TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: August 25, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

The cyber threat landscape is evolving in August 2026, with threat actors mounting ever more sophisticated and tightly coordinated campaigns across deeply interconnected digital environments. Conventional defence models are being pushed to their limits as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now hinges on organisations reinforcing foundational security controls, adopting layered defence strategies, and weaving forward-looking intelligence into every layer of their operational frameworks.

In this fast-shifting environment, the Tata Communications Cyber Threat Intelligence report remains an indispensable resource for security practitioners. Published weekly, it offers sharp, timely analysis of emerging threat campaigns, evolving attacker methodologies, and sector-specific risk exposures. By turning intelligence into practical defence guidance, it enables security teams to anticipate, counter, and contain threats with confidence — safeguarding the continuity of critical operations at scale.

TATA COMMUNICATIONS

CISA warn of Gunra ransomware exploiting known firewall authentication bypass flaws

A joint advisory from CISA, the FBI, NSA, US Secret Service, DC3 and South Korea's National Police Agency has warned of Gunra, a Conti-derived ransomware-as-a-service operation using a double-extortion model. The group gains initial access by exploiting two known Fortinet authentication bypass flaws, CVE-2024-55591 and CVE-2025-24472, in internet-facing FortiOS and FortiProxy appliances to obtain administrative privileges.

Once inside, Gunra affiliates steal credentials, move laterally, and in some cases alter authentication files to persistently bypass multi-factor authentication. They then exfiltrate data before deploying ransomware across both Windows and Linux environments, negotiating through a Tor-based portal. Organisations are urged to patch the affected Fortinet appliances immediately, enforce phishing-resistant MFA and maintain offline, immutable backups.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, BFSI, Manufacturing, Construction, Government, Transportation, Retail and Distribution, Logistics and Shipping
REGION	Middle East, Europe, Africa, Canada, Japan, Brazil, Egypt, South Korea, Taiwan, Turkey, United States, APAC	**APPLICATION**	Microsoft Active Directory Services, Fortinet FortiClient SSL VPN, OneDrive, Windows, Linux, FortiOS

Source - https://thehackernews.com/2026/08/gunra-ransomware-exploits-fortinet-and.html

TATA COMMUNICATIONS

Weaxor ransomware hijacks SQL Server for high-privilege command execution and stealth

An analysis of a Weaxor ransomware intrusion reveals how attackers abused Microsoft SQL Server for high-privilege command execution. From there, the chain unfolded through obfuscated PowerShell, an AMSI bypass and Cobalt Strike Beacon staging. Using dynamic API resolution and executing from RWX memory, the operators kept much of their activity in memory to evade traditional detection tools.

The attack then injected code into the legitimate SQLPS.exe process before deploying a ChaCha20-based encryptor and clearing Windows event logs to reduce forensic visibility. Weaxor, a rebranded successor to Mallox, typically compromises exposed SQL Server instances through weak credentials. Organisations are urged to enforce strong passwords, restrict internet-facing database access and closely monitor for anomalous PowerShell activity.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Microsoft SQL Server, Windows, PowerShell

Source - https://labs.k7computing.com/index.php/when-sql-server-becomes-the-initial-launcher-a-deep-dive-into-weaxor-ransomware-execution/

TATA COMMUNICATIONS

DeadLock adopts decentralised infrastructure to resist disruption and evade detection

DeadLock is a financially motivated ransomware operation that pairs double extortion with a decentralised recovery infrastructure designed to resist law enforcement takedowns. Rather than relying on a traditional Tor site, its victim-facing application queries a Polygon blockchain smart contract to retrieve the current proxy address. Operators can rotate this address on-chain without altering the malware itself.

Victim communications are routed through the decentralised Session network, while stolen data is hosted on Wasabi cloud storage for leak operations. The Windows encryptor adds resource-aware encryption, language-based geofencing, security tool disruption, log tampering and self-deletion. Observed intrusions leveraged stolen credentials, AnyDesk, RDP and a vulnerable Baidu driver. Microsoft stresses that maintaining immutable backups remains the strongest defence.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Manufacturing, Transportation, Hospitality, Mining, Logistics and Shipping
REGION	North America, South America, Europe, Africa, Asia	**APPLICATION**	Microsoft Windows Defender, AnyDesk, PuTTY, Windows, Microsoft OneDrive, PowerShell, Google Drive

Source - https://www.bleepingcomputer.com/news/security/deadlock-ransomware-uses-blockchain-to-resist-infrastructure-takedown/

TATA COMMUNICATIONS

Indian sectors face rising wave of DDoS attacks, defacements, and ransomware incidents

Recent intelligence points to a sustained rise in cyber threat activity targeting Indian organisations, spanning DDoS attacks, website defacements, data breach claims, unauthorised access sales and ransomware incidents. Both ideologically driven hacktivist collectives and financially motivated criminal actors are involved, often coordinating across borders and blending disruptive tactics with propaganda to maximise reputational and operational impact against their chosen targets.

Targeted sectors include government, healthcare, education, banking, defence and technology, leaving public-facing and critical infrastructure organisations especially exposed. Activity has intensified around nationally significant dates, with multiple groups claiming attacks in quick succession. Organisations are urged to harden internet-facing assets, strengthen DDoS mitigation and monitoring, patch known vulnerabilities promptly and rehearse incident response plans to sustain operational resilience.

ATTACK TYPE	Hacktivism, DDoS	**SECTOR**	Healthcare, Manufacturing, IT, Government, Transportation, Education, E-Commerce, Law, BFSI, Hospitality, Telecommunications
REGION	India	**APPLICATION**	Apple macOS, Windows, Linux

Source - CTI Team Internal Research

TATA COMMUNICATIONS

Akira affiliate disables endpoint protection using safe mode reboot during VPN intrusion

An Akira ransomware affiliate breached a network through an exposed SonicWall SSL VPN that lacked multi-factor authentication, gaining entry via credential spraying. The operator then used RDP to reach the domain controller, enumerated Active Directory, and archived mapped file shares with WinRAR. Stolen data was exfiltrated to an attacker-controlled S3 bucket using the high-speed s5cmd transfer utility.

Before detonation, the attacker installed AnyDesk for persistence and rebooted the host into Safe Mode with Networking to disable EDR and Microsoft Defender. The tactic neutralised defences but backfired: the stripped-down memory environment triggered virtual memory failures that crashed the encryptor within seconds. Huntress urges organisations to enforce MFA on all VPN accounts and monitor Safe Mode boot changes.

ATTACK TYPE	Ransomware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Windows Defender, Windows, PowerShell, Notepad

Source - https://securityaffairs.com/197339/malware/akira-ransomware-uses-safe-mode-to-bypass-edr.html

TATA COMMUNICATIONS

Japanese MAJINAHANASHI operation locks files and wipes backups to pressure its victims

First observed in August 2026, MAJINAHANASHI is a newly identified, Japanese-themed ransomware operation that runs a Tor-based data leak site alongside separate archive servers. The malware encrypts victims' files using AES-256, appends the .MAJIN extension, and relies on an embedded RSA public key to wrap each per-file encryption key, ensuring only the attackers can restore access.

Before encryption, the ransomware disables recovery mechanisms, terminates security and backup processes, clears event logs, and performs language and geographic checks to select its targets. It also applies network-control measures during execution to evade detection. Early victims span retail, manufacturing, agriculture, technology and healthcare, with initial access often traced to credentials stolen by infostealers. Multi-factor authentication remains a key defence.

ATTACK TYPE	Ransomware, Emerging Threats	**SECTOR**	IT, Manufacturing, Services, E-Commerce
REGION	India, Bulgaria, Chile, Colombia, France, Germany, Lithuania, Portugal, Switzerland, Thailand	**APPLICATION**	Microsoft Windows Defender, Windows, Qualys, SentinelOne, Veeam

Source - https://theravenfile.com/2026/08/14/majinahanashi-ransomware-another-japanese-locker/

TATA COMMUNICATIONS

Fake VPN installers deliver undocumented PATCHCORD backdoor to telecom infrastructure

Threat Research Unit has uncovered an ongoing espionage campaign delivering a previously undocumented backdoor named PATCHCORD against Afghan telecom providers and South Asian critical infrastructure. The compiled C/C++ implant spreads through sector-specific lures, including fake VPN installers impersonating Afghan Telecom and telecom management tools. Researchers assess with moderate confidence that the activity overlaps with the APT36 (Transparent Tribe) cluster.

Infrastructure pivoting revealed two related implants: SHEETCORD, a Go-based backdoor abusing Google Sheets for command-and-control, and the HACKERAI C2 Agent, which leverages GitHub Gists. The malware employs browser shortcut hijacking, registry and Startup folder persistence, remote command execution, process discovery and in-memory shellcode execution. Organisations should verify software through official channels and monitor for anomalous cloud-service traffic.

ATTACK TYPE	Cyber-espionage, APT	**SECTOR**	Government, Energy, Defence, Telecommunications
REGION	India, Afghanistan, South Asia	**APPLICATION**	Microsoft Edge, Mozilla Firefox, Opera Browser, Windows, Google Chrome, PowerShell, GitHub

Source - https://www.acronis.com/en/tru/posts/patchcord-new-malware-cluster-targets-afghan-telecom-and-south-asian-critical-infrastructure/

TATA COMMUNICATIONS

Unauthenticated attackers hijack WordPress admin accounts via plugin security flaws

Wordfence has disclosed two critical vulnerabilities affecting widely used WordPress plugins. The first, an unrestricted file upload flaw in Simple File List (CVE-2020-36847, CVSS 9.8), allows unauthenticated attackers to upload malicious files and execute arbitrary code. The second, an authentication bypass in User Profile Builder (CVE-2026-15826, CVSS 9.8), can let unauthenticated attackers log in as the site administrator.

The User Profile Builder flaw stems from a type of confusion error in the plugin's registration and automatic-login flow and is exploitable only where the 'Automatically Log In after Registration' setting is enabled. It affects versions up to and including 3.16.4, resolved in 3.16.5. Administrators are urged to update both plugins promptly and audit sites for unauthorised administrator accounts.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	WordPress

Source - https://www.wordfence.com/blog/2026/08/40000-wordpress-sites-affected-by-authentication-bypass-vulnerability-in-user-profile-builder-wordpress-plugin/

TATA COMMUNICATIONS

Microsoft patches SharePoint flaw enabling remote code execution on enterprise servers

Microsoft has disclosed CVE-2026-63520, a high-severity remote code execution vulnerability affecting all supported versions of SharePoint Server, alongside certain Project Server and Office Web Apps Server deployments. The flaw stems from improper input validation in Business Connectivity Services, permitting arbitrary code execution through unsafe .NET type instantiation under the SharePoint site's service account privileges.

Rated 8.1 on the CVSS scale, the flaw requires an authenticated session on its own. However, when chained with CVE-2026-55040, a SharePoint JWT authentication bypass patched in July, attackers can achieve fully unauthenticated remote code execution against internet-facing servers. Microsoft addressed the flaw in its August updates, and administrators are urged to apply both patches without delay.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, BFSI, Manufacturing, IT, Government, Education
REGION	Global	**APPLICATION**	Microsoft SharePoint Server, Microsoft Windows SharePoint Services, Microsoft Office 365

Source - https://gbhackers.com/microsoft-sharepoint-rce-vulnerability/

TATA COMMUNICATIONS

Hackers exploit internet-facing applications to deploy stealthy fileless SNOWLIGHT malware

Researchers have uncovered an exposed adversary-controlled staging server that revealed a sweeping campaign linked to the SNOWLIGHT malware family and China-nexus access brokers UNC5174 and UNC6586. Active between late April and early June 2026, the operation targeted government and commercial infrastructure across more than 100 countries, with over 85% of reconnaissance focused on government domains.

The attackers combined automated reconnaissance and weaponised vulnerabilities with a cracked Chinese reimplementation of Cobalt Strike, Metasploit, tunnelling utilities and multi-platform loaders. Confirmed compromises involved exploiting internet-facing applications, deploying web shells, harvesting credentials and executing fileless SNOWLIGHT across Linux and Windows systems. Organisations are urged to patch public-facing services promptly and monitor for the published indicators of compromise.

ATTACK TYPE	Cyber-espionage, APT	**SECTOR**	Healthcare, Government, Education
REGION	Global	**APPLICATION**	Microsoft Exchange Server, Atlassian Confluence, Windows, Linux, F5 BIG-IP, Apache Tomcat, Laravel, Apache Struts 2 , cPanel and WHM

Source - https://socradar.io/blog/snowlight-government-chinese-campaign/

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