TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: September 2, 2025

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

In today's fast-changing digital landscape, cybersecurity has become a critical priority for organisations worldwide. As threats continue to advance, companies are expanding their focus beyond data security to strengthen the fundamental infrastructure that drives modern business operations. The goal is to develop robust defences capable of withstanding a continuously growing spectrum of new cyber challenges.

Enhance your company's cyber defence capabilities through Tata Communications' weekly threat intelligence briefings. Gain actionable intelligence on current cyber threats and implement preventive strategies to fortify your security posture, enabling you to minimise exposure to potential risks.

TATA COMMUNICATIONS

EncryptHub group launches complex multi-vector cyber attacks

A Russian cyber-threat actor, aka EncryptHub (aka LARVA-208/Water Gamayun), tracked under multiple aliases, has launched sophisticated campaigns that combine social engineering with exploitation of a Microsoft Management Console flaw (CVE-2025-26633, also known as MSC EvilTwin). The intrusion begins with convincing IT-support impersonation via Microsoft Teams to establish remote access, triggering deployment of PowerShell loaders that drop dual .msc files. These facilitate the execution of the malicious duplicate and initiate infection routines.

Once executed, the malicious .msc leverages trusted platform abuse — such as hosting payloads via Brave Support or fake conferencing services—to deliver tools like Golang backdoors, Fickle Stealer and custom malware modules. The actor maintains persistence, decrypts AES-encrypted C2 commands via PowerShell, exfiltrates sensitive data, and obfuscates network traffic with simulated web activity. The campaign underscores the need for layered defences, rapid patching and heightened user awareness.

ATTACK TYPE	Vulnerability, Malware	**SECTOR**	Financial services, IT, BFSI
REGION	Global	**APPLICATION**	WinRAR

Source - https://thehackernews.com/2025/08/russian-group-encrypthub-exploits-msc.html

Malicious phishing campaign uses government impersonation for theft

A recently discovered Android phishing campaign is targeting users in India by masquerading as a government-run electricity subsidy initiative. Malicious actors are deploying YouTube-hosted tutorials, fake government-style websites and GitHub-hosted APK files to entice victims into downloading malware. Once installed, the app harvests banking credentials, intercepts SMS messages, sends phishing content to contacts and enables remote control of the compromised device.

The application exploits Firebase for command-and-control functions and can silently exfiltrate sensitive information, while propagating via SMS messages sent from infected phones. This attack not only puts individual privacy at grave risk but also threatens financial security through credential theft and smishing. The campaign underscores the urgent need for heightened user vigilance, robust mobile-security defences and stricter controls over sideloaded Android applications.

ATTACK TYPE	Malware, Mobile	**SECTOR**	BFSI
REGION	India	**APPLICATION**	Android

Source - https://www.mcafee.com/blogs/other-blogs/mcafee-labs/android-malware-promises-energy-subsidy-to-steal-financial-data/

Modular malware exploits zero-day for system compromise

A modular backdoor first identified in 2022 has resurfaced, exploiting a patched Windows privilege-escalation flaw (CVE-2025-29824) to infiltrate systems. The malware is being deployed under the guise of a ChatGPT-style desktop application, using loader methods such as Microsoft Help Index files, fake ChatGPT clients and DLL hijacking. These tactics enable attackers to surreptitiously install the backdoor with elevated privileges, evade defences and gain foothold access.

Once deployed, the payload communicates locally using encrypted named pipes and linked-list structures to receive plug-in modules. These modules provide capabilities including payload injection, credential theft, asynchronous communication and lateral movement via tools like ProcDump to extract LSASS credentials. Recent campaigns targeting organisations in Saudi Arabia and Brazil demonstrate the backdoor's adaptability and persistence, underscoring the ongoing threat despite incremental changes over the years.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Brazil, Saudi Arabia	**APPLICATION**	Windows

Source - https://securelist.com/pipemagic/117270/
https://www.microsoft.com/en-us/security/blog/2025/08/18/dissecting-pipemagic-inside-the-architecture-of-a-modular-backdoor-framework/

Trigona variant targets industries leveraging partnership attack models

The BlackNevas ransomware, a new variant of Trigona, also known as “Trial Recovery”, is expanding its global reach across sectors including law, finance, IT and manufacturing. It employs robust hybrid encryption — AES-256 for symmetric and RSA-4096 for asymmetric protection across multiple environments such as Windows, Linux, NAS and VMware ESXi. Its deployment methods and propagation capabilities underscore its elevated sophistication and resilience.

The ransomware’s operators leverage a partnership-driven extortion model, working with other criminal groups to leak stolen data when victims resist paying. Victim organisations face serious operational, financial and reputational risks from both data encryption and potential public exposure. Its persistent, multi-platform infection strategy highlights the critical importance of comprehensive defences — including network segmentation, off-site backups and incident readiness to mitigate escalating ransomware threats.

ATTACK TYPE	Ransomware	**SECTOR**	Tourism/Hospitality, Financial services, Manufacturing, IT, Energy, Business, BFSI, Telecommunications
REGION	Japan, UK, South Korea, Spain, Thailand, United States	**APPLICATION**	VMWare ESXi, Windows, Linux

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

Windows kernel vulnerability leads to complete device takeover

In April 2025, a zero-day vulnerability in Windows' Common Log File System (CVE-2025-29824) was patched after being actively exploited by a ransomware group. The flaw, a use-after-free issue in the kernel driver clfs.sys, allowed attackers to elevate privileges to SYSTEM by hijacking dllhost.exe, facilitating unauthorised deployment of ransomware payloads. This incident demonstrates the high stakes of kernel-level privilege escalation.

Although now patched, the exploit underscores the increasing reliance on kernel-mode driver weaknesses by threat actors to bypass defences. It highlights the importance of layered security, continuous endpoint detection and response monitoring, and prompt application of patches to safeguard systems. The incident is a stark reminder that proactive defence and vigilance are essential in defending against sophisticated privilege-escalation and ransomware threats.

ATTACK TYPE	Ransomware, Vulnerability	**SECTOR**	All
REGION	Saudi Arabia, Spain, United States, Venezuela	**APPLICATION**	Windows

Source - https://securityonline.info/researcher-details-cve-2025-29824-a-windows-clfs-0-day-exploited-by-ransomware-gang/

The Paper Werewolf group delivers malware through archive exploits

A threat actor known as Paper Werewolf (GOFFEE) in July 2025, leveraged a known WinRAR flaw (CVE-2025-6218) and a newly exploited zero-day affecting versions through 7.12, in phishing campaigns disguised as official correspondence. Recipients were sent poisoned RAR archives that, once extracted, dropped trojanised executables and .NET loaders. This enabled automated persistence and covert remote access on compromised systems.

These campaigns underscore the rising misuse of archive-based malware delivery, along with the underground market for zero-day exploits reportedly sold for substantial sums. They reinforce the need for continuous security monitoring, threat hunting, and prompt application of updates—including manual patches, given the lack of auto-updates in many archive utilities. Vigilance remains paramount to defend against increasingly sophisticated espionage tactics targeting trusted file formats.

ATTACK TYPE	Malware	**SECTOR**	Government, Transportation, Aviation
REGION	Russia	**APPLICATION**	Windows, WinRAR

Source - https://bi.zone/eng/expertise/blog/paper-werewolf-atakuet-rossiyu-s-ispolzovaniemuyazvimosti-nulevogo-dnya-v-winrar/

TATA COMMUNICATIONS

SharePoint servers become a gateway for Warlock ransomware deployment

The Warlock ransomware group has swiftly emerged as a global cyber-threat by exploiting unpatched on-premises Microsoft SharePoint vulnerabilities to gain initial access. Through HTTP POST requests, web shells are deployed to achieve reconnaissance, privilege escalation, credential theft and lateral movement via native Windows tools. The campaign culminates in ransomware that appends files with the .x2anylock extension, highlighting the peril of delayed patching and emphasising the need for layered defences.

Following encryption, victim data is exfiltrated using RClone, enabling double-extortion tactics that amplify operational, financial and reputational impact. The group appears to operate under a ransomware-as-a-service model, rapidly weaponising enterprise vulnerabilities globally. This trend underscores the critical importance of continuous security monitoring, threat hunting, proactive patching and segmentation to counter fast-evolving ransomware groups targeting unprotected infrastructure.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Government
REGION	North America, Europe, Africa, Asia	**APPLICATION**	Microsoft SharePoint Server, Windows

Source - https://www.trendmicro.com/en_us/research/25/h/warlock-ransomware.html

TATA COMMUNICATIONS

Hacktivists exploit IoT-botnets for sustained DDoS attack operations

In July 2025, botnet-driven DDoS attacks surged, averaging over 600 daily incidents, peaking above 1,100 during holiday periods. A prominent hacktivist collective led a significant share — exceeding 200 attacks targeting sectors such as government, transportation and finance. Adversaries exploited compromised IoT devices, home routers and long-unpatched vulnerabilities to execute multivector flood campaigns. Smaller allied groups also contributed to relentless pressure on the web and VPN infrastructure.

This sustained wave of attacks underscores the growing challenge of defending digital infrastructure amid coordinated botnet operations. By weaponising fragmented IoT ecosystems with weak patching and standard configurations, attackers can overwhelm even hardened defences. Multiple vectors, including TCP SYN, HTTP and UDP floods — demand layered security approaches such as automated detection, rate limiting, and resilient incident response. The trend highlights the urgent need for enhanced visibility and proactive mitigation strategies.

ATTACK TYPE	Vulnerability, Hacktivism, DDOS	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source - Threat Intel Internal Research

TATA COMMUNICATIONS

APT36 targets Linux systems for government espionage globally

Researchers have uncovered an advanced cyber-espionage campaign, APT36 (Transparent Tribe), targeting Indian government infrastructures running BOSS Linux. Attackers initiate compromise via spear-phishing emails containing ZIP archives that house deceptive .desktop shortcut files disguised as legitimate documents. Once executed, these files silently download and launch hidden ELF binaries while displaying benign PDFs. The operation establishes persistence through systemd services and cron jobs, enabling stealthy remote command-and-control communication.

The malicious payload communicates with attacker-controlled domains via WebSocket or DNS channels to receive instructions and exfiltrate data. With anti-debugging and anti-sandbox techniques observed in payloads, the campaign demonstrates tailored delivery methods that evade conventional defences. The focus on Linux-specific vectors like .desktop shortcuts reinforces the need for extended endpoint security controls, suspicious file monitoring, and proactive domain filtering in critical infrastructure environments.

ATTACK TYPE	Malware, Cyberespionage	**SECTOR**	Government, Defence Industry
REGION	India	**APPLICATION**	Windows, Linux

Source - https://www.cyfirma.com/research/apt36-targets-indian-boss-linux-systems-with-weaponized-autostart-files/

Emerging RaaS employs anti-analysis defence methods

Bqtlock, a newly surfaced Ransomware-as-a-Service strain, is changing the threat landscape through a subscription-based model operated by a hacktivist collective. Distributed via ZIP archives containing executables, the malware encrypts files using hybrid AES-256 and RSA-4096 cryptography, appending a unique extension and demanding cryptocurrency payment within a tight timeframe. Failure to comply triggers ransomware doubling and permanent deletion of decryption keys, while threatened data leaks intensify pressure.

Beyond encryption, the malware incorporates robust anti-analysis and persistence mechanisms—string obfuscation, debugger detection, virtual machine evasion, process hollowing, UAC bypasses, and scheduled tasks masquerading as legitimate system utilities. It also steals browser credentials and employs exfiltration via Discord and Telegram. These evolving capabilities underscore the necessity for layered defences, including behaviour-based detection, phishing-resistant delivery strategies, and rapid incident response to counter such agile threats.

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

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