TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: September 8, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As September 2026 progresses, the cyber threat landscape continues to accelerate, with threat actors launching ever more sophisticated and tightly coordinated campaigns across deeply interconnected digital environments. Traditional defence models are buckling under pressure as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now depends on organisations strengthening foundational security controls, adopting layered defence strategies, and threading forward-looking intelligence through every layer of their operational frameworks.

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

TATA COMMUNICATIONS

Iranian APT Tortoiseshell expands operations using reverse SSH tunnels and TWOSTROKE

Researchers have uncovered new malware, infrastructure and activity linked to the Iranian state-aligned group Tortoiseshell, also tracked as Mirage Kitten, UNC1549 and Nimbus Manticore. Enriching previously reported indicators, they identified a reverse SSH tunnelling utility that redirects traffic from command-and-control servers into compromised networks, alongside continued use of the TWOSTROKE backdoor family first documented in late 2025.

The C++ backdoor masquerades as the legitimate wtsapi32.dll and is loaded through DLL search-order hijacking, communicating with hardcoded servers over HTTPS while decrypting sensitive strings at runtime. The expanded infrastructure spans Europe and the Middle East, pointing to broader regional targeting and sustained espionage. Organisations are urged to monitor for the published indicators and hunt for suspicious DLL sideloading.

ATTACK TYPE	Malware, Cyber-espionage, APT	**SECTOR**	Government, Military, Aerospace, Defence Industry
REGION	Middle East, Australia, Europe, Canada, Japan, UK, Belgium, Saudi Arabia, UAE, United States	**APPLICATION**	Windows, OpenSSH

Source - https://www.infosecurity-magazine.com/news/tortoiseshell-new-backdoor-ssh/

TATA COMMUNICATIONS

Unauthenticated attackers can hijack WordPress sites through critical Avada and Pods flaws

Two critical vulnerabilities have been disclosed across popular WordPress components, each carrying a CVSS score of 9.8. CVE-2026-18431 is an arbitrary file write flaw in the Avada theme and its required Fusion Builder plugin, which unauthenticated attackers can chain through six steps to write and execute malicious PHP, achieving remote code execution and complete site compromise.

The second flaw, CVE-2026-19598, is a privilege escalation vulnerability in the Pods plugin, letting unauthenticated attackers gain administrator rights or reset any user's password, including the site owner's. Avada versions up to 7.16 and Fusion Builder up to 3.16 are affected, alongside Pods up to 3.3.9. Administrators should update all affected components to their latest patched versions immediately.

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/wordfence-argus-finds-complex-6-step-critical-rce-in-avada-theme-with-1-million-sales/

TATA COMMUNICATIONS

Oracle urges immediate patching as critical WebLogic flaws threaten full server compromise

Oracle has released its August 2026 Critical Security Patch Update, addressing multiple vulnerabilities in Oracle WebLogic Server. Four critical flaws — CVE-2026-60672, CVE-2026-60696, CVE-2026-60698 and CVE-2026-60977, each rated CVSS 9.8 — could allow unauthenticated network attackers to compromise or fully take over affected servers through the T3, IIOP or RMI protocols, all long-standing WebLogic deserialization attack surfaces.

The affected releases span WebLogic Server versions 12.2.1.4.0 through 15.1.1.0.0. The update also resolves HTTP-based access-control weaknesses and several earlier WebLogic vulnerabilities. Given WebLogic's history of rapid post-patch exploitation, administrators should apply the fixes immediately. Where patching must be delayed, they should block external access to admin ports 7001 and 7002 and restrict T3 and IIOP at the perimeter.

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

Source - https://www.cert.ssi.gouv.fr/avis/CERTFR-2026-AVI-1053/

TATA COMMUNICATIONS

Misconfigured RADIUS exposes FortiWeb apps to unauthorised remote admin takeover

CERT-In has issued vulnerability note CIVN-2026-0424, addressing a high-severity improper authentication flaw in Fortinet FortiWeb. Tracked as CVE-2026-26035 with a CVSS score of 8.8, the vulnerability allows a remote unauthenticated attacker to log in to the FortiWeb GUI or CLI using a random username and password, granting full administrative access to the appliance.

The flaw only affects deployments where a Remote RADIUS type administrator account is configured with the non-default wildcard setting enabled. Fortinet has released fixes in FortiWeb versions 8.0.3, 7.6.7, 7.4.12 and 7.2.13, and advises disabling the wildcard option as a workaround. No active exploitation had been reported at disclosure, though prompt patching is strongly recommended.

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

Source - https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2026-0424

TATA COMMUNICATIONS

Allied hacktivist groups join forces to disrupt Indian government and public services

Throughout August 2026, two hacktivist groups — RBL Leviathan Ghost and Cyber Team Indonesia — maintained sustained activity against Indian organisations under the “OpIndia” campaign. Targeted sectors spanned government, education, law enforcement, aviation, healthcare and the wider public sector. RBL Leviathan Ghost focused primarily on distributed denial-of-service attacks and website disruption, claiming outages across several government portals during the period.

Cyber Team Indonesia demonstrated a broader repertoire, combining denial-of-service attacks with website defacement and alleged data breach or leak activity. Publicly shared sources also point to a reported alliance between the two groups within the wider campaign, which is driven by ideological and retaliatory motives. Organisations are advised to strengthen DDoS mitigation, monitor for defacement and verify any leak claims.

ATTACK TYPE	Hacktivism, DDoS	**SECTOR**	Healthcare, Public Health, Government, Transportation, Education, Military, Law, Aviation, IT Services and Consulting
REGION	India	**APPLICATION**	Apple macOS, Windows, Linux

Source- CTI Team Internal Research

TATA COMMUNICATIONS

Aurora blends helpdesk vishing, AI assistance, and targeted hypervisor encryption attacks

Aurora ransomware has been observed conducting multi-stage intrusions that begin with email bombing followed by vishing, in which operators impersonate IT helpdesk staff to gain remote access via the open-source Xray-core utility. From there, attackers move laterally across the network, compromise Active Directory, harvest credentials, disable Microsoft Defender, clear logs, and exfiltrate sensitive data before deploying their encryptors.

The operators maintain persistence through scheduled tasks and Registry Run keys, alongside extensive anti-forensic measures. Recent investigations identified victim-specific lockers, a custom Linux encryptor targeting VMware ESXi environments, AI-assisted attack planning and ransom payments tied to broader laundering infrastructure. Organisations are urged to harden Active Directory, restrict ESXi and remote administration access, and secure backups against tampering.

ATTACK TYPE	Ransomware	**SECTOR**	BFSI, Pharmaceuticals, Waste Disposal, Manufacturing, IT, F&B Service, Retail and Distribution, Logistics and Shipping
REGION	Canada, UK, Germany, Netherlands, United States	**APPLICATION**	Microsoft Windows Defender, Microsoft Active Directory Services, VMware ESXi, PowerShell, Veeam

Source - https://cyberpress.org/aurora-uses-cursor-ai/

TATA COMMUNICATIONS

Chinese TA4922 threat group uses tax-themed phishing to spread a modular PackClient RAT

Cyber researchers have identified PackClient, a modular remote access trojan and command-and-control framework marketed through Chinese-language Telegram channels and deployed by the financially motivated, Chinese-speaking threat actor TA4922. Observed in May and July 2026, the campaigns targeted organisations in mainland China and India using tax-themed lures that impersonated the Shandong Provincial Tax Bureau and the Indian Income Tax Department.

Victims received ZIP archives containing executables or IMG disk images, with payloads deployed through DLL sideloading and staged loaders before PackClient was installed. The framework supports persistence, surveillance, keylogging, credential theft, remote access, plugin deployment, proxy tunnelling and data collection, making it suitable for espionage or fraud. Organisations should reinforce email security and train staff to scrutinise unexpected tax-related attachments.

ATTACK TYPE	Malware	**SECTOR**	Government, BFSI
REGION	India, Asia, China	**APPLICATION**	Windows, Telegram

Source - https://cyberpress.org/ta4922-hackers-use-tax-phishing/

TATA COMMUNICATIONS

Multi-language SynkLoader malware spreads via Teams phishing to enable intrusions

Researchers have identified SynkLoader, a previously undocumented modular malware framework distributed through Microsoft Teams phishing messages in which attackers impersonate the IT helpdesk staff. Victims are lured into installing a fake PowerShell Cleaner MSI hosted on Microsoft Azure. The framework unusually blends PowerShell, Python, C# and C++ across its components, using multi-stage in-memory execution to evade endpoint detection.

A Python-based loader bridges these languages and retrieves further modules on demand. These provide system profiling, persistence via scheduled tasks, reverse-proxy tunnelling, remote PowerShell shells and VNC control, enabling hands-on-keyboard intrusions. A standout component, PhishLocker, mimics the Windows lock screen to capture passwords directly. Organisations should treat unsolicited Teams IT-support requests with caution and block untrusted MSI installations.

ATTACK TYPE	Malware	**SECTOR**	IT
REGION	Global	**APPLICATION**	Python, Microsoft Office 365, Microsoft Teams, Microsoft Azure

Source - https://www.bleepingcomputer.com/news/security/new-synkloader-malware-pushed-in-microsoft-teams-phishing-campaign/

TATA COMMUNICATIONS

Popular npm code generation package poisoned by credential-stealing supply chain worm

Attackers compromised the npm package @7nohe/openapi-react-query-codegen on 28 August 2026, publishing ten malicious versions across every maintained release branch in under twenty-one minutes. The incident exploited a flaw in the project's GitHub Actions workflow where an unsecured issue_comment trigger allowed any GitHub user to initiate a publish simply by commenting on a pull request, with no stolen credentials required.

The malicious releases were triggered through preinstall hooks and an obfuscated binding.gyp file was executed even when package scripts were disabled. After downloading Bun 1.4.0, the payload harvested cloud, Kubernetes, Vault and registry credentials, then propagated to npm, RubyGems and PyPI. Affected releases carried valid npm provenance. Developers who installed any compromised version should rotate all credentials immediately from a clean machine.

ATTACK TYPE	Supply Chain	**SECTOR**	IT
REGION	Global	**APPLICATION**	Microsoft Windows Defender, Kubernetes, VS Code, SentinelOne, Microsoft Azure, CrowdStrike, AWS, npm, PyPI, GitHub

Source - https://safedep.io/mini-shai-hulud-openapi-react-query-codegen-compromised

TATA COMMUNICATIONS

DARKLANTERN and SPEAKINGSTONE routers found with covert factory-installed backdoor

Security researchers have disclosed two previously undocumented implants, DARKLANTERN and SPEAKINGSTONE, embedded in firmware shipped with ZBT-manufactured routers and white-labelled variants distributed globally. DARKLANTERN listens on UDP port 9992 with no authentication required. The router's default firewall explicitly permits inbound traffic to this port, giving any remote attacker a root shell with a single packet.

SPEAKINGSTONE takes a different approach, beaconing outbound over UDP to a hardcoded command-and-control server. It supports arbitrary command execution, credential theft, DNS hijacking and reverse SSH tunnelling, with all communications in plaintext. VulnCheck detected 203 internet-facing DARKLANTERN instances across 22 countries in late August 2026. Organisations are urged to audit hardware and replace affected devices promptly.

ATTACK TYPE	Malware	**SECTOR**	Transportation, Business, Retail and Distribution, Telecommunications
REGION	Australia, Canada, Russia, China, Germany, Israel, Philippines, Taiwan, Ukraine, United States, Hong Kong	**APPLICATION**	Linux

Source - https://cyberveille.ch/posts/2026-08-29-endlessdoors-backdoor-d-usine-dans-les-routeurs-zbtlink-root-shell-non-authentifie/

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