TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: August 4, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As August 2026 begins, the cyber threat landscape shows no sign of relenting, 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

APT42 adds GenAI and TAMECAT phishing arsenal in expanding espionage operation

APT42, an Iran-linked advanced persistent threat group, has expanded its SpearSpecter campaign by upgrading its modular TAMECAT backdoor and integrating generative AI across its operations. The group now applies AI to target research, persona creation, multilingual lure generation and malware development, stripping away the grammatical and cultural tells that once exposed state-sponsored phishing attempts to alert recipients.

The campaign blends patient rapport-building, credential harvesting and abuse of trusted cloud services with fileless malware to compromise high-value targets across government, defence, think tanks and the nuclear sector. TAMECAT can steal browser cookies and session tokens that survive password resets, so organisations are urged to revoke active sessions, refresh tokens and scrutinise suspicious sign-ins following any suspected compromise.

ATTACK TYPE	Phishing, Cyber-espionage, APT	**SECTOR**	Government, Journalism, Energy, Defence, Consultancy
REGION	Middle East, Israel, United States	**APPLICATION**	Microsoft Edge, Microsoft Excel, Microsoft Outlook, Microsoft Windows, Google Chrome, Microsoft OneDrive, PowerShell, Discord, WhatsApp

Source - https://gbhackers.com/apt42-uses-ai-assisted-phishing/

INTRODUCTION | APT42 ENHANCES TAMECAT WITH AI-DRIVEN PHISHING AND ADVANCED ESPIONAGE | CISA ADDS ACTIVELY EXPLOITED SHAREPOINT AND CHECK POINT FLAWS TO ITS URGENT CATALOG | UTA0533 EXPLOIT SONICWALL VPN ZERO-DAYS TO GAIN ROOT ACCESS AND DEPLOY MALWARE | TAX REFUND LURES DELIVER FILELESS MALWARE GIVING ATTACKERS FULL CONTROL OF SYSTEMS | NEW RUST-BASED TROJAN HIJACKS BROWSERS TO CONCEAL RANSOMWARE COMMAND AND CONTROL | CRITICAL NINJA FORMS SCRIPTING FLAW COULD HAND ATTACKERS FULL ADMINISTRATOR CONTROL | MUDDYWATER-LINKED BACKDOOR DELIVERED THROUGH CLICKFIX AND TELEGRAM LURES | CL0P EXPLOITS CRITICAL WINDCHILL AND FLEXPLM VULNERABILITY FOR DATA THEFT | CISA EXPAND WARNING AS IRANIAN HACKERS MANIPULATE INDUSTRIAL CONTROL SYSTEMS | STATE-BACKED ACTOR EXPLOITS ZIMBRA WEBMAIL ZERO-DAY FOR EMAIL ESPIONAGE CAMPAIGN

TATA COMMUNICATIONS

CISA urges immediate patching of active attacks on SharePoint and Check Point flaws

The US Cybersecurity and Infrastructure Security Agency (CISA) has added two critical flaws to its Known Exploited Vulnerabilities Catalog, citing evidence of active exploitation. The first, CVE-2026-50522, is a deserialisation vulnerability in Microsoft SharePoint enabling remote code execution. The second, CVE-2026-16232, is an authentication bypass in Check Point SmartConsole granting attackers full administrative access to management servers.

Successful exploitation could allow complete system compromise, unauthorised administrative access and modification of security policies across managed networks. Check Point has confirmed that a small number of internet-exposed customers were targeted, while a public proof-of-concept has accelerated SharePoint attacks. Federal agencies were ordered to remediate by 25 July 2026, and all organisations are urged to patch immediately.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, BFSI, IT, Government, Defence, Business, Airlines, Automobile, Broadcast Media Production, Retail and Distribution, Logistics
REGION	Global	**APPLICATION**	Microsoft SharePoint Server, Microsoft Windows SharePoint Services, Check Point Management Server

Source - https://www.cisa.gov/news-events/alerts/2026/07/22/cisa-adds-two-known-exploited-vulnerabilities-catalog

TATA COMMUNICATIONS

UTA0533 chains SonicWall zero-days to plant stealthy malware and harvest credentials

Security researchers have detailed the active exploitation of SonicWall Secure Mobile Access 1000 series VPN appliances by a threat actor tracked as UTA0533. The attackers chained two zero-day vulnerabilities, CVE-2026-15409 and CVE-2026-15410, to bypass authentication, exploit server-side request forgery, execute commands and escalate privileges — ultimately achieving root-level access on compromised devices before public disclosure of the flaws.

Following compromise, UTA0533 deployed the custom malware families KNUCKLEBALL, ORANGETAIL and ROOTRUN to establish persistent, covert access. The actor harvested credentials, monitored LDAP traffic and attempted lateral movement into internal networks. SonicWall has released patched appliance versions and urged customers to update immediately, hunt for the published indicators, and rotate credentials only after confirming appliance integrity has been restored.

ATTACK TYPE	Vulnerability, Malware	**SECTOR**	Healthcare, Hospitality, BFSI, IT, Government, Defence, Business, Airlines, Automobile, Broadcast Media Production, Retail and Distribution, Logistics
REGION	Global	**APPLICATION**	SonicWall SMA (Secure Mobile Access), SonicWall SRA (Secure Remote Access), SonicWall Firewall, SonicWall VPN

Source - https://cybersecuritynews.com/sonicwall-0-day-vulnerabilities-exploited/

TATA COMMUNICATIONS

Phishing emails posing as tax refunds deploy Remcos malware using in-memory evasion

Security researchers have uncovered a phishing campaign that spoofs official GST refund notifications to deliver the Remcos remote access trojan through a sophisticated multi-stage .NET infection chain. Victims receive malicious RAR attachments containing a packed .NET executable disguised as a legitimate file. The lures exploit government branding, financial incentives and urgency to persuade recipients into opening the attachment.

The infection relies heavily on stealth, concealing subsequent payloads inside a bitmap object and loading each stage directly into memory to avoid disk-based detection. The chain uses reflection-based execution, privilege escalation via cmstp.exe and registry-based persistence to maintain long-term access. Organisations are urged to strengthen email filtering; block spoofed government domains and scrutinise archive attachments carrying executable content.

ATTACK TYPE	Phishing, Malware	**SECTOR**	Financial services
REGION	India	**APPLICATION**	Windows

Source - https://www.seqrite.com/blog/behind-the-refund-from-gst-phishing-to-remcos-rat-through-a-multi-stage-net-infection-chain/

TATA COMMUNICATIONS

Chaos ransomware abuses browser debugging tools to mask its command and control

Cisco Talos researchers have identified msaRAT, a Rust-based remote access trojan attributed to the Chaos ransomware group and deployed ahead of file encryption. Rather than contacting attacker infrastructure directly, the implant launches Chrome or Edge in headless mode and drives it through the Chrome DevTools Protocol, keeping its own process traffic confined to the local host.

All command-and-control traffic instead leaves through the browser over a WebRTC channel, with signalling routed via Cloudflare Workers and the connection relayed through Twilio's TURN service. Because this rides on widely trusted infrastructure, the attacker's true server address never appears on the wire. Defenders are urged to monitor for browsers launched with remote-debugging options enabled.

ATTACK TYPE	Ransomware, Malware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Edge, Windows, Google Chrome

Source - https://thehackernews.com/2026/07/chaos-ransomware-uses-msarat-to-route.html

TATA COMMUNICATIONS

Unauthenticated scripting flaw threatens hundreds of WordPress sites using Ninja Forms

Researchers have disclosed four vulnerabilities in Ninja Forms, a popular WordPress plugin installed on more than 600,000 websites. The most severe, CVE-2026-65048, carries a CVSS score of 9.3 and is an unauthenticated stored cross-site scripting flaw. An attacker can submit a public form containing a malicious script that later executes in an administrator's browser, potentially hijacking their session.

The remaining flaws allow attackers to manipulate payment totals down to zero, wipe all plugin data across a WordPress Multisite network, and expose form submissions without authorisation. All issues affect versions up to 3.14.9 and have been resolved in Ninja Forms 3.14.10. Site administrators are strongly urged to update immediately, given that two flaws require no authentication.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, BFSI, IT, Government, Defence, Business, Airlines, Automobile, Broadcast Media Production, Retail and Distribution, Logistics
REGION	Global	**APPLICATION**	WordPress

Source - https://securityonline.info/ninja-forms-vulnerability-cve-2026-65048/

INTRODUCTION | APT42 ENHANCES TAMECAT WITH AI-DRIVEN PHISHING AND ADVANCED ESPIONAGE | CISA ADDS ACTIVELY EXPLOITED SHAREPOINT AND CHECK POINT FLAWS TO ITS URGENT CATALOG | UTA0533 EXPLOIT SONICWALL VPN ZERO-DAYS TO GAIN ROOT ACCESS AND DEPLOY MALWARE | TAX REFUND LURES DELIVER FILELESS MALWARE GIVING ATTACKERS FULL CONTROL OF SYSTEMS | NEW RUST-BASED TROJAN HIJACKS BROWSERS TO CONCEAL RANSOMWARE COMMAND AND CONTROL | CRITICAL NINJA FORMS SCRIPTING FLAW COULD HAND ATTACKERS FULL ADMINISTRATOR CONTROL | MUDDYWATER-LINKED BACKDOOR DELIVERED THROUGH CLICKFIX AND TELEGRAM LURES | CL0P EXPLOITS CRITICAL WINDCHILL AND FLEXPLM VULNERABILITY FOR DATA THEFT | CISA EXPAND WARNING AS IRANIAN HACKERS MANIPULATE INDUSTRIAL CONTROL SYSTEMS | STATE-BACKED ACTOR EXPLOITS ZIMBRA WEBMAIL ZERO-DAY FOR EMAIL ESPIONAGE CAMPAIGN

TATA COMMUNICATIONS

MuddyWater-linked backdoor spreads through ClickFix lures and hidden Telegram traps

Security researchers have reverse-engineered a three-stage intrusion chain, assessed with high confidence as linked to the MuddyWater threat group, which delivers a custom backdoor known as PatchAgent. The campaign relies on ClickFix social-engineering lures and Telegram-enabled components for delivery. Infection begins with a COM DLL dropper, cloud.dll, which is executed via regsvr32 and launches a secondary loader, wuaupdt.exe.

The loader validates a custom PTCH v2 container, verifies its integrity using HMAC-SHA256 and decrypts an AES-256-CBC payload. The resulting shellcode backdoor performs process hollowing, executes PowerShell commands, establishes persistence and manages files, before communicating with attacker-controlled infrastructure over HTTP. Dedicated check-in, tasking and exfiltration endpoints allow operators to issue commands and retrieve stolen data from compromised hosts.

ATTACK TYPE	Malware, Cyber-espionage, APT	**SECTOR**	Government, Oil and gas, Defence, Telecommunications
REGION	North America, Middle East, Europe, Africa, Asia	**APPLICATION**	Windows

Source - https://ransom-isac.org/blog/muddywater-clickfix-patchagent/

TATA COMMUNICATIONS

Cl0p targets exposed product lifecycle platforms in new data theft and extortion campaign

Cl0p ransomware affiliates are actively exploiting internet-exposed PTC Windchill and FlexPLM deployments, chaining a pre-authentication FlexPLM WSDL information disclosure flaw with CVE-2026-12569, a critical remote code execution vulnerability in the Windchill login servlet. The combination grants unauthenticated code execution, allowing attackers to deploy hex-named JSP webshells, enumerate the filesystem, and stage sensitive engineering and product design data for theft.

The stolen data fuels double-extortion operations, with hundreds of employees at affected organisations reportedly receiving extortion emails. Victims have been observed across the manufacturing, automotive, aerospace and retail sectors, where compromised intellectual property carries severe consequences. PTC has released fixed builds, and the flaw was added to CISA's Known Exploited Vulnerabilities catalogue, making prompt patching essential for exposed instances.

ATTACK TYPE	Vulnerability	**SECTOR**	Manufacturing, Aerospace, Automobile, Retail and Distribution
REGION	Global	**APPLICATION**	Windows

Source - https://ransom-isac.org/blog/clop-windchill-flexplm-exploitation/

TATA COMMUNICATIONS

Iranian threat actors exploit internet-facing controllers to disrupt essential infrastructure

A coalition of US federal agencies — including CISA, the FBI, NSA and EPA — has warned of ongoing Iranian-affiliated cyber operations targeting internet-exposed programmable logic controllers across critical infrastructure. Using legitimate engineering software, the attackers accessed vulnerable operational technology environments, exfiltrated PLC project files, altered control logic, manipulated HMI and SCADA displays, and disabled safety functions on affected devices.

The campaign has affected government, water, wastewater and energy sectors, causing operational disruption and financial losses. Originally issued in April 2026, the advisory was updated in July to expand its scope beyond Rockwell Automation to Schneider Electric, Siemens and other controllers. Organisations are urged to remove PLCs from internet exposure, change default passwords and monitor project files for unauthorised changes.

ATTACK TYPE	Cyber-espionage	**SECTOR**	Government, Energy
REGION	United States	**APPLICATION**	Siemens Simatic PLC, Siemens SICAM, Schneider Electric, SIEMENS, Rockwell Automation

Source - https://blog.polyswarm.io/iranian-plc-exploitation-campaign-targets-us-critical-infrastructure

TATA COMMUNICATIONS

Hackers exploit Zimbra zero-day to steal emails and bypass two-factor authentication

A Russian state-backed threat actor known as LAUNDRY BEAR has been exploiting CVE-2025-66376, a stored cross-site scripting flaw in the Zimbra Collaboration Suite Classic UI, as a zero-day since July 2025. Exploitation requires no user interaction: simply viewing a malicious email triggers embedded JavaScript, granting attackers access to the victim's authenticated webmail session without a single click.

The campaign deploys the custom Ulej capability and Flowerbed collection framework to exfiltrate up to ninety days of emails, Global Address Lists, account metadata, passwords, 2FA recovery codes and application passcodes. Attackers establish persistence by enabling IMAP and creating ZimbraWeb application passwords. Organisations are urged to patch affected versions immediately, rotate credentials and revoke active sessions.

ATTACK TYPE	Cyber-espionage, APT	**SECTOR**	IT, Government, Education, Energy, Defence Industry, Broadcast Media Production and Distribution
REGION	Australia, Canada, UK, Netherlands, New Zealand, Ukraine	**APPLICATION**	Zimbra Collaboration

Source - https://socradar.io/blog/cve-2025-66376-russian-apt-zimbra-zero-day/

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