TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: September 23, 2025

THREAT INTELLIGENCE ADVISORY REPORT

Organisations have witnessed an unprecedented surge in AI-enhanced social engineering attacks, meticulously orchestrated supply chain compromises, and increasingly elusive ransomware variants throughout 2025. This represents compelling evidence that conventional security measures are fundamentally inadequate for today's threat landscape. As we approach the final quarter of this year, cyber adversaries continue to intensify with alarming persistence. Maintaining enterprise cyber resilience demands the fortification of foundational security architecture and implementing multi-layered, threat intelligence-driven frameworks capable of predicting and neutralising emerging risks.

Tata Communications' weekly threat intelligence briefings are precisely 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 mitigate risks before they can compromise your business continuity.

INTRODUCTION

MASSIVE NPM MAINTAINER HACK REDIRECTS CRYPTOCURRENCY TRANSACTIONS

REGISTRY HIJACKING BACKDOOR ENSURES PERSISTENT SYSTEM ACCESS

MEMORY-BASED ESPIONAGE TOOL TARGETS DEFENCE INDUSTRY FIRMS

SVG EMAIL VECTORS DEPLOY SOPHISTICATED REMOTE TROJANS

HYBRIDPETYA RANSOMWARE BYPASSES SECURE BOOT USING UEFI FLAW

SOPHISTICATED TROJANS TARGET WINDOWS, LINUX, AND MACOS

EMERGING RANSOMWARE THREAT USES POWERSHELL SCRIPT ATTACKS

ADVANCED RAT PHISHING ATTACK ENABLES COMPLETE SYSTEM COMPROMISE

UNIFIED COMMAND INFRASTRUCTURE POWERS MULTI-TOOL CYBER ATTACK

COMPLEX MALWARE INFRASTRUCTURE ENABLES PERSISTENT SYSTEM COMPROMISE

Major npm supply chain breach hijacks crypto payments

A major supply chain attack in the npm ecosystem after Qix, a prolific maintainer, was compromised via a phishing-style 2FA reset email sent from what appeared to be support@npmjs.help. The attackers spoofed npm branding in the message, warning that outdated 2FA credentials would cause account lockout, and included a malicious “Update 2FA Now” link.

Many widely used packages co-maintained by Qix and Sindre Sorhus have been affected, with compromised versions published that receive billions of downloads weekly. The malware intercepts fetch() and XMLHttpRequest calls, scans for cryptocurrency wallet addresses in several chains (including Ethereum, Bitcoin legacy and SegWit, Solana, TRON, Litecoin, Bitcoin Cash), and replaces recipients with attacker-controlled addresses.

ATTACK TYPE	Malware	SECTOR	Financial services, IT, Software Development
REGION	Global	APPLICATION	Generic, Node Packager Manager (NPM)

Source - https://socket.dev/blog/npm-author-qix-compromised-in-major-supply-chain-attack

Evasion backdoor targets high-value networks via trojanised downloads

A recently analysed backdoor malware known as Backdoor.Win32.Buterat has emerged as a serious threat to government and enterprise networks. It propagates via phishing campaigns, malicious email attachments, and trojanised software downloads. Once executed, Buterat drops several files — such as amhost.exe, bmhost.exe, cmhost.exe, dmhost.exe, and lqL1gG.exe into a user's directory, disguising itself under legitimate system tasks and employing encrypted or obfuscated strings to hide its internal execution flow.

To maintain persistence, Buterat modifies registry keys and employs advanced thread manipulation techniques such as SetThreadContext and ResumeThread. These methods enable it to hijack existing threads without creating new ones or altering entry points, thereby evading detection by many behaviour-based systems. It also reaches out to a remote command-and-control server at ginomp3.mooo.com. It triggers unusual file creations, posing a high risk unless organisations deploy strong endpoint protection, firewall controls, and threat hunting.

ATTACK TYPE	Malware	**SECTOR**	Financial services, Government, Defence Industry
REGION	Global	**APPLICATION**	Windows

Source - https://www.pointwild.com/threat-intelligence/analysis-of-backdoor-win32-buterat

Multi-stage espionage tool conducts long-term corporate infiltration

A Chinese APT group has been linked to a sophisticated cyber-attack on a Philippine military company, deploying the fileless EggStreme framework to maintain covert access. Leveraging DLL sideloading and in-memory execution, the framework avoids traditional detection. Its multi-stage chain begins with EggStremeFuel, which sets up persistence, before launching EggStremeLoader and EggStremeReflectiveLoader, culminating in EggStremeAgent — a versatile backdoor enabling surveillance, keylogging, and lateral movement across compromised systems.

EggStremeAgent, the framework’s core, supports 58 commands, allowing attackers to perform system fingerprinting, privilege escalation, data theft, and process injection. The attackers also deployed EggStremeWizard, a secondary backdoor resilient to takedowns through multiple command-and-control servers. This campaign reflects the hallmarks of a professional threat actor aligned with China’s strategic objectives in the South China Sea.

ATTACK TYPE	Malware	SECTOR	All
REGION	China, Philippines	APPLICATION	Windows, PowerShell

Source - https://www.bitdefender.com/en-us/blog/businessinsights/eggstreme-fileless-malware-cyberattack-apac

INTRODUCTION
MASSIVE NPM MAINTAINER HACK REDIRECTS CRYPTOCURRENCY TRANSACTIONS
REGISTRY HIJACKING BACKDOOR ENSURES PERSISTENT SYSTEM ACCESS
MEMORY-BASED ESPIONAGE TOOL TARGETS DEFENCE INDUSTRY FIRMS
SVG EMAIL VECTORS DEPLOY SOPHISTICATED REMOTE TROJANS
HYBRIDPETYA RANSOMWARE BYPASSES SECURE BOOT USING UEFI FLAW
SOPHISTICATED TROJANS TARGET WINDOWS, LINUX, AND MACOS
EMERGING RANSOMWARE THREAT USES POWERSHELL SCRIPT ATTACKS
ADVANCED RAT PHISHING ATTACK ENABLES COMPLETE SYSTEM COMPROMISE
UNIFIED COMMAND INFRASTRUCTURE POWERS MULTI-TOOL CYBER ATTACK
COMPLEX MALWARE INFRASTRUCTURE ENABLES PERSISTENT SYSTEM COMPROMISE

Malicious SVG email campaigns target systems with RATs

Recent campaigns demonstrate how threat actors are innovating delivery methods by embedding obfuscated BAT loaders in SVG files and email attachments. These loaders are often hidden within ZIP archives hosted on legitimate platforms like ImgKit, luring unsuspecting users. Once executed, the BAT scripts employ PowerShell commands to decode, decrypt, and execute payloads directly in memory, enabling stealthy fileless infections that bypass traditional endpoint security controls.

The campaigns ultimately deploy Remote Access Trojans such as XWorm and Remcos, both known for capabilities like keylogging, remote command execution, screenshot capture, and data exfiltration. Persistence is achieved by planting BAT files in Windows startup folders, ensuring repeated execution. Moreover, the malware disables key security features such as AMSI and ETW, allowing its PowerShell scripts and loaders to execute unhindered while evading logging and detection by security solutions.

ATTACK TYPE	Malware	SECTOR	IT, Healthcare, Financial services, Manufacturing, Construction, Government, Transportation, Oil and gas, Aviation, E-Commerce, BFSI, Telecommunications
REGION	Global	APPLICATION	Windows

Source - https://www.seqrite.com/blog/xworm-remcos-bat-svg-malware-analysis/

Sophisticated HybridPetya ransomware bypasses UEFI secure boot

Researchers have uncovered a new ransomware strain dubbed HybridPetya, first uploaded to VirusTotal in February 2025. It resembles both Petya and NotPetya, but its distinguishing feature is its capability to attack UEFI-based systems by installing a malicious EFI application in the EFI System Partition. This component encrypts the NTFS Master File Table (MFT), which holds crucial metadata for all files.

One variant of HybridPetya exploits CVE-2024-7344, a UEFI Secure Boot bypass vulnerability patched earlier in the year. It uses a crafted cloak.dat file bundled with a vulnerable Microsoft-signed UEFI application to ignore integrity checks during boot, thus circumventing Secure Boot on outdated firmware.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Healthcare, Financial services, Manufacturing, Construction, Government, Education, Aerospace, BFSI, Software Development
REGION	Global	**APPLICATION**	Windows

Source - https://www.welivesecurity.com/en/eset-research/introducing-hybridpetya-petya-notpetya-copycat-uefi-secure-boot-bypass/

Modular RAT and Backdoor families enable cross-platform cyber attacks

Two new malware families have recently been uncovered that underscore growing risks across operating systems. The first, dubbed CHILLYHELL, is a modular backdoor developed in C++ for Intel-based macOS systems, attributed to UNC4487, an espionage actor active since at least October 2022. CHILLYHELL creates persistence via LaunchAgent or LaunchDaemon and shell profile modifications, uses timestomping to hide artefacts and profiles hosts extensively, and supports commands for reverse shells, brute-force attacks, payload downloads, and more.

The second threat, ZynorRAT, is a Go-based Remote Access Trojan that can infect Windows and Linux hosts and is centrally managed through a Telegram bot called @lraterrorsbot. It offers functionalities including file exfiltration, system enumeration, screenshot capture, arbitrary command execution, persistence via systemd (on Linux), directory listing, process-killing, and payload delivery—all indicating a rapid development trajectory and cross-platform ambition.

ATTACK TYPE	Malware	**SECTOR**	Government
REGION	Ukraine	**APPLICATION**	Apple Mac OS, Windows, Linux

Source - https://thehackernews.com/2025/09/chillyhell-macos-backdoor-and-zynorrat.html

PowerShell-based ransomware employs double extortion tactics

Yurei was first observed on 5 September 2025 when a Sri Lankan food-manufacturing firm became its first public victim. The group runs a double-extortion model, encrypting files while exfiltrating data, then threatening publication unless demands are met. Yurei's code is largely derived from the open-source Prince-Ransomware family written in Go, with only minor modifications, making visible flaws like retained debug symbols and leftover module names.

Technically, Yurei encrypts files using the ChaCha20 algorithm with a unique key and nonce per file, then protects those with ECIES using the attacker's public key. It appends the extension ".Yurei", monitors connected network drives, and encrypts in parallel using goroutines — speeding its operation. Importantly, it does not delete Volume Shadow Copies, leaving open the possibility of restoration in environments where VSS is enabled, even though exfiltration retains leverage over victims.

ATTACK TYPE	Ransomware	SECTOR	Government
REGION	IT, Healthcare, Financial services, Manufacturing, Construction, Government, Transportation, Education, Aerospace, BFSI, Software Development, Textiles	APPLICATION	Windows

Source - https://research.checkpoint.com/2025/yurei-the-ghost-of-open-source-ransomware/

Remote access trojan payload bypasses security via privilege abuse

Researchers at Fortinet have exposed a sophisticated phishing campaign aimed at Japanese Windows users through which a Remote Access Trojan, MostereRAT, is deployed. The attack begins with deceptive emails mimicking business enquiries, leading targets to download Word documents embedding ZIP archives. Within the archives is a malicious executable that stages further payloads. Key evasion techniques include the use of Easy Programming Language (EPL), mutual TLS (mTLS) for encrypted command-and-control, privilege escalation via the TrustedInstaller account, and the suppression or blocking of many antiviruses and EDR solutions.

Once deployed, MostereRAT delivers full system compromise by installing legitimate remote access tools like AnyDesk, TightVNC, and RDP Wrapper to allow persistent covert access. It also implements modules to capture keystrokes and screenshots, enumerate users, create hidden administrator accounts, execute shellcode, and inject additional payloads. Such multi-stage aggressiveness, combined with its ability to disable security mechanisms, makes detection and mitigation particularly challenging.

ATTACK TYPE	Malware	SECTOR	Government, Business
REGION	Japan	APPLICATION	Windows

Source - https://www.fortinet.com/blog/threat-research/mostererat-deployed-anydesk-tightvnc-for-covert-full-access

Persistent APT37 threat group targets human rights activists worldwide

APT37, also tracked as ScarCruft, has been linked to fresh campaigns deploying a Rust-based backdoor named Rustonotto alongside a Python loader. According to Zscaler, the actor continues to refine its malware arsenal, targeting South Korean individuals tied to human rights or regime-related matters. The group uses sophisticated tactics such as Process Doppelgänging to evade detection, underlining its emphasis on stealth and persistence in espionage operations.

The campaign also integrates multiple malware families under a single command-and-control framework, including Chinotto, a PowerShell-based backdoor, and FadeStealer, designed for large-scale data exfiltration. Infection chains observed by Zscaler exploit Windows shortcut files and malicious help files to deliver payloads efficiently. This coordinated approach highlights APT37's evolving technical capabilities and its growing reliance on multi-layered malware delivery systems to sustain long-term intelligence-gathering efforts.

ATTACK TYPE	Malware	SECTOR	Government
REGION	South Korea	APPLICATION	Python, Windows, PowerShell

Source - https://www.zscaler.com/blogs/security-research/apt37-targets-windows-rust-backdoor-and-python-loader

Multi-stage malware infrastructure enables stealth system compromise

Since March 2025, TAG-150 has demonstrated rapid escalation in capability, operating an extensive, multi-tiered infrastructure supporting malware families including CastleLoader, CastleBot, and CastleRAT. The latter, available in both Python and C variants, allows system reconnaissance, payload deployment, and remote command execution. TAG-150 leverages phishing campaigns, fraudulent GitHub repositories, and domains imitating legitimate services to deceive victims into executing malicious PowerShell commands, enabling initial compromise and sustained access.

TAG-150 employs a vast toolset, including information stealers such as RedLine, Rhadamanthys, and Stealc, alongside secondary payloads like WarmCookie and SectopRAT. Infrastructure is supported by threat-enabling providers and anti-detection services such as Kleenscan, while file-sharing platforms, including temp[.]sh, facilitate operations. Defenders are urged to block associated IPs and domains, update YARA and Snort rules, and continuously monitor the threat landscape to counter evolving risks.

ATTACK TYPE	Malware	SECTOR	IT, Business
REGION	Russia, United States	APPLICATION	Windows

Source - https://www.recordedfuture.com/research/from-castleloader-to-castlerat-tag-150-advances-operations

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.