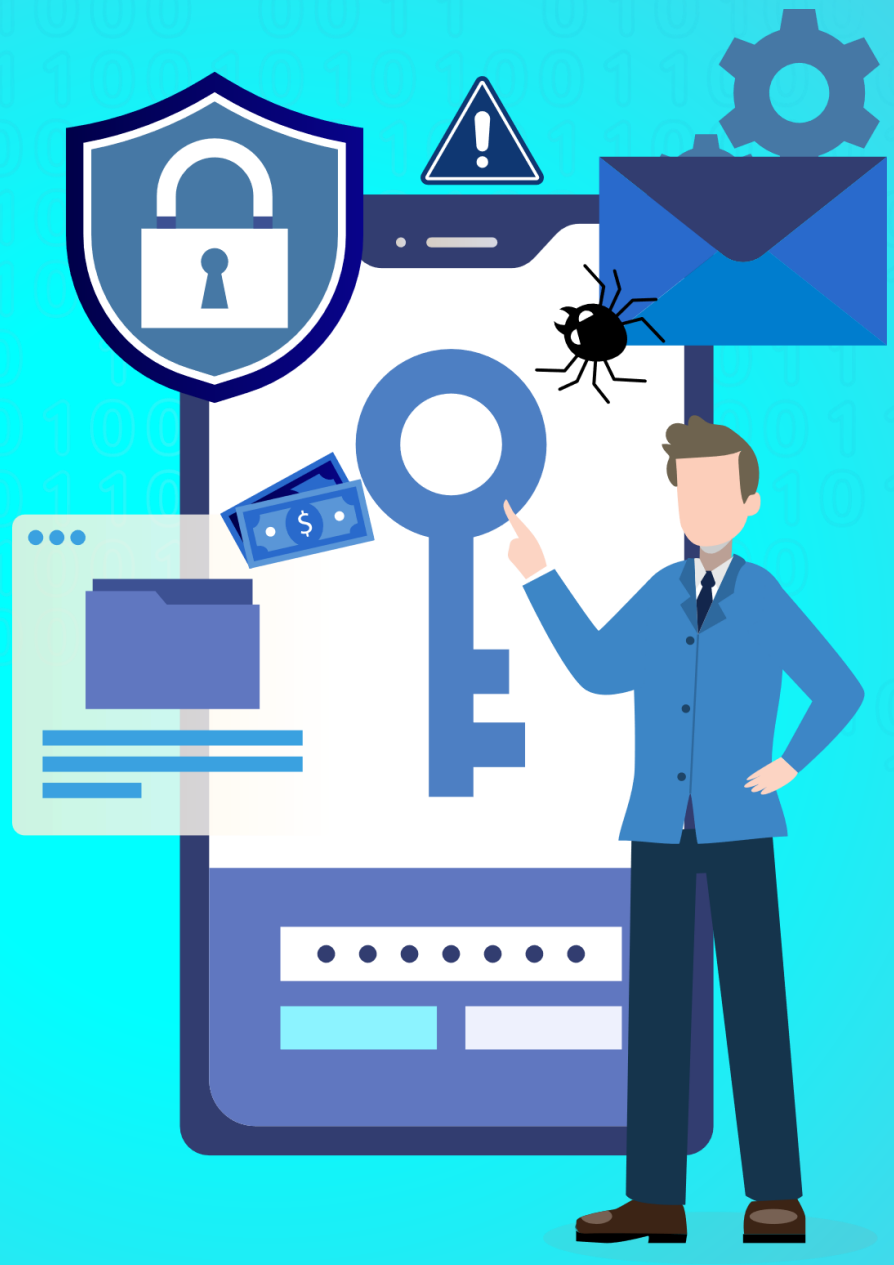
TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: September 30, 2025



TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

Organisations have experienced escalating AI-powered social engineering offensives, precisely coordinated supply chain infiltrations, and progressively sophisticated ransomware iterations throughout 2025. This demonstrates the chronic inadequacy of traditional security protocols in contemporary threat environments. As we enter the last quarter of this year, cyber adversaries continue their advanced campaigns with relentless determination. Staying cyber resilient requires that businesses strengthen their core security infrastructure while deploying comprehensive, intelligence-led defensive systems capable of anticipating and countering evolving threats.

Tata Communications' weekly threat intelligence updates are specifically designed to equip your security teams with the tactical superiority they need. Each report provides timely threat evaluations and actionable recommendations, enabling you to detect, prioritise, and neutralise vulnerabilities before they can disrupt your operations.

TATA COMMUNICATIONS

Sophisticated Gentlemen ransomware launches multi-sector cyberattacks

In August 2025, cybersecurity researchers uncovered a sophisticated campaign by the Gentlemen ransomware group, revealing an exceptionally tailored attack methodology. The group exploited vulnerable signed drivers to disable protection software, manipulated Group Policy Objects to expand their reach, and deployed custom anti-AV tools to neutralise defences. They escalated privileges, compromised domain-level accounts, and exfiltrated sensitive data using encrypted channels.

This campaign struck across countries, with victims primarily in manufacturing, construction, healthcare, and insurance sectors. The attackers demonstrated advanced reconnaissance, persistence, and evasion while shifting tactics mid-campaign, abusing common tools (e.g., PowerRun.exe, PsExec), and using domain-wide deployment via NETLOGON shares. Their evolving, context-aware methods pose a critical threat to enterprise security globally.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Financial services, Manufacturing, Construction
REGION	Thailand, United States, APAC	**APPLICATION**	AnyDesk, Fortinet FortiGate, VMWare ESXi, Windows

Source - https://hivepro.com/threat-advisory/the-gentlemen-ransomware-a-rising-global-cyber-threat/

TATA COMMUNICATIONS

Malicious EvilAI campaign disguises itself as legitimate AI productivity tools

Researchers have recently tracked and identified EvilAI, a sophisticated global malware campaign that masquerades as legitimate productivity and AI tools. With polished interfaces and legitimately signed binaries, the threat has been observed targeting manufacturing, government, and healthcare organisations across Europe, the Americas, and AMEA. Operators use convincing functionality to bypass scrutiny and gain initial footholds via deceptive installers and social engineering.

EvilAI exfiltrates browser credentials, establishes persistence through scheduled tasks and registry modifications, and maintains AES-encrypted command-and-control channels to receive instructions. The campaign executes remote commands, deploys additional payloads, and deliberately obfuscates its activity using AI-generated code and dynamic behaviour. This frustrates detection and analysis, complicating incident response for affected organisations and threatening data confidentiality, operational continuity, and regulatory compliance across enterprises.

ATTACK TYPE	Malware	**SECTOR**	IT, Healthcare, Financial services, Manufacturing, Construction, Government, Education, Retailer, and Distributor
REGION	USA, Europe, India	**APPLICATION**	Microsoft Edge, Google Chrome OS, Mozilla Firefox, Google Chrome

Source - https://www.broadcom.com/support/security-center/protection-bulletin/evilai-malware-mimics-legitimate-tools

Multi-vector CountLoader targets corporate domain-joined systems

A sophisticated new malware loader named CountLoader, usually operated in three forms — .NET, PowerShell, and JScript — is implicated in campaigns tied to LockBit, BlackBasta, and Qilin ransomware groups. The loader was distributed in phishing lures masquerading as Ukrainian police documents, leveraging domain-joined environments to establish initial access.

Once executed, CountLoader stages payloads such as Cobalt Strike, AdaptixC2, PureHVNC, and Lumma Stealer, deploying through multiple techniques tailored for corporate networks. It utilises persistence vectors like scheduled tasks and registry modifications, while dynamically communicating with evolving C2 infrastructure across dozens of domains.

ATTACK TYPE	Malware	**SECTOR**	Financial services, IT, Government, BFSI
REGION	Ukraine	**APPLICATION**	Windows

Source - https://www.silentpush.com/blog/countloader/

Tax authority phishing campaign deploys advanced remote access trojan

A recent surge in phishing campaigns has seen malicious actors impersonating India's Income Tax Department to dupe unsuspecting users into clicking fake links or visiting counterfeit sites. These attacks commonly promise refunds or request manual verification, often citing fabricated norms or amounts to make the deception seem credible. The emails typically use spoofed domains or lookalike addresses; one such fake sender is donotreply@incometaxindiafilling.gov.in.

Victims may become infected with the XWorm RAT, giving attackers full access to the system to possibly perform credential theft, keylogging, data exfiltration, and broader reconnaissance. These campaigns exploit spear-phishing, masquerading, and malicious execution techniques to compromise confidentiality, integrity, and financial security while evading standard detection. Authorities urge all recipients to forward suspicious emails to webmanager@incometax.gov.in or incident@cert-in.org.in and never divulge passwords, OTPs, or banking details.

ATTACK TYPE	Phishing, Malware	**SECTOR**	Financial services, IT, Government, BFSI
REGION	Global	**APPLICATION**	Windows

Source - CERT-IN MAILS

AI-powered MalTerminal uses advanced LLM technology for infiltration

Cyber researchers have now documented a novel class of LLM-embedded malware capable of generating malicious logic at runtime called MalTerminal. This uses GPT-4 to dynamically craft ransomware or reverse-shell code, alongside related tools like PromptLock and LAMEHUG (aka PROMPTSTEAL). Their specimens included embedded API keys and structured prompt patterns, representing a deliberate shift in adversarial tradecraft.

To detect these threats, researchers applied wide YARA rules targeting API-key signatures and then combined prompt extraction with LLM-based classification models. This hybrid approach surfaced previously unknown malware constructs, even before any confirmed real-world deployment. At the time of discovery, MalTerminal's use of a deprecated OpenAI API endpoint suggests it was developed before November 2023, making it among the earliest known examples of LLM-powered malware.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Government, Business, Software Development
REGION	Global	**APPLICATION**	Generic

Source - https://thehackernews.com/2025/09/researchers-uncover-gpt-4-powered.html

Compromised typosquatted libraries target developer code repositories

In July 2025, a malicious PyPI package named termncolor was discovered by Zscaler ThreatLabz. Moreover, on 4 August 2025, they uncovered two more packages, sisaws and secmeasure, that deliver a Python RAT ThreatLabz named SilentSync. The attackers used typosquatting and uploaded secmeasure under the same author identity. Both packages contain initialization code that decodes a hex string to reveal a curl command that downloads a helper Python script from Pastebin and executes it. This delivers the SilentSync payload, a Python-based RAT that supports remote command execution, file exfiltration, screenshot capture, and theft of browser data from Chromium-based browsers and Firefox.

The RAT contacts a hardcoded C2 (200.58.107[.]25) over HTTP on a REST-style API and implements persistence using platform-specific techniques, including Windows registry Run keys, Linux crontab @reboot entries, or macOS LaunchAgents, and cleans up artifacts after exfiltration.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, IT Services and Consulting, Software Development
REGION	Global	**APPLICATION**	Apple Mac OS, Windows, Linux, Python Package Index (PyPI)

Source - https://www.zscaler.com/blogs/security-research/malicious-pypi-packages-deliver-silentsync-rat

State-linked threat actor UNC1549 conducts long-term corporate espionage

Since June 2022, Subtle Snail (UNC1549), a covert, Iran-linked espionage cell aligned with Charming Kitten, has infiltrated 34 devices across 11 organisations, with a concerted shift toward European telecom, aerospace, and defence sectors. Its modus operandi includes LinkedIn recruiting lures targeting employees by inducing them to deploy a MINIBIKE backdoor that relays via Azure-proxied C2 infrastructure to cloak malicious activity.

Once established in the network, Subtle Snail uses spearphishing, DLL sideloading, and signed binaries to quietly deliver custom modules, including keyloggers, browsers, and credential stealers. The group pursues long-term persistence through credential harvesting, exfiltration of sensitive files, and lateral movement, thereby enabling sustained espionage against critical infrastructure and strategic industrial targets.

ATTACK TYPE	Malware	**SECTOR**	Aerospace, Defence Industry, Telecommunications
REGION	Europe	**APPLICATION**	Windows

Source - https://catalyst.prodaft.com/public/report/modus-operandi-of-subtle-snail/overview

Microsoft Entra ID actor token vulnerability enables global admin takeover

Researchers have disclosed CVE-2025-55241, a critical Microsoft Entra ID vulnerability with a CVSS score of 10. The flaw combined undocumented Actor tokens, such as 24-hour service-to-service impersonation JWTs, and a tenant-validation bug in the legacy Azure AD Graph API. Actor tokens bypass Conditional Access, lack revocation and logging, and when paired with public tenant IDs and incremental B2B guest links, could facilitate undetected Global Admin impersonation.

The exploitation could have allowed attackers full tenant takeover, including access to Microsoft 365 and Azure resources. Actor tokens enabled impersonation of any user across tenants without leaving logs. The vulnerability's simplicity meant that a single token could compromise multiple tenants rapidly. Following responsible disclosure by researcher Dirk-Jan Mollema, Microsoft Security Response Center swiftly issued mitigations, patched the flaw, and blocked Actor token requests via the vulnerable Azure AD Graph API.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, Financial services, Manufacturing, Government, Defence Industry, Airline, BFSI, Automobile, Chemical Manufacturing, Mining, Telecommunications, Software Development
REGION	Global	**APPLICATION**	Microsoft Azure, Microsoft Entra

Source - https://securityonline.info/cve-2025-55241-microsoft-entra-id-flaw-with-cvss-10-0-could-have-compromised-every-tenant-worldwide/

Expanding npm affects hundreds of packages across code libraries

In September 2025, the popular @ctrl/tinycolor npm package, with 2.2 million weekly downloads, was compromised in a sophisticated supply chain attack. Initially affecting over 40 packages, including several maintained by CrowdStrike, the malicious update injected a bundle.js script that trojanized downstream packages. The script harvested developer and cloud credentials using TruffleHog, created GitHub Actions workflows, and exfiltrated sensitive data to attacker-controlled endpoints, marking the start of the Shai-Hulud campaign.

Further investigations revealed that the attack expanded to nearly 500 npm packages. The malicious payload ran automatically upon package installation, targeting tokens, CI credentials, and cloud metadata to access sensitive information. By validating npm tokens via the whoami endpoint and integrating with GitHub APIs, attackers exploited automated workflows to steal data systematically. Security teams continue to analyse the evolving attack chain to mitigate further impacts and secure affected packages.

ATTACK TYPE	Malware	**SECTOR**	IT Services and Consulting, Software Development
REGION	Global	**APPLICATION**	CrowdStrike, Node Packager Manager (NPM), GitHub

Source - https://socket.dev/blog/tinycolor-supply-chain-attack-affects-40-packages

Software repository breach attack compromises CrowdStrike libraries

The CrowdStrike npm supply chain attack represents a significant escalation of the same campaign that earlier compromised @ctrl/tinycolor. Whereas the earlier incident impacted about 40 packages across different maintainers, this phase expanded dramatically, with attackers publishing more than 500 malicious packages under the CrowdStrike-publisher account. The core payload, bundle.js, remained consistent, designed to scan for secrets and exfiltrate them. However, unlike the earlier wave, the CrowdStrike attack introduced multiple evolving variants (v1–v7) that steadily refined their tactics by reducing noise, modifying credential checks, and altering workflow logic to improve stealth.

Another key difference lies in targeting: Tinycolor was a popular open-source dependency, but the CrowdStrike compromise demonstrates a deliberate focus on a high-value security vendor. This evolution, tracked as the Shai-Hulud campaign, underscores how the threat is maturing from isolated opportunistic compromises into sustained, large-scale assaults on critical ecosystems.

ATTACK TYPE	Malware	**SECTOR**	IT Services and Consulting, Software Development
REGION	Global	**APPLICATION**	CrowdStrike, Node Packager Manager (NPM), GitHub

Source - https://socket.dev/blog/ongoing-supply-chain-attack-targets-crowdstrike-npm-packages

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