TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: June 16, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As June 2026 progresses, the cyber threat landscape shows no sign of abating, with threat actors deploying increasingly sophisticated and coordinated tactics across highly interconnected digital environments. Conventional defence models continue to be tested as adversaries exploit systemic vulnerabilities at scale. Organisations must reinforce foundational security controls, adopt layered defence strategies, and embed forward-looking intelligence into operational frameworks to sustain resilience and competitive advantage.

Against this backdrop, the Tata Communications Cyber Threat Intelligence report remains an essential resource for security practitioners. Published weekly, it delivers incisive analysis of emerging threat campaigns, evolving attacker methodologies, and sector-specific risk exposures. By translating intelligence into actionable defence guidance, it equips security teams to anticipate, respond to, and mitigate threats effectively, safeguarding the continuity of critical operations at scale.

TATA COMMUNICATIONS

Unauthenticated attackers exploit WordPress plugin flaw to create rogue admin accounts

A critical vulnerability in the WP Maps Pro WordPress plugin, affecting all versions up to 6.1.0, allows unauthenticated attackers to create administrator accounts and achieve full site takeover. The flaw originates in a vendor support feature whose AJAX endpoint was publicly accessible; its nonce-based protection was ineffective as the nonce value was embedded in every frontend page served to visitors.

Active exploitation was confirmed shortly after disclosure, with Wordfence recording over 2,000 attacks within 24 hours. The vulnerability affects a commercial plugin distributed through the Envato Market, where slower update cycles leave a significant portion of installations exposed. Version 6.1.1, which fixes the flaw by restricting the vulnerable endpoint to authenticated administrators, was released on 20 May 2026.

ATTACK TYPE	Vulnerability	**SECTOR**	Business and E-commerce
REGION	Global	**APPLICATION**	WordPress

Source - https://securityaffairs.com/192977/hacking/cve-2026-8732-the-wp-maps-pro-flaw-that-lets-anyone-create-a-wordpress-admin-without-a-password.htmlv

TATA COMMUNICATIONS

Scripted destruction campaign wipes virtualisation and backup infrastructure across sectors

Analysts at Gambit Security linked Ababil of Minab to Black Shadow, an Iran-affiliated group attributed to Iran's Ministry of Intelligence and Security. Surfacing in late March 2026, the campaign targeted transportation, media, and education organisations. Attackers combined scripted automation with hands-on keyboard techniques to delete virtual machines, wipe storage volumes, and destroy databases, leaving victims no path to recovery.

Beyond destruction, investigators uncovered two bespoke exfiltration tools: a method uploading stolen files to victim-controlled websites before retrieval, and FileFiend, a custom C++ tool forwarding data to a hardcoded command-and-control server. Notably, an attacker used an AI chatbot to refine a purpose-built destruction script, adding a deeply concerning new dimension to state-linked offensive cyber operations.

ATTACK TYPE	Malware, Cyber-espionage	**SECTOR**	IT, Transportation, Education, Broadcast Media Production and Distribution
REGION	Middle East, Europe, Israel, the United States	**APPLICATION**	Microsoft Internet Information Services (IIS), VMware vCenter Server, Windows, Veeam, Veeam Backup Enterprise Manager

Source - https://industrialcyber.co/industrial-cyber-attacks/gambit-links-iran-linked-black-shadow-group-to-destructive-cyber-campaign-targeting-us-middle-east-organizations/

TATA COMMUNICATIONS

DriveSurge threat delivers fake browser updates and ClickFix across compromised sites

A critical vulnerability in the WP Maps Pro WordPress plugin, affecting all versions up to 6.1.0, allows unauthenticated attackers to create administrator accounts and achieve full site takeover. The flaw originates in a vendor support feature whose AJAX endpoint was publicly accessible; its nonce-based protection was ineffective as the nonce value was embedded in every frontend page served to visitors.

Active exploitation was confirmed shortly after disclosure, with Wordfence recording over 2,000 attacks within 24 hours. The vulnerability affects a commercial plugin distributed through the Envato Market, where slower update cycles leave a significant portion of installations exposed. Version 6.1.1, which fixes the flaw by restricting the vulnerable endpoint to authenticated administrators.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, IT, E-Commerce
REGION	Global	**APPLICATION**	Apple macOS, Windows

Source - https://www.silentpush.com/blog/drivesurge/

TATA COMMUNICATIONS

Public exploit code heightens urgency around Cisco Unified CM SSRF vulnerability

Cisco has patched CVE-2026-20230, a high-severity SSRF vulnerability in Unified Communications Manager and Unified CM SME, carrying a CVSS score of 8.6. The flaw arises from improper HTTP request input validation and can be exploited remotely without authentication when the WebDialer service is enabled, allowing attackers to write files to the underlying operating system and subsequently escalate privileges to root.

Cisco released Unified CM and Unified CM SME version 14SU6 to remediate the vulnerability, with further patches expected in version 15SU5 due in September 2026. The company has acknowledged that proof-of-concept exploit code is publicly available, though no active exploitation has been confirmed. Concurrently, Cisco also addressed two medium-severity XSS vulnerabilities in Webex Meetings and Finesse.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, BFSI, IT, Government, Education, Business, Aviation, Automobile, Broadcast Media Production, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Cisco Unified Communications Domain Manager, Cisco Unified Operations Manager

Source - https://www.securityweek.com/cisco-warns-of-available-poc-for-critical-unified-cm-vulnerability/

TATA COMMUNICATIONS

Active exploitation of RCE vulnerability found in Everest Forms Pro WordPress plugin

A critical remote code execution flaw, CVE-2026-3300 (CVSS 9.8), has been identified in Everest Forms Pro, affecting versions 1.9.12 and earlier. The vulnerability resides in the plugin's complex calculation feature, where the process_filter() function passes submitted field values directly to PHP's eval() without adequate sanitisation, enabling unauthenticated attackers to inject arbitrary PHP code and achieve full server compromise.

Active exploitation has been observed since April 2026, with Wordfence reporting over 17,900 blocked exploit attempts on 16 May 2026 alone. The most prevalent payload targets the creation of a rogue administrator account to establish persistent backdoor access. A patch is available in version 1.9.13; administrators are advised to update immediately and audit user profiles for unauthorised accounts.

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

Source - https://securityonline.info/everest-forms-pro-flaw-active-exploitation/

TATA COMMUNICATIONS

State-sponsored Red Lamassu threat actor targets firms with JFMBackdoor campaign

Threat Intelligence has tracked Red Lamassu, also known as Calypso APT, since 2019, observing its targeting of telecommunications and government entities across the Asia-Pacific region. Researchers identified an exposed open directory hosted between July and October 2025, containing Linux malware alongside a fully featured Windows backdoor, JFMBackdoor, delivered via DLL side-loading through a legitimate executable.

JFMBackdoor supports an extensive command set covering remote shell access, file system operations, screenshot capture, registry manipulation, process management, network proxying, and self-removal for anti-forensic purposes. The malware communicates with its command-and-control infrastructure via multiple Cloudflare-obfuscated domains, enabling operators to dynamically update its behaviour and maintain a persistent, covert foothold within targeted telecommunications environments globally.

ATTACK TYPE	Malware, Cyber-espionage, APT	**SECTOR**	Government, Telecommunications
REGION	India, Afghanistan, Kazakhstan, Thailand, APAC	**APPLICATION**	Windows, Linux, PowerShell

Source - https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/red-lamassu-open-season.html

TATA COMMUNICATIONS

TaxShadow operation delivers in-memory malware via government tax authority lures

Operation TaxShadow has been active since at least 20 May 2026, targeting Windows users through phishing emails impersonating official tax authorities. Urgency-driven messaging threatening financial penalties redirects victims to convincingly crafted multilingual phishing sites complete with official logos and bilingual content. Victims are prompted to download a ZIP archive containing staged malware payloads designed to evade conventional security detection.

The malware employs DLL search order hijacking to load a malicious DLL, followed by API hooking and token manipulation to strip permission barriers. The final payload, encrypted with a mutated RC4 cipher, loads directly into memory via Reflective PE Loading, leaving no trace on disk. Command-and-control communications are routed through WebSocket connections, enabling traffic to blend with legitimate application activity.

ATTACK TYPE	Malware	**SECTOR**	Government, Business, BFSI
REGION	India, Japan	**APPLICATION**	Windows

Source - https://ransom-isac.org/blog/shinyhunters-silent-maas/

TATA COMMUNICATIONS

High-severity HTTP/2 flaw (CVE-2026-49975) enables memory exhaustion DoS attacks

Security firm Calif publicly disclosed full details and a proof-of-concept exploit for CVE-2026-49975, a high-severity HTTP/2 vulnerability dubbed HTTP/2 Bomb. The flaw chains HPACK header compression abuse with a Slowloris-style hold, enabling remote unauthenticated attackers to force excessive memory allocation on targeted servers. The attack bypasses standard volume-based defences, as amplification stems from per-entry bookkeeping rather than oversized payload headers.

Researchers confirmed that a single attacker can consume and hold 32GB of server memory in approximately 20 seconds against Apache httpd and Envoy. A zero-byte flow-control window maintains memory pressure indefinitely by preventing connection timeouts. Shodan data indicates over 880,000 public web portals remain exposed, whilst Microsoft IIS, Envoy, and Cloudflare Pingora have yet to receive formal security patches.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Internet Information Services (IIS), Apache Software Foundation Apache HTTP Server, NGINX

Source - https://securityonline.info/http2-bomb-exploit-poc-disclosed/

TATA COMMUNICATIONS

SRG Social Engineering escalates law firm attacks with in-person data theft tactics

The FBI issued a flash alert on 26 May 2026, warning that SRG — also tracked as Luna Moth, Chatty Spider, and UNC3753 — has consistently targeted law firms since Spring 2023. Unlike conventional ransomware actors, the group forgoes file encryption entirely, focusing instead on rapid data exfiltration and threatening public disclosure of stolen records to extort victims.

As of Spring 2026, SRG actors impersonate IT staff through phishing emails and direct calls, directing employees to grant remote desktop access using legitimate tools such as Quick Assist and Rclone to exfiltrate sensitive data. If unsuccessful, operatives are dispatched physically to the victim's premises, inserting a storage device into a computer — a highly unusual escalation in criminal tradecraft.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, BFSI, Legal Services
REGION	United States	**APPLICATION**	AnyDesk, Windows, WinSCP, Microsoft OneDrive, Google Drive

Source - https://www.bleepingcomputer.com/news/security/fbi-warns-of-silent-ransom-group-in-person-data-theft-attacks/

TATA COMMUNICATIONS

Self-spreading Shai-Hulud worm spawns Hades variant to attach to developer supply chains

The Hades campaign — the PyPI branch of the Mini Shai-Hulud and Miasma supply chain lineage — distributed 37 malicious wheel artefacts across 19 packages on the Python Package Index. Abusing legitimate Python *-setup.pth startup files, the malware executed automatically at interpreter startup, bootstrapping the Bun JavaScript runtime to deploy a heavily obfuscated credential-stealing payload without explicit package import.

The payload harvested credentials from GitHub, npm, PyPI, AWS, GCP, Azure, and Kubernetes, exfiltrating data to attacker-controlled repositories. A worm-like self-propagation mechanism used stolen tokens to backdoor additional packages, whilst a gh-token-monitor persistence daemon threatened destructive action if credentials were revoked. The malware further embedded a prompt-injection text to mislead AI-based security scanners into classifying it as benign.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, BFSI, IT Services and Consulting, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Visual Studio, Docker, Kubernetes, VS Code, Azure, npm, PyPI, GitHub, Cursor IDE, Anthropic Claude, LangChain, Google Gemini

Source - https://orca.security/resources/blog/hades-pypi-supply-chain-attack/

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