TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: August 26, 2025

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

Today's rapidly evolving digital environment has made protecting against cybersecurity risks a critical concern for organisations across the globe. As these risks evolve, businesses are focusing not only on protecting their data but also on reinforcing the core infrastructures that underpin modern operations. The aim is to build resilience against an ever-expanding range of emerging threats.

Boost your organisation’s cybersecurity preparedness with Tata Communications’ weekly threat intelligence advisory. Discover valuable insights into the latest cyber risks and adopt proactive measures to strengthen your defences, helping you effectively reduce potential vulnerabilities.

Hackers actively leverage critical WinRAR vulnerability

Researchers recently uncovered a previously unknown WinRAR zero-day vulnerability (CVE-2025-8088) – a directory-traversal flaw exploiting alternate data streams – that was actively weaponised against financial, manufacturing, defence, and logistics firms across Europe and Canada. Spear-phishing emails carrying malicious RAR attachments disguised as job applications delivered backdoors such as SnipBot, RustyClaw/MeltingClaw and Mythic Agent, underscoring the sophistication and geopolitical targeting of the threat actor.

This incident marks at least the third occasion the RomCom group has leveraged a zero-day vulnerability in live campaigns — their earlier exploits included Microsoft Word and Firefox flaws. Fortunately, no successful compromises were observed in monitored systems. A patch was expedited in WinRAR version 7.13, yet users must manually update, as the application does not auto-update, to fully mitigate the threat.

ATTACK TYPE	Vulnerability, Malware	**SECTOR**	Manufacturing, Defence Industry, BFSI, Logistics
REGION	Europe, Canada	**APPLICATION**	WinRAR

Source - https://www.welivesecurity.com/en/eset-research/update-winrar-tools-now-romcom-and-others-exploiting-zero-day-vulnerability/

Public sectors face advanced Charon ransomware threat

A newly emerged ransomware strain, known as Charon, is targeting the Middle East's public sector and aviation industry using sophisticated, APT-style methods. The attack employs DLL sideloading of a malicious msedge.dll via a legitimate browser binary to inject a hidden payload, while deploying process injection and anti-endpoint detection techniques for stealth and persistence. Tailored ransom notes and partial encryption elevate the threat beyond opportunistic ransomware.

Once executed, the ransomware disables security services, deletes shadow copies and Recycle Bin files, and utilises partial encryption with a hybrid Curve25519-ChaCha20 scheme. Encrypted files are tagged with a unique infection marker and a custom ".Charon" extension. It spreads across network shares while avoiding ADMIN$ paths and includes a dormant anti-EDR driver — highlighting both current threat sophistication and the potential for future capability enhancements.

ATTACK TYPE	Ransomware	**SECTOR**	Aviation
REGION	Middle East	**APPLICATION**	Windows

Source - https://securityonline.info/charon-ransomware-emerges-apt-style-precision-meets-destructive-encryption/

Major hacker groups partner for combined attack strategy

A resurgent cybercrime campaign has seen a notorious data-theft group, ShinyHunters, evolve from traditional breaches to highly targeted social engineering and vishing operations, alongside Scattered Spider. Their coordinated efforts have focused on harvesting credentials from Salesforce users, employing phishing infrastructure and Okta-style credential-theft pages. Domain registration patterns and shared aliases suggest more than a year of strategic alignment and shared tactics across campaigns.

The concerted operations are now shifting towards financial services and technology sectors, hinting at an expanded scope of intrusion and extortion. These developments coincide with a surge in voice-phishing campaigns and the use of impersonated IT support to penetrate enterprise systems, followed by targeted credential harvesting. Organisations must remain vigilant, particularly around SaaS platforms where human-led deception is increasingly leveraged.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source - https://reliaquest.com/blog/threat-spotlight-shinyhunters-data-breach-targets-salesforce-amid-scattered-spider-collaboration/
https://thehackernews.com/2025/08/cybercrime-groups-shinyhunters.html

Hackers deploy ransomware targeting VM infrastructures

The DarkBit ransomware operation targeted VMware ESXi environments by halting virtual machines using ESXCLi commands and encrypting critical files with a bespoke tool. Several VMware-specific formats — including .vmdk, .vmx and .nvram — were retitled with a .Darkbit extension, rendering enterprise systems inoperable within minutes. The attack emphasises the escalating precision and severity of ransomware threats in virtualised infrastructures.

Subsequent analysis exposed a flaw in the ransomware's AES-128-CBC implementation, where weak key generation and predictable VMDK file headers enabled recovery via brute-force techniques and sparse-file extraction. Incident responders could reconstruct much of the data without paying a ransom. Practitioners are advised to audit ESXi activity, maintain isolated backups and enforce network segmentation to strengthen defences against similar high-impact attacks.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	VMWare ESXi

Source - Cert-In Feeds

CrossC2 ReadNimeLoader detected in recent ransomware attacks

Between September and December 2024, JPCERT/CC observed highly sophisticated campaigns involving CrossC2, an unofficial Linux-compatible extension of Cobalt Strike, and custom malware "ReadNimeLoader" to Linux and macOS systems. A custom loader, written in Nim language, was sideloaded via a legitimate process to deploy shellcode entirely in memory. Anti-analysis features — such as junk-code insertion and decryption routines tied to execution flow enabled stealthy compromise of both Linux and Windows servers.

Adversaries further engaged with Active Directory using tools like PsExec, Plink, SystemBC, and GetNPUsers for lateral movement and privilege escalation. Overlapping infrastructure and naming conventions suggest operational links to known sophisticated ransomware campaigns. Many Unix-based servers lack endpoint detection and response measures, leaving them exposed. Security teams are advised to enhance monitoring of cross-platform environments, audit scheduled tasks and investigate unusual process loading to detect similar intrusions.

ATTACK TYPE	Ransomware, Malware	**SECTOR**	All
REGION	Japan	**APPLICATION**	Windows, Linux

Source - https://blogs.jpcert.or.jp/en/2025/08/crossc2.html

Advanced bypass tools enable Crypto24 operations

Crypto24 showcases advanced ‘living-off-the-land’ tactics, combining legitimate IT tools with bespoke malware to evade defences. Operators disable endpoint detection and response via a customised EDR bypass tool, then maintain access using privileged accounts, scheduled tasks and keylogging services. Sensitive data is stealthily exfiltrated—typically via cloud storage—before the ransomware payload is finally deployed, highlighting deep operational planning and technical prowess across global targets

Targets span Asia, Europe and the US — particularly high-value sectors such as finance, manufacturing, entertainment and technology — where attackers exploit off-hours to minimise detection. They employ tools such as PSExec, AnyDesk and Group Policy utilities to pivot laterally, reactivate disabled accounts and maintain persistence. Security leaders are urged to deploy layered defences, enforce least-privilege access, safeguard cloud exfiltration channels and vigilantly monitor for signs of EDR tampering.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Manufacturing, Entertainment, BFSI
REGION	Australia, Germany, New Zealand, United States	**APPLICATION**	Enterprise IT, EDR solutions, Cloud storage platforms

Source - https://www.trendmicro.com/en_us/research/25/h/crypto24-ransomware-stealth-attacks.html
https://www.darkreading.com/cybersecurity-operations/crypto24-ransomware-bypass-edr

Emerging Jackpot ransomware threatens data theft encryption

The newly identified ransomware strain Jackpot, derived from the MedusaLocker family, encrypts victim files using RSA and AES cyphers and affixes a unique ".jackpot[number]" extension to each one. On execution, it alters the desktop wallpaper and drops a READ_NOTE.html ransom message. Victims are warned that third-party recovery tools may permanently damage encrypted files and are offered decryption of a few less critical items as proof.

The campaign notably employs double-extortion tactics, combining strong encryption with threats to leak stolen data if the ransom is not paid. Built-in anti-analysis checks and stealth methods — such as automation through WMI — enhance evasion capabilities. Attackers pressure victims with a 72-hour deadline to comply. This structured, high-pressure approach underlines the growing shift toward highly targeted, high-impact ransomware operations that blend cryptographic sophistication with strategic coercion.

ATTACK TYPE	Ransomware	**SECTOR**	Government
REGION	Global	**APPLICATION**	Windows

Source - https://www.cyfirma.com/news/weekly-intelligence-report-15-august-2025/

TATA COMMUNICATIONS

XZ-Utils vulnerability continues endangering Docker builds

New intelligence reveals that Docker Hub still hosts at least 35 Linux container images — including various Debian builds — that contain a stealthy backdoor inserted into the XZ-Utils compression library in 2024. These images, preserved as legacy artefacts by maintainers, pose a persistent supply-chain threat, especially when used in automated builds or CI pipelines. Nested child images may also transitively inherit the compromise.

While the backdoor requires a narrow set of conditions—such as running an SSH daemon inside the container and possessing a specific private key—to be exploitable, its mere availability elevates risk. Security experts warn of the danger of pulling outdated images, recommending that organisations remove these compromised artefacts entirely, adopt only updated container sources, and institute robust binary-level monitoring to safeguard against silent, lingering vulnerabilities.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Linux

Source - https://securityonline.info/critical-xz-backdoor-still-lurks-in-docker-images-posing-supply-chain-risk/

TATA COMMUNICATIONS

Banking Trojan platform leak exposes compromised infrastructure

A full leak of the banking trojan ERMAC V3.0 source code has exposed its entire malware-as-a-service infrastructure, including a PHP/Laravel backend, React operator panel, Golang exfiltration server and Android builder. This variant, evolved from earlier families like Cerberus, now targets over 700 banking, shopping and cryptocurrency applications. The disclosure offers rare visibility into its operational mechanics and elevated form-injection capabilities.

Analysis revealed multiple critical flaws in ERMAC's setup — including hardcoded JWT secrets, default root credentials and open signup in the admin panel — offering defenders tangible opportunities to disrupt active campaigns. The Android backdoor, built in Kotlin, supports device control, SMS capture, overlay injection and AES-CBC encrypted communications. Protection measures should include blocking known command-and-control endpoints and scanning for exposed builder infrastructure.

ATTACK TYPE	Malware	**SECTOR**	Financial services, E-commerce, BFSI
REGION	Global	**APPLICATION**	Android

Source - https://thehackernews.com/2025/08/ermac-v30-banking-trojan-source-code.html

Updated FireWood backdoor refines command operations

A newly emerged variant of the longstanding FireWood Linux backdoor retains core remote-access capabilities while introducing refined startup, networking and persistence behaviour. The updated version removes early permission gating, streamlines beaconing into a continuous connection loop, and enhances OS detection with fallback parsing of /etc/issue.net. File-path configurations have also been reorganised, reflecting ongoing operator-driven optimisation for stealth and reliability.

Adversaries continue to employ kernel-level rootkit modules aligned with Project Wood-era tooling, using TEA encryption for covert communication and exfiltration. Command sets have been slimmed down, with legacy options removed and new features — such as an 'auto-kill' control added. Samples detected across regions, including the Philippines and Iran, signal growing geographic dispersion and underline the persistent threat of Linux-centric backdoors.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Iran, Philippines	**APPLICATION**	Linux

Source - https://intezer.com/blog/threat-bulletin-firewood/

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