TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: September 22, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As September 2026 advances, the cyber threat landscape shows no sign of slowing, with threat actors mounting ever more sophisticated and tightly coordinated campaigns across deeply interconnected digital environments. Traditional defence models are straining to keep pace as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now rests on organisations reinforcing foundational security controls, adopting layered defence strategies, and embedding forward-looking intelligence throughout every layer of their operational frameworks.

In this fast-moving environment, the Tata Communications Cyber Threat Intelligence report remains an indispensable resource for security practitioners. Released weekly, it delivers 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 — sustaining the continuity of critical operations at scale.

TATA COMMUNICATIONS

Emerging Panzer ransomware targets virtualised ESXi-ready and cross-platform platforms

Panzer is an emerging Ransomware-as-a-Service operation, first observed on 5 August 2026 with a dedicated leak site and a claimed 16 victims across 11 countries. The group targets a broad spread of sectors, including technology, manufacturing, government, agriculture, energy and retail, suggesting opportunistic rather than tightly focused targeting. It advertises cross-platform builds for Windows, Linux, VMware ESXi and FreeBSD.

The operation runs a semi-open affiliate programme on an 80/20 revenue split favouring affiliates, recruiting partners via Tox with a screening process before dashboard access. Panzer employs double extortion, pairing data theft and encryption with leak-site pressure. Its mature dashboard, automated Bitcoin invoicing, per-build negotiation tooling and affiliate vetting point to a rapidly professionalising ransomware ecosystem worthy of close attention.

ATTACK TYPE	Ransomware, Emerging Threats
REGION	Singapore, Cyprus, Czech Republic, France, Germany, Hungary, Indonesia, Italy, South Korea, Nigeria, Portugal, Saudi Arabia, Serbia, Slovakia, Spain, Switzerland, Thailand, UAE, United States
SECTOR	IT, Manufacturing, Government, Education, Energy, Defence, E-Commerce, Retail and Distribution
APPLICATION	FreeBSD, VMware ESXi, Windows, Linux

Source - https://gbhackers.com/new-panzer-ransomware-hits-16-victim/

TATA COMMUNICATIONS

Unpatched WordPress CVE-2026-14894 plugin exploited, enabling unauthenticated RCE

Wordfence has reported active exploitation of a critical vulnerability in the WordPress Super Forms – Drag and Drop Form Builder plugin. Tracked as CVE-2026-14894 and carrying a maximum CVSS score of 9.8, the flaw affects all versions up to and including 6.3.313. It allows unauthenticated attackers to upload executable PHP files, potentially leading to remote code execution and complete website compromise.

The weakness stems from missing file-type validation in the plugin's submission handler, with a required nonce trivially obtainable through an unauthenticated AJAX action. Exploitation began on 14 July 2026 and surged in late August, with Wordfence blocking over 250,000 attempts. Administrators are urged to upgrade to version 6.3.314 immediately and inspect upload directories for suspicious PHP files.

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

Source - https://securityonline.info/super-forms-cve-2026-14894-rce/

TATA COMMUNICATIONS

Record-breaking Microsoft patch fixes 973 flaws, including two actively exploited zero-days

Microsoft's September 2026 Patch Tuesday is its largest security release on record, addressing 973 vulnerabilities — more than double August's total and a sharp rise from the 621 patched in July. The updates span Windows, Office, SQL Server, Exchange Server, SharePoint Server, Azure and developer tools, with Windows alone accounting for 723 of the flaws. Elevation-of-privilege issues dominate the release.

Two of the flaws are being actively exploited as zero-days. CVE-2026-81963 in the Windows Update Stack and CVE-2026-85880 in the Advanced Local Procedure Call component both allow attackers to elevate privileges to SYSTEM level, aiding post-compromise activity. Given the sheer volume and the confirmed exploitation, organisations are strongly urged to prioritise remediation and apply the cumulative updates without delay.

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

Source - https://cybersecuritynews.com/microsoft-patch-tuesday-update-september-2026/

TATA COMMUNICATIONS

Evilginx2-based BigBear phishing-as-a-service hijacks Microsoft 365 sessions despite MFA

Cybersecurity team has uncovered BigBear 2.0, a rebranded Evilginx2-based phishing-as-a-service operation targeting Microsoft 365 users across more than 40 countries. Operating an adversary-in-the-middle reverse proxy, it relays victim traffic to Microsoft's genuine login portal while capturing credentials and the authenticated session cookie issued after sign-in, allowing attackers to hijack fully authenticated sessions without triggering further MFA challenges.

The operation combined geo-matched residential proxies, real-time Telegram exfiltration and automated cookie replay, while custom JavaScript disabled FIDO2/WebAuthn to force victims onto weaker, interceptable authentication methods. After gaining access to the threat actor panel, researchers found 5,137 records spanning 461 organisations, including plaintext passwords and session cookies. Organisations are urged to enforce phishing-resistant, FIDO2-only authentication and eliminate weaker fallbacks.

ATTACK TYPE	Phishing	**SECTOR**	Pharmaceuticals, ONGC, IT Services and Consulting
REGION	India, France, Germany, New Zealand, Saudi Arabia	**APPLICATION**	Microsoft Outlook, Microsoft Office 365, Microsoft Teams, Microsoft Entra , Microsoft OneDrive

Source - https://www.cloudsek.com/blog/tracking-bigbear-2-0-evilginx2-phishing-campaign

TATA COMMUNICATIONS

Multiple ClickFix campaigns deliver infostealers to macOS and Windows users worldwide

Researchers are tracking a wave of ClickFix-driven campaigns that lure victims through compromised websites, fake CAPTCHA overlays, malvertising and malicious browser content. On macOS, the MacSync stealer harvests credentials, browser sessions, cryptocurrency wallets and other sensitive data, while on Windows, the newly documented WordlistLoader reconstructs and deploys Amatera Stealer, one of the more actively evolving infostealers currently in circulation.

Related activity abuses Google services, Binance Smart Chain smart contracts, browser extensions and WebRTC to deliver payloads and manipulate cryptocurrency transactions. Because victims execute the commands themselves, these campaigns bypass many file-based defences while employing in-memory execution and anti-analysis techniques. Organisations are urged to restrict command-line and script execution for standard users and train staff against fake verification prompts.

ATTACK TYPE	Social engineering, Phishing, Malware
REGION	Australia, Singapore, Canada, India, Japan, UK, Global, France, Germany, Netherlands, United States
SECTOR	IT, Government, Defence, Business, BFSI, Trading, Cryptocurrency
APPLICATION	Apple macOS, Microsoft Edge, Microsoft Outlook, Apple Safari, Chromium, Mozilla Firefox, WordPress, Windows, Microsoft Teams, Google Chrome, AWS, Telegram, Slack, Okta, GitHub, Discord, Google Workspace

Source - https://cyberpress.org/macsync-clickfix-wallet-heist/

TATA COMMUNICATIONS

CISA flags four actively exploited flaws added to federal catalogue, prompting urgent patching

The US Cybersecurity and Infrastructure Security Agency has added four actively exploited vulnerabilities to its Known Exploited Vulnerabilities Catalog. Two carry the maximum CVSS score of 10.0: CVE-2026-75650, a template-engine injection flaw in Adobe Commerce and Magento, and CVE-2026-86218, a pre-authentication static code injection vulnerability in N-able N-central. Both can enable unauthenticated remote code execution on affected systems.

The remaining two are Microsoft Windows local privilege-escalation flaws: CVE-2026-81963, a link-following weakness, and CVE-2026-85880, a heap-based buffer overflow, both allowing attackers to elevate privileges to SYSTEM. With all four confirmed under active exploitation, federal agencies faced remediation deadlines in September 2026. Organisations are strongly urged to apply vendor patches promptly and review systems for prior compromise.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Google ChromeOS, Windows, Adobe Commerce, Google Chrome, N-able N-central, Adobe Magento

Source - https://www.cisa.gov/news-events/alerts/2026/09/08/cisa-adds-four-known-exploited-vulnerabilities-catalog

INTRODUCTION | CROSS-PLATFORM PANZER RANSOMWARE CLAIMS 16 VICTIMS WITHIN ITS FIRST MONTH ONLINE | CRITICAL WORDPRESS SUPER FORMS FLAW (CVE-2026-14894) ACTIVELY EXPLOITED FOR RCE | MICROSOFT RECORDS SEPTEMBER UPDATE, FIXING 973 FLAWS AND TWO EXPLOITED ZERO-DAYS | BIGBEAR 2.0 PHISHING KIT BYPASSES MFA TO HIJACK THOUSANDS OF MICROSOFT 365 ACCOUNTS | FAKE CAPTCHA LURES USERS VIA BLOCKCHAIN AND BROWSER ABUSE FOR CREDENTIALS THEFT | FOUR NEWLY CATALOGUED FLAWS UNDER ACTIVE ATTACK PUT UNPATCHED SYSTEMS AT RISK | SLEEPWALKER BACKDOOR STAYS DORMANT UNTIL CRAFTED NETWORK TRIGGERS ITS EXECUTION | CLICKFIX EVOLVES INTO A FLEXIBLE DELIVERY ENGINE FOR LOADERS, RATS, AND C2 | GRYXA BUILT WITH AI TURNS LEGITIMATE REMOTE TOOLS INTO COVERT PERSISTENT ACCESS | FORTINET FIXES CRITICAL UNAUTHENTICATED FLAWS ACROSS ENTERPRISE SECURITY PRODUCT RANGE

TATA COMMUNICATIONS

SLEEPWALKER backdoor uses ESET agent DLL sideloading for network-triggered execution

SLEEPWALKER is a novel passive Windows backdoor disclosed in August 2026 that operates through DLL sideloading into the ESET Management Agent process (ERAAgent.exe). The unsigned 64-bit sample masquerades as Microsoft's dpapi.dll and carries copied ESET version metadata, helping it blend into a trusted security environment. Crucially, it embeds no fixed command-and-control infrastructure and generates no outbound beaconing traffic.

Instead, the implant remains dormant in memory until a crafted trigger packet arrives, decrypting attacker-supplied bytecode using AES-256-CCM across a 23-instruction command language spanning covert transports, scheduling, lateral movement and in-memory shellcode execution. As a post-compromise tool exploiting Windows search order rather than any vendor flaw, there is nothing to patch; defenders should hunt for suspicious dpapi.dll files besides ERAAgent.exe.

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

Source - https://blog.polyswarm.io/sleepwalker-passive-backdoor-awakens-only-when-attackers-call

TATA COMMUNICATIONS

ClickFix multi-stage malware delivers loaders and RATs using blockchain-backed C2

Threat intelligence gathered throughout 2026 reveals how ClickFix has matured from a simple social engineering trick into a flexible malware-delivery ecosystem. Independent clusters now abuse fake CAPTCHA and verification pages, malicious npm-hosted HTML, cloaked macOS lures, steganographic loaders, trojanised installers and compromised websites to deliver families including PavinLoader, DOUBLECUP, CountLoader, DeviceManager, Starland RAT, Cruciferra, AMOS and Remus.

These campaigns increasingly favour in-memory execution, DNS and WebSocket tunnelling, and security-process termination to evade detection. Loaders such as DOUBLECUP stage payloads inside browser-cached PNG images and lock them to each victim's IP address, while several RATs use EtherHiding to resolve command-and-control via blockchain smart contracts. Organisations should prioritise behavioural analytics over static indicators and restrict PowerShell execution.

ATTACK TYPE	Phishing, Malware	**SECTOR**	IT, BFSI, Services, Business, Cryptocurrency
REGION	Global	**APPLICATION**	Apple macOS, Microsoft Edge, Apple Safari, Chromium, Cisco Webex, Mozilla Firefox, Opera Browser, Python, Windows, Zoom Meetings, Google Chrome, npm, Telegram, Salesforce

Source - https://securityonline.info/doublecup-clickfix-loader/

TATA COMMUNICATIONS

AI-built Gryxa toolkit hijacks RMM software to steal credentials and resist removal

Researchers at ReliaQuest have identified Gryxa, a financially motivated toolkit observed across up to 324 listed hosts, with substantial portions of its development likely assisted by a commercial AI coding agent. Delivered through invoice-themed phishing, it abuses legitimate remote monitoring and management software to establish covert, persistent access, backed by multiple independent recovery mechanisms including scheduled tasks and WMI event subscriptions.

Gryxa also harvests credentials stored in Chromium-based browsers, targeting cryptocurrency and financial accounts. When its relay becomes unreachable, it disables or uninstalls endpoint protection within roughly ten to thirteen minutes, while a surviving component collects and exfiltrates evidence of defender remediation activity. Analysts urge behaviour-based detection over file hashes and coordinated, rather than partial, containment of affected hosts.

ATTACK TYPE	Cyber Crime, Phishing, Malware	**SECTOR**	BFSI, Cryptocurrency
REGION	Global	**APPLICATION**	Microsoft Windows Defender, Chromium, Windows, Google Chrome, Telegram

Source - https://cyberpress.org/gryxa-tracks-defender-removal/

TATA COMMUNICATIONS

Fortinet update fixes authentication bypass and certificate validation flaws across products

Fortinet has released security updates addressing multiple vulnerabilities across its product portfolio, including two rated critical. The most severe, CVE-2026-84390 (CVSS 9.6), stems from sensitive information exposed in the FortiMonitor OnSight web portal's source code, letting a remote unauthenticated attacker bypass authentication using a forged or reused JSON Web Token and reach protected functionality within the portal.

The second critical flaw, CVE-2026-84388 (CVSS 9.1), lets attackers proxy a victim's browser traffic via the Privileged Access Agent Chrome extension. High-severity issues in FortiSandbox, FortiOS, and the FortiProxy ZTNA portal enable unauthorised data retrieval and man-in-the-middle attacks. No active exploitation has been reported, though Fortinet urges customers to apply the coordinated updates without delay.

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

Source - https://www.hkcert.org/security-bulletin/fortinet-products-multiple-vulnerabilities_20260909

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