints, allowing attackers to execute arbitrary commands via crafted requests. Security researchers warn that exposed development environments and CI pipelines present high-value entry points for supply chain compromise.

Observed attack chains involve multi-stage PowerShell loaders that disable endpoint protection, establish outbound command-and-control connections, and deploy Rust-based payloads designed to evade analysis. Thousands of exposed Metro instances have been identified online, underscoring systemic risks associated with misconfigured developer tooling. Experts emphasise that development services accessible from the internet must be treated as production-grade infrastructure with equivalent security controls and patching discipline.

ATTACK TYPE	Vulnerability, Malware	**SECTOR**	Healthcare, Hospitality, IT, Government, Education, Business, BFSI, Aviation, Automobile, Retailer, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Apple Mac OS, Windows, Linux, React

Source - https://www.vulncheck.com/blog/metro4shell_eitw#new_tab

TATA COMMUNICATIONS

Update infrastructure breach delivers backdoors through the Notepad++ platform

Developers of Notepad++ confirmed that attackers compromised its update infrastructure following a hosting provider breach, enabling malicious updates to be selectively delivered between July and October 2025. Threat actors frequently rotated delivery chains, C2 infrastructure, and payloads to evade detection, with telemetry revealing multiple infection chains targeting individuals and organisations in Asia, Australia, and Latin America, including government and financial sector entities.

The campaigns deployed Metasploit loaders, Cobalt Strike Beacons, and bespoke backdoors, with some chains collecting detailed system information before dropping secondary payloads. Researchers warned that earlier compromise indicators differed significantly from those publicly reported, meaning organisations relying solely on October indicators may have missed infections. Investigations continue, with additional malicious hashes, domains, and infrastructure uncovered across the campaign timeline.

ATTACK TYPE	Malware	**SECTOR**	Financial Services, IT, Government, Software Development
REGION	Australia, El Salvador, the Philippines, Vietnam, South Asia, East Asia	**APPLICATION**	Apple Mac OS, Notepad++, Windows, Linux

Source - https://securelist.com/notepad-supply-chain-attack/118708/
https://www.validin.com/blog/exploring_notepad_plus_plus_network_indicators/

Crimson RAT deployed against startups in expanded APT36 operation

Threat researchers observed Transparent Tribe (APT36) expanding spear-phishing activity into India's startup sector, using startup-themed lures delivered via ISO files to initiate a multi-stage infection chain. The campaign deploys Crimson RAT through embedded LNK shortcuts and batch scripts, granting persistent remote access. This marks a shift from the group's historic focus on government, defence, and academic targets to private-sector innovation organisations.

Analysis shows the attackers reused infrastructure, command-and-control patterns and tradecraft previously linked to APT36, underscoring continuity in espionage-driven operations. Researchers identified layered obfuscation, custom network protocols, and persistence mechanisms, consistent with the group's long-running intelligence collection campaigns. The targeting of OSINT and cybersecurity firms suggests intent to monitor research activity and defensive capabilities within India's emerging technology ecosystem.

ATTACK TYPE	Social engineering, Malware, Cyber Espionage	**SECTOR**	IT, Government, Education, Defence
REGION	India	**APPLICATION**	Windows

Source - https://www.acronis.com/en/tru/posts/new-year-new-sector-transparent-tribe-targets-indias-startup-ecosystem/

TATA COMMUNICATIONS

Unauthenticated attackers exploit FortiClient EMS via SQL injection flaw

Fortinet has issued security updates to remediate a critical SQL injection vulnerability in FortiClient Enterprise Management Server (EMS), tracked as CVE-2026-21643. The flaw affects FortiClient EMS 7.4.4 and enables unauthenticated attackers to execute arbitrary code or commands through specially crafted HTTP requests, posing an elevated risk of system compromise and data manipulation in exposed deployments.

The vulnerability carries a CVSS score of 9.8, indicating severe impact across confidentiality, integrity, and availability, and has been publicly disclosed following internal discovery by Fortinet's Product Security team. Organisations are urged to upgrade to FortiClient EMS 7.4.5 or later and review internet-facing instances to mitigate potential exploitation, even though no widespread, in-the-wild abuse has been confirmed to date.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, BFSI, Manufacturing, IT, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Apple Mac OS, Windows, Linux, FortiClient EMS, FortiClient

Source - https://fortiguard.fortinet.com/psirt/FG-IR-25-1142

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