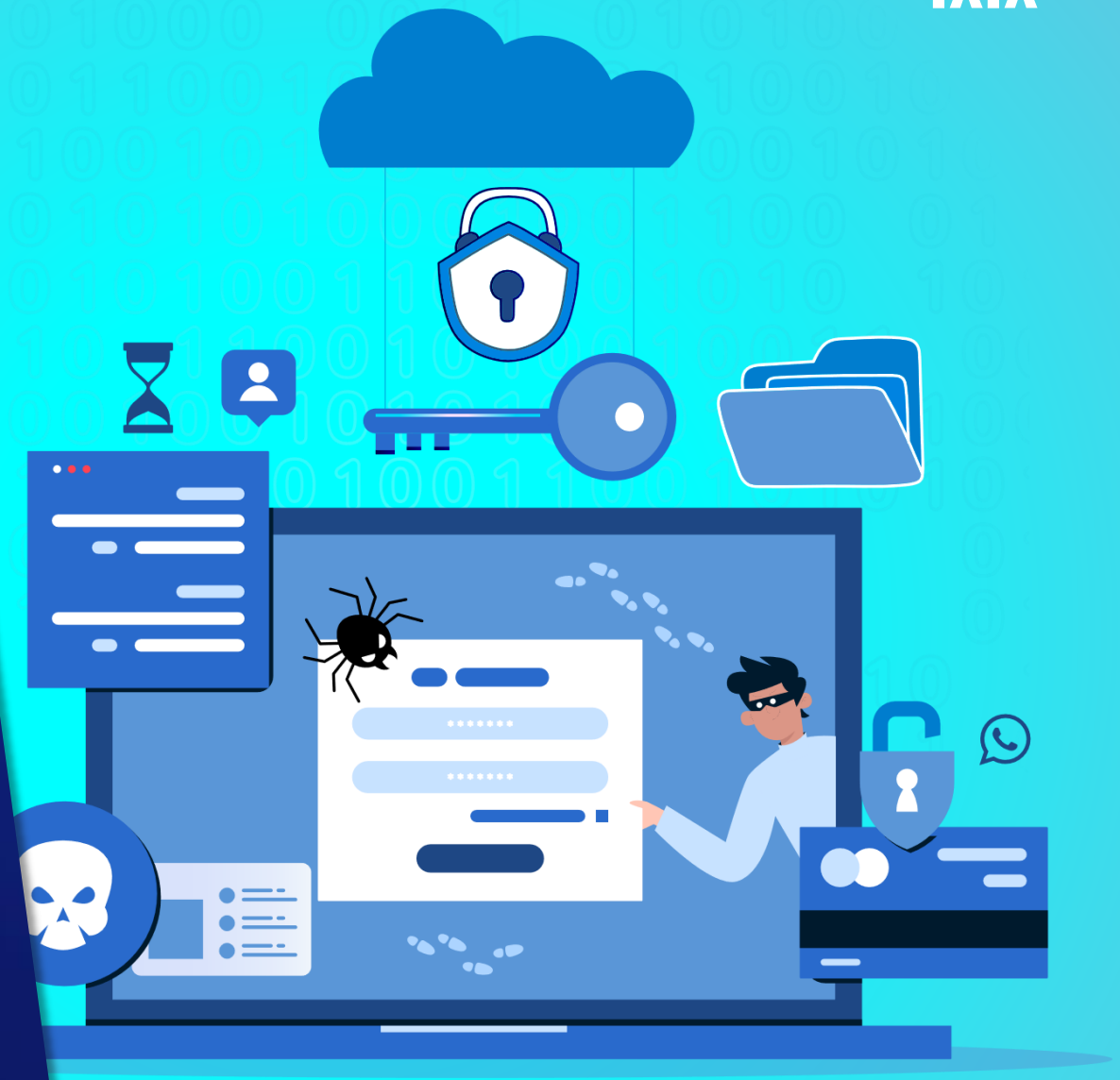
TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: August 19, 2025



TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

The fast-paced evolution at the heart of today's digital landscape has turned cybersecurity risk mitigation into a pressing priority for organisations worldwide. As these threats continue to change, companies are focusing not only on safeguarding their data but also on reinforcing the critical infrastructures that support modern business operations. The aim is to develop resilience against an ever-widening array of emerging dangers.

Boost your organisation's cybersecurity preparedness with Tata Communications' weekly threat intelligence advisory. Access critical updates on the latest cyber threats and adopt proactive measures to fortify your defences, effectively reducing potential vulnerabilities.

Advance Pakistan-linked phishing campaign bypasses MFA security

A sophisticated phishing campaign, possibly orchestrated by Pakistan-linked APT36 (Transparent Tribe), has targeted Indian defence and government organisations via typo-squatted domains resembling official government portals. The attackers employ advanced social engineering and real-time harvesting of both passwords and Kavach one-time passwords (OTPs), thereby circumventing multi-factor authentication. Infrastructure investigation highlights connections to Pakistani IP addresses and potential staging via Zah Computers, raising serious national security concerns.

The counterfeit sites replicate official visual elements—logos, layout and titles—to deceive users into entering credentials and Kavach codes, which are then transmitted over encrypted channels to external command-and-control servers. The campaign leverages legitimate cybersecurity reporting addresses to bolster authenticity and reduce suspicion. If successful, such tactics could enable unauthorised access to sensitive systems and expose classified data.

ATTACK TYPE	Malware	**SECTOR**	Government
REGION	India	**APPLICATION**	Windows

Source - https://www.cyfirma.com/research/apt36-a-phishing-campaign-targeting-indian-government-entities/

TATA COMMUNICATIONS

Akira ransomware exploits firewall vulnerability for access

Since mid-July 2025, a wave of Akira ransomware attacks has been traced to SonicWall TZ and NSa-series firewalls with SSL VPN enabled, prompting speculation of a zero-day exploit bypassing multifactor authentication. Investigations by Huntress, Arctic Wolf and others indicate attackers swiftly pivot to domain controllers post-initial access. SonicWall attributes the activity to CVE-2024-40766—related to migrations from Gen 6 to Gen 7—rather than an unknown flaw.

Akira affiliates employ a “bring-your-own-vulnerable-driver” (BYOVD) technique, misusing legitimate drivers (rwdrv.sys, hlpdrv.sys) to gain kernel-level access and disable Microsoft Defender before encryption. Organisations are advised to disable SonicWall SSL VPN where feasible, restrict access via IP whitelists, enforce MFA and password hygiene, and monitor for these malicious drivers to detect or hunt related intrusion activity.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Sonicwall Firewall

Source - https://www.guidepointsecurity.com/blog/gritrep-akira-sonicwall/

TATA COMMUNICATIONS

Makop ransomware exploits remote desktop protocol vulnerabilities

Makop ransomware incidents in South Korea have increasingly exploited Remote Desktop (RDP) services as a primary access point, leveraging brute-force and dictionary attacks against weak credentials. Once access is achieved, operators deploy credential-theft utilities drawn from NirSoft and Mimikatz to harvest passwords and scan internal networks. These techniques enable lateral movement and deeper compromise before final encryption efforts are launched—raising serious security concerns.

The attackers encrypt files—typically using AES-256 and RSA-1024—before disabling recovery mechanisms by deleting backups and terminating critical processes. The threat also leaves ransom notes and alters desktop backgrounds to prompt payment. Mitigation recommendations include disabling unused RDP services, enforcing strong authentication, improving access control, and implementing continuous monitoring to detect both initial intrusion attempts and subsequent internal reconnaissance.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	South Korea	**APPLICATION**	Windows

Source - https://asec.ahnlab.com/ko/89365/

Storm-2603 deploy custom ransomware via SharePoint

An actively identified exploit chain, dubbed “ToolShell,” is actively targeting unpatched Microsoft SharePoint servers via four vulnerabilities (CVE-2025-49706, CVE-2025-49704, CVE-2025-53770, CVE-2025-53771). Threat actors associated with Storm-2603 are leveraging this chain to deploy 4L4MD4R ransomware. The attacks begin with server reconnaissance, followed by exploitation to gain persistence, exfiltrate sensitive server keys, and install web shells—facilitating full control over compromised environments.

Once access is secured, the attackers execute payload shifts and encrypt stored data, using previously compromised infrastructure to speed up operations. Observed tactics include lateral movement, privilege escalation, and the disabling of recovery mechanisms. Security teams are urged to patch vulnerable SharePoint instances immediately, reset affected credentials, rotate machine keys, and review logs for signs of unauthorised access or file encryption activity.

ATTACK TYPE	Ransomware, Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Microsoft SharePoint Server

Source - https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/#post-147463-_50343o6a6han

New ransomware campaign leverages SharePoint weaknesses

A financially motivated threat cluster tracked as CL-CRI-1040 is exploiting unpatched Microsoft SharePoint servers through the ToolShell exploit chain, previously associated with Storm-2603. The attackers deploy a bespoke toolkit called Project AK47, which includes a multi-protocol backdoor, custom ransomware dubbed AK47/X2ANYLOCK, and DLL side-loading loaders. These tools enable persistence, lateral movement, and rapid encryption, demonstrating a high degree of operational sophistication and tailored development.

Investigations indicate links between CL-CRI-1040 and a former LockBit 3.0 affiliate, as well as associations with the Warlock Client leak site. Such overlaps suggest a blurring of boundaries between ransomware-as-a-service operations and proprietary malware campaigns. The group's activity reflects an increasing convergence of advanced exploitation techniques with financially motivated cybercrime, underscoring the importance of timely patching, threat hunting, and multi-layered defence measures.

ATTACK TYPE	Ransomware, Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Microsoft SharePoint Server

Source - https://unit42.paloaltonetworks.com/ak47-activity-linked-to-sharepoint-vulnerabilities/

TATA COMMUNICATIONS

PEAR ransomware emerges as new threat

A newly identified cyber extortion group, dubbed PEAR (Pure Extraction and Ransom), surfaced in June 2025 with a distinctive non-encryption model. Instead of deploying ransomware, the operators focus on infiltrating targets via stolen or purchased credentials, conducting extensive reconnaissance, and exfiltrating sensitive data. The stolen information is archived and staged on Tor-hosted infrastructure, enabling anonymity and resilience against takedowns while preparing for subsequent extortion activity.

PEAR's extortion playbook blends data-broker tactics with double-extortion pressure, threatening victims with selective leaks, timed disclosures, or complete public dumps. The group's methods mirror those of Karakurt and BianLian, leveraging Tor servers for storage, communications, and leak site operations. By avoiding encryption, PEAR sidesteps some endpoint detection, underscoring a growing shift towards pure data-theft extortion campaigns in the ransomware ecosystem.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Manufacturing, Construction, Business
REGION	Australia , Germany , New Zealand , United States	**APPLICATION**	Windows

Source - Internal Threat Intel Research

TATA COMMUNICATIONS

GAGAKICK wreaks havoc by blending encryption and data theft

GAGAKICK ransomware has emerged as a Windows-targeting threat that encrypts files with a distinctive victim ID and the ".GAGAKICK" extension. Once deployed, it leaves a ransom note directing payment negotiations via email or messaging platforms. In addition to encryption, the operators exfiltrate sensitive information such as credentials, financial records, employee data, and manufacturing documentation, using these stolen assets to intensify extortion pressure through threats of public disclosure.

Initial infection vectors include phishing emails, cracked software, and counterfeit installers, with the ransomware leveraging Windows Management Instrumentation (WMI) for stealthy execution and persistence. Victims are advised that halting the malware's processes can prevent further encryption, though file recovery is only possible via secure backups. The campaign's dual-pronged encryption and data-theft tactics highlight the growing overlap between ransomware operations and broader cyber-espionage techniques.

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

Source - https://www.pcrisk.com/removal-guides/33487-gagakick-ransomware
https://www.linkedin.com/posts/cyfirma_cybersecurity-cyfirma-etlm-activity-7356933062556831744-4FP5/

New NoBackups ransomware group launches operations

NoBackups ransomware is a newly identified Windows-targeting strain that encrypts files, appending a unique victim ID alongside the ".nobackups" extension. A ransom note titled "README.TXT" instructs victims to initiate contact via Mailum email or Session messenger. Beyond encryption, operators engage in double extortion by stealing sensitive data and threatening public leaks, increasing the pressure on victims to meet payment demands quickly.

The ransomware uses multiple evasion and persistence tactics, including Windows Management Instrumentation (WMI) abuse, anti-debugging checks, staged payload execution, extended sleep intervals, and registry modifications. It has been observed targeting organisations across various sectors and geographies. Security experts advise maintaining offline backups, segmenting networks, and monitoring for WMI anomalies to detect early-stage activity and reduce the risk of both encryption and data exfiltration.

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

Source - https://www.cyfirma.com/news/weekly-intelligence-report-08-august-2025/ | https://www.pcrisk.com/removal-guides/33529-nobackups-ransomware#:~:text=What%20kind%20of%20malware%20is%20NoBackups%3F%20NoBackups%20is,and%20generates%20a%20ransom%20note%20%28%22%20README.TXT%20%22%29
https://www.enigmasoftware.com/pa/nobackupsransomware-hatao/

Interlock Group escalates attacks on critical sectors

Since late 2024, the hacktivist-style collective known as Interlock Group has escalated its operations with a sophisticated ransomware campaign active across North America and Europe. Their attacks initiate via compromised websites and social engineering, deploying obfuscated PowerShell scripts, PHP backdoors, and DLL payloads. These elements enable stealthy persistence, encrypted command-and-control communication, and eventual deployment of ransomware in a controlled, multi-stage compromise model.

Once established in the target environment, the group executes advanced reconnaissance and exfiltration workflows before encryption. The threat chain favours living-off-the-land techniques and dynamic command infrastructure to evade detection, achieving lateral movement and privilege escalation. Organisations are advised to exercise heightened vigilance—particular surrounding website integrity and unwelcome script execution—while reinforcing segmentation, monitoring C2 activity, and ensuring patching of web-facing assets.

ATTACK TYPE	Hacktivism, DDoS	**SECTOR**	Government, Education, Military, BFSI
REGION	Global	**APPLICATION**	Generic

Source - Internal Threat Intel Research

TATA COMMUNICATIONS

WinRAR flaw actively targeted in cyber attacks

A critical zero-day vulnerability in WinRAR (CVE-2025-8088) was actively exploited throughout July 2025 in targeted phishing campaigns, primarily against Russian organisations. The directory-traversal flaw enabled malicious archives to place executables in autorun locations—such as Windows Startup folders—triggering remote code execution and facilitating deployment of the RomCom malware family. The vulnerability was patched in WinRAR version 7.13, which users must install manually.

A related flaw, CVE-2025-6218, also affected Windows versions of WinRAR and related tools, allowing similar exploitation via crafted RAR files. Both CVEs enabled backdoor deployment using alternate data streams to evade detection. With active exploitation reported, particularly by advanced threat actors, users are advised to update to WinRAR 7.13 without delay and monitor for suspicious activity involving RAR extraction or startup-folder modifications.

ATTACK TYPE	Vulnerability, Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	WinRAR

Source - https://thehackernews.com/2025/08/winrar-zero-day-under-active.html

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