TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: October 7, 2025

THREAT INTELLIGENCE ADVISORY REPORT

Organisations have witnessed an exceptional acceleration in AI-driven social engineering campaigns, strategically orchestrated supply chain breaches, and increasingly advanced ransomware variants throughout the second quarter of 2025. This provides conclusive evidence that conventional security frameworks are demonstrably inadequate for modern threat landscapes. As we transition into the last months of FY25, cyber adversaries continue to intensify their sophisticated operations with unwavering persistence. Consequently, maintaining cyber resilience necessitates that enterprises reinforce their foundational security architecture whilst implementing holistic, intelligence-driven protection mechanisms capable of predicting and mitigating emerging risks.

Tata Communications' weekly threat intelligence briefings are purposefully engineered to provide your security teams with this strategic advantage. Each bulletin delivers current threat assessments and practical guidance, empowering you to identify, triage, and address vulnerabilities before they can compromise your business continuity.

ShinyHunters’ AI-driven vishing and supply chain intrusions reshape cybercrime

ShinyHunters is rapidly evolving into a sophisticated cybercrime actor, leveraging AI-driven vishing, insider access, and supply chain intrusions to expand its operations. Threat analysts note that the group recruits from Scattered Spider and The Com to infiltrate single sign-on platforms used by major sectors, including retail and telecom. Their campaigns focus on exfiltrating sensitive customer data, with stolen datasets sold to ransomware affiliates for sums exceeding $1 million.

The group is also actively developing the ‘shinysp1d3r’ ransomware-as-a-service, designed to encrypt VMware ESXi environments and extend its extortion ecosystem. Targeting high-privilege engineering accounts on Git platforms, BrowserStack, and CI/CD pipelines, ShinyHunters aims to facilitate large-scale supply chain attacks. By exploiting AI-powered voice agents and scalable phishing tools, the group is industrialising cyber extortion and reinforcing its role within the wider cybercriminal ecosystem

ATTACK TYPE	Cybercrime, Phishing, Malware	SECTOR	Financial Services, Manufacturing, Energy, E-Commerce, BFSI, Aviation, Automobile, Hospitality, Retailer, and Distributor
REGION	Global	APPLICATION	VMWare ESXi, Microsoft Office 365, Salesloft-Drift

Source - https://blog.eclecticiq.com/shinyhunters-calling-financially-motivated-data-extortion-group-targeting-enterprise-cloud-applications

Privilege escalation attack deploys ransomware via Oracle Job Scheduler

Attackers gained entry through Oracle DBS Job Scheduler, exploiting the external jobs function to execute malicious commands with elevated privileges. Evidence showed repeated login attempts, eventually granting SYSDBA-level access and enabling payload delivery via extjobo.exe. Encoded PowerShell commands and WSMan facilitated reconnaissance and C2 communications, while Ngrok tunnels were leveraged to bypass perimeter defence and maintain persistence within the compromised environment.

Once inside, adversaries escalated privileges, created local accounts, and used tools such as Process Hacker to disable security controls. The attack culminated in the deployment of “Elons” ransomware, associated with Proxima/Black Shadow. Segmentation limited the spread, restricting encryption to a single server. Notably, no data exfiltration was observed, mitigating broader reputational risks, though confidentiality and availability remained at stake.

ATTACK TYPE	Ransomware	SECTOR	IT Services and Consulting, Business, Software Development
REGION	Morocco, Eastern Europe	APPLICATION	Oracle

Source - https://labs.yarix.com/2025/09/elons-proxima-black-shadow-related-ransomware-attack-via-oracle-dbs-external-jobs/

Dual-layer CyberVolk ransomware threatens enterprise data security

CyberVolk ransomware, which emerged in May 2024, remains active and continues to target public institutions in nations regarded as hostile to Russia. Its stated victims include infrastructure and scientific organisations in Japan, France, and the UK, and the group communicates via Telegram.

Its technique employs a dual-layer encryption: file contents are first encrypted with AES-256-GCM, then re-encrypted using ChaCha20-Poly1305, each file using a unique 12-byte nonce. Because the nonce is not stored with the ciphertext, even though a decryption key is hardcoded, proper decryption fails. To defend, organisations must keep off-site, access-controlled backups and regularly practice recovery drills.

ATTACK TYPE	Ransomware	SECTOR	Manufacturing, IT, Government, Education, E-Commerce, Airline, BFSI, Hospitality
REGION	Japan, UK, France	APPLICATION	Windows

Source - https://asec.ahnlab.com/ko/90033/

Sophisticated BlackLock malware threatens Windows, Linux, and VMware systems

BlackLock (formerly El Dorado) emerged in March 2024 and rebranded in September 2024, operating as a rapidly expanding Ransomware-as-a-Service (RaaS) group. Its operators appear to be Russian-speaking, judging by coding style and promotion on RAMP forums. The group actively enlists affiliates to extend its reach across sectors and regions.

Developed in Go for cross-platform deployment, BlackLock supports Windows, Linux, and VMware ESXi targets and can encrypt files on SMB shares. Each file is encrypted with a unique FileKey and nonce, and metadata is further secured via ECDH-derived shared keys. After encryption, it deletes backups via VSS manipulation and leaves ransom notes across all affected paths, making recovery extremely challenging.

ATTACK TYPE	Ransomware	SECTOR	Construction, Government, Transportation, Education, IT Services, and Consulting
REGION	Japan, South Korea, United States	APPLICATION	VMWare ESXi, Windows, Linux

Source - https://asec.ahnlab.com/ko/90157/

QR code steganography abused in the Fezbox npm supply chain attack

Threat analysts recently uncovered a malicious npm package dubbed fezbox, which posed as a benign JavaScript/TypeScript utility library. Published under the alias janedu, the package embeds multi-layered obfuscation techniques — including reversed strings, QR-code steganography, and encrypted payloads — to evade detection. Importing the library triggers hidden execution paths that remain dormant initially before activating malicious routines.

After a brief delay, fezbox extracts sensitive credentials — specifically, usernames and passwords — from browser cookies and transmits them to a remote server. Its payload is encapsulated within a QR code hosted on a reverse-encoded URL, which is parsed and executed to initiate data exfiltration. This incident underscores the continuously evolving obfuscation tactics and heightened risks lurking within open-source software supply chains.

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

Source - https://socket.dev/blog/malicious-fezbox-npm-package-steals-browser-passwords-from-cookies-via-innovative-qr-code

AI-themed deceptive Android apps drive widespread SlopAds fraud operation

Researchers from HUMAN's Satori Threat Intelligence team exposed "SlopAds," a large-scale Android ad fraud scheme that exploited 224 AI-themed apps with more than 38 million downloads. The apps, active across 228 countries, generated up to 2.3 billion daily ad requests by leveraging hidden WebViews, encrypted configurations, and steganography. Most fraudulent impressions came from the U.S. (30%), India (10%), and Brazil (7%).

The malicious apps used Firebase Remote Config to fetch encrypted payloads and reassembled concealed malware, dubbed FatModule, from image files. Once deployed, FatModule impersonated gaming and news sites to drive continuous ad impressions and clicks through cashout domains controlled by attackers. Google has removed the identified apps and strengthened Play Protect, though researchers warn the campaign's scale suggests similar schemes may re-emerge.

ATTACK TYPE	Malware	SECTOR	IT Services and Consulting, Software Development, Business, E-Commerce, Broadcast Media Production and Distribution
REGION	India, Brazil, United States	APPLICATION	Android

Source - https://www.bleepingcomputer.com/news/security/google-nukes-224-android-malware-apps-behind-massive-ad-fraud-campaign/

Destructive LokiLocker ransomware campaign threatens total system failure

LokiLocker is a highly sophisticated, .NET-based ransomware that targets Windows systems by encrypting files with AES-256 and protecting keys with RSA-2048, all while appending the ".loki" extension. It is disseminated via trojanised tools and exploit kits, employing advanced obfuscation through NETGuard and KoiVM to hinder analysis.

Once installed, LokiLocker achieves persistence by manipulating registry entries, the startup folder, and scheduled tasks. If the ransom demand is not met, it can activate a destructive module to wipe non-system files and overwrite the Master Boot Record, rendering systems permanently unbootable and irrecoverable.

ATTACK TYPE	Ransomware	**SECTOR**	Manufacturing, Construction, IT, Chemical Manufacturing
REGION	Global	**APPLICATION**	Windows

Source - https://thrive.trellix.com/s/article/KB95584?language=en_US&amp;page=content&amp;id=KB95584

Network-propagating Obscura ransomware employs advanced encryption methods

On 29 August 2025, threat analysts uncovered a previously unknown ransomware strain labelled “Obscura,” first observed on a domain controller’s NETLOGON folder, a location that replicates across domain controllers and enables rapid distribution. The executable was embedded with a Go build ID and replicated via scheduled tasks named SystemUpdate, leveraging its placement in a commonly synchronised folder to propagate across the infrastructure.

Obscura enforces strict execution policies, terminating dozens of security and database processes, disabling recovery via VSS deletion, and requiring administrative privileges to run. It employs modern cryptographic constructs — Curve25519 and XChaCha20 — to encrypt data while omitting core system file types and encodes its ransom instructions in base64. Huntress notes that Obscura is part of a pattern of evolving rebrands following variants like Crux and Cephalus.

ATTACK TYPE	Ransomware	SECTOR	Healthcare, Financial Services, Manufacturing, IT, Defence Industry, Business, E-Commerce, Consultancy, BFSI, Retailer and Distributor, and Software Development
REGION	Global	APPLICATION	Windows

Source - https://www.huntress.com/blog/obscura-ransomware-variant

Enterprise VPN vulnerabilities exploited in Akira ransomware campaign

Researchers have observed a significant uptick in Akira ransomware attacks targeting SonicWall SSL VPN accounts since late July 2025. These intrusions often exploit the critical CVE-2024-40766 vulnerability, enabling unauthorised access even when multi-factor authentication (MFA) is enabled. Attackers have been observed moving swiftly through the network, achieving lateral movement, data exfiltration, and encryption in under four hours, with some incidents occurring in as little as 55 minutes.

The ongoing campaign has affected organisations across various sectors, indicating a broad, opportunistic exploitation rather than targeted attacks. To mitigate risks, organisations are urged to promptly apply firmware updates, reset all VPN credentials, enforce MFA, block malicious IP addresses and Autonomous System Numbers (ASNs), and secure LDAP synchronisation accounts. These measures are essential to defend against the rapidly evolving threat posed by the Akira ransomware group.

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

Source - https://arcticwolf.com/resources/blog-uk/september-2025-update-on-aggressive-ongoing-akira-ransomware-campaign/

Malicious Rust crates compromised in a credential harvesting campaign

Analysts identified two malicious Rust crates, faster_log and async_println, masquerading as the legitimate fast_log library. The crates, published under the aliases rustguruman and dumbnbased, contained functional logging features to avoid suspicion but secretly scanned Rust source files for Ethereum and Solana private keys. Matches were exfiltrated via a fake Solana RPC endpoint. Both crates were downloaded 8,424 times since May 25, 2025, before prompt removal.

Following Socket’s disclosure, the Crates security team swiftly removed the malicious packages and locked the associated publisher accounts. They preserved all files for further analysis and issued an official advisory detailing the investigation. The incident highlights the growing risks of typosquatting and supply chain attacks in open-source ecosystems. Developers are urged to verify package authenticity and exercise caution when importing third-party crates.

ATTACK TYPE	Malware	SECTOR	Financial services
REGION	Global	APPLICATION	Apple Mac OS, Windows, Linux, GitHub

Source - https://socket.dev/blog/two-malicious-rust-crates-impersonate-popular-logger-to-steal-wallet-keys | https://socket.dev/blog/two-malicious-rust-crates-impersonate-popular-logger-to-steal-wallet-keys

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.