TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: September 1, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As September 2026 opens, 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.

INTRODUCTION

UPDATED ADVISORY WARNS MEDUSA EXPLOITS NEWLY DISCLOSED FLAWS WITHIN 24 HOURS

UAT-10147 USE AI-DRIVEN WORKFLOWS TO EXPLOIT GLOBAL WEB SERVERS AUTOMATICALLY

FAKE CAPTCHA PROMPTS EXPLOITED TO SPREAD STOPANDPROTECT VIA HACKED WEBSITES

MICROSOFT PATCHES 22 CLOUD FLAWS INCLUDING A MAXIMUM-SEVERITY ENTRA ID RCE BUG

ATTACKERS EXPLOIT MACOS SCREEN SHARING FLAW TO SEIZE ROOT AND MINE CRYPTOCURRENCY

MULTI-STAGE OCTAGON ANDROID RAT POSES AS GOVERNMENT SAFETY APP TO HIJACK DEVICES

CISCO FIX CRITICAL FLAWS IN NETWORK AUTOMATION AND WORKLOAD SECURITY PLATFORMS

CITRIX PATCHES CRITICAL NETSCALER ADC AND GATEWAY FLAWS AS ATTACK RISK RISES SHARPLY

NEW SILKPARASITE MALWARE POWERS ESPIONAGE AGAINST GOVERNMENT ORGANISATIONS

TWINLOOT ABUSES SHAREPOINT AND TEAMS TO STEAL CREDENTIALS AND MOVE LATERALLY

TATA COMMUNICATIONS

Agencies warn Medusa ransomware has struck over 500 critical infrastructure organisations

CISA, the FBI and HHS updated joint advisory AA25-071A on 18 August 2026, detailing expanded Medusa ransomware activity affecting more than 500 critical infrastructure organisations. The revised guidance highlights the exploitation of CVE-2025-10035 in Fortra GoAnywhere and CVE-2026-1731 in BeyondTrust, noting that Medusa affiliates frequently weaponise newly disclosed vulnerabilities within 24 hours of public announcement, occasionally even earlier.

To confirm successful exploitation, the operators rely on Interactsh callbacks before advancing their intrusion. Medusa then combines credential theft, legitimate remote monitoring and management tools, covert command-and-control, Active Directory manipulation and data exfiltration ahead of encryption. Organisations are urged to prioritise rapid patching of internet-facing systems, enforce phishing-resistant multi-factor authentication and maintain offline, immutable and regularly tested backups.

ATTACK TYPE	Vulnerability, Cybercrime, Ransomware, Phishing, Breaches
REGION	Global
SECTOR	IT, Healthcare, BFSI, Legal Services, Public Health, Manufacturing, Government, Education, Defence
APPLICATION	Apple macOS, Windows, Linux, BeyondTrust Privileged Remote Access, FortiClient EMS, ScreenConnect, Fortra's GoAnywhere MFT, ConnectWise

Source - https://www.safebreach.com/blog/safebreach-coverage-us-cert-aa25-071a-medusa-ransomware/

TATA COMMUNICATIONS

Cybercrime group UAT-10147 harnesses agentic AI to automate web server attacks at scale

Cisco Talos has identified UAT-10147, a financially motivated, Chinese-speaking cybercrime group targeting internet-exposed Windows and Linux web servers worldwide through publicly disclosed vulnerabilities. After achieving remote code execution, the actor deploys web shells and implants, escalates privileges, modifies Windows Defender exclusions and establishes persistence. Researchers uncovered a target list of roughly 170,000 URLs on the group's infrastructure.

What distinguishes the group is its integration of agentic AI. It combined DeepAudit, PentestGPT and ysoserial with AI-generated workflows for exploit development, validation, reconnaissance, payload deployment and post-compromise automation across multiple regions and industries. Talos warns this lowers the expertise needed to scale complex attacks. Organisations should patch exposed applications promptly and audit Defender exclusions and IIS modules.

ATTACK TYPE	Cybercrime, Malware	**SECTOR**	IT, Government, Education, Gaming industry, Journalism
REGION	Australia, Canada, India, UK, Bolivia, Brazil, China, Denmark, France, Germany, Iran, Ireland, Italy, Netherlands, Turkey, United States, Vietnam, Hong Kong	**APPLICATION**	Windows, Linux, Zimbra Collaboration

Source - https://securityonline.info/uat-10147-agentic-ai-attacks/

TATA COMMUNICATIONS

Fake CAPTCHA lures visitors into installing StopAndProtect via hacked WordPress sites

StopAndProtect is a large-scale cybercriminal operation uncovered by Check Point Research, which first identified its ransomware component in mid-May 2026. The campaign abuses thousands of compromised WordPress websites as malware distribution points, command-and-control infrastructure and storage for stolen data. A rare operational security lapse by the developer exposed detailed victim logs, revealing more than 6,000 affected machines worldwide.

Infection begins with a fake CAPTCHA using the ClickFix social engineering technique, which tricks Windows users into running a malicious PowerShell command. Multiple PowerShell and .NET stages then deploy a modular toolkit spanning ransomware, credential stealers, worms, screen lockers and remote utilities. Organisations should keep WordPress installations updated, monitor for suspicious PowerShell activity and train users against ClickFix lures.

ATTACK TYPE	Malware	**SECTOR**	IT Services and Consulting, Business
REGION	Russia, India, Ukraine, United States	**APPLICATION**	WordPress, Windows, PowerShell

Source - https://research.checkpoint.com/2026/thousands-of-hacked-wordpress-sites-one-operation-unmasking-stopandprotect/

TATA COMMUNICATIONS

Microsoft fixes multiple critical cloud vulnerabilities across Azure Entra ID and Exchange

Microsoft has patched a critical remote code execution vulnerability in Entra ID, its cloud identity and access management service, tracked as CVE-2026-69836 and carrying the maximum CVSS score of 10.0. Caused by deserialization of untrusted data, the flaw could let an unauthenticated attacker execute code remotely. Microsoft has fully mitigated the issue, requiring no customer action.

The disclosure formed part of a wider release of 22 patches spanning Entra ID, Fabric, Exchange Online, Partner Center, Azure Arc, Azure SQL Database, Logic Apps and Data Factory. The flaws cover elevation of privilege, information disclosure, SQL injection, server-side request forgery and path traversal. Microsoft initially reported exploitation of CVE-2026-69836 but later revised this status to none.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Office 365, Microsoft Azure, Microsoft Entra

Source - https://www.securityweek.com/microsoft-rolls-out-22-fresh-security-patches/

TATA COMMUNICATIONS

Authentication bypass in macOS Screen Sharing exploited to plant cryptomining malware

The US Cybersecurity and Infrastructure Security Agency has added CVE-2026-65400 to its Known Exploited Vulnerabilities Catalog following confirmed active exploitation. The critical flaw affects Apple's macOS Screen Sharing service and stems from improper authentication, allowing remote attackers to connect without valid credentials. With public proof-of-concept code circulating, CISA has rescored the vulnerability to a critical severity rating of 9.8.

Attacks have been observed against internet-exposed Macs with Screen Sharing reachable over port 5900, granting intruders root-level access that was used to deploy Monero cryptominers. Apple has released fixes across macOS Sonoma, Sequoia and Tahoe. Administrators are urged to update immediately, disable Screen Sharing where it is not required and block external access to the affected port.

ATTACK TYPE	Vulnerability, Malware	**SECTOR**	Healthcare, Hospitality, BFSI, IT, Government, E-Commerce, Aviation, Automobile, Retail and Distribution, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Apple macOS

Source - https://thehackernews.com/2026/08/apple-macos-screen-sharing-flaw.html

TATA COMMUNICATIONS

Fake emergency alert app hides powerful Octagon trojan targeting banking and wallets

Octagon is a multi-stage Android remote access trojan sold as a malware-as-a-service offering, linked by iVerify to the Russian-speaking operator AndroidKitKat and advertised for around 1,400 US dollars a month. K7 Labs documented an active campaign in which the malware impersonated the official BH Alert emergency application, luring victims through fake government and app store pages.

The malware loads encrypted DEX and JAR payloads while abusing Accessibility services, registering a malicious VPN, deploying overlays, capturing screens and credentials, intercepting SMS and enabling remote control. Multiple persistence mechanisms help it survive reboots. Recovered samples target banking, cryptocurrency, exchange and messaging apps. Users should install apps only from official stores and avoid granting Accessibility access to unfamiliar software.

ATTACK TYPE	Social engineering, Malware	**SECTOR**	Government, BFSI, Cryptocurrency
REGION	Bahrain	**APPLICATION**	Android

Source - https://zimperium.com/blog/rapid-response-zimperium-secures-mobile-endpoints-against-octagon-android-malware

TATA COMMUNICATIONS

Cisco patches multiple severe flaws across Crosswork Secure Workload and BroadWorks

Cisco released security updates on 19 August 2026 addressing multiple vulnerabilities across its Crosswork, Secure Workload and BroadWorks products. Discovered during internal security reviews, the flaws span nine issues in Crosswork and Secure Workload alone, five of which carry the maximum CVSS score of 10.0. The weaknesses include SQL injection, authentication bypass, access-control failures, memory safety flaws and XXE injection.

Successful exploitation could enable remote code execution, authentication bypass, credential compromise and unauthorised file manipulation on affected systems. Cisco stated the issues were found internally and are not known to be exploited, with no workarounds available. Internet-facing Crosswork deployments pose the greatest risk. Administrators are urged to upgrade to the fixed releases, including Crosswork 7.2.1-SP, without delay.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Cisco BroadWorks Application Server, Cisco Secure Workload

Source - https://securityonline.info/cisco-secure-workload-cve-2026-20315/

TATA COMMUNICATIONS

Citrix fixes NetScaler ADC and Gateway vulnerabilities amid active exploitation concerns

Citrix has issued a security update for NetScaler ADC and NetScaler Gateway, addressing two flaws: CVE-2026-19489, a memory overflow rated CVSS 8.8, and CVE-2026-19490, a critical authentication bypass rated CVSS 9.3. The latter allows an unauthenticated attacker to circumvent login checks entirely on appliances configured as a Gateway or AAA virtual server, requiring no user interaction.

Separately, researchers at watchTowr Labs published a technical analysis and working proof-of-concept for the related CVE-2026-8452, also rated CVSS 8.8. The exploit demonstrates pre-authentication remote code execution via a heap overflow in NetScaler's SAML handling, ultimately gaining root privileges. With no workarounds available, organisations should upgrade to patched firmware immediately and monitor exposed appliances for compromise.

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

Source - https://securityonline.info/citrix-netscaler-pre-auth-rce-cve-2026-8452/

TATA COMMUNICATIONS

SilkParasite targets governments with malware and cloud-based command channels

Researchers at Bitdefender Labs have uncovered SilkParasite, a cyber-espionage operation assessed with medium confidence as China-nexus, targeting government bodies across Central Asia. First detected in late 2025 at an agency involved in economic decision-making, the campaign had run for almost a year. Investigators identified seven remote access tool families, five of them previously undocumented, forming a compact, modular arsenal.

Initial access relied on spear-phishing emails carrying malicious Office documents, often concealed within password-protected RAR archives, with payloads deployed through DLL sideloading and modular in-memory execution. The operators abused Google Drive for command-and-control, blending malicious traffic into trusted cloud activity. Researchers also noted signs of AI-assisted development. Organisations should tighten email security and monitor unusual cloud service usage.

ATTACK TYPE	Cyberespionage, APT	**SECTOR**	Government
REGION	Georgia, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan, Central Asia	**APPLICATION**	Microsoft Windows Defender, Windows, Node.js, Google Drive

Source - https://www.bitdefender.com/en-us/blog/businessinsights/silkparasite-tracking-china-nexus-apt-across-central-asia

TATA COMMUNICATIONS

Python TWINLOOT implant routes all its C2 through Microsoft services to dodge detection

Researchers have disclosed TWINLOOT, a modular, PyArmor-hardened Python implant that conceals its entire command-and-control infrastructure within trusted Microsoft services. Discovered during a July 2026 incident, it routes tasking through SharePoint Online via the Microsoft Graph API, relays interactive sessions through Microsoft Teams TURN servers, and drives traffic through a headless instance of the victim's own Edge browser.

Initial access begins with Teams-based social engineering, where an attacker posing as IT support persuades a user to run a malicious PowerShell command. Because the implant authenticates to an attacker-controlled Azure tenant, no sign-in events appear in the victim's logs. Organisations are advised to restrict PowerShell execution, disable Edge headless mode and flag connections to external SharePoint tenants.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, BFSI, Government, IT Services and Consulting
REGION	Global	**APPLICATION**	Microsoft Edge, Microsoft SharePoint Server, Python, Windows, Microsoft Office 365, Microsoft Teams, Microsoft Azure

Source - https://www.darkreading.com/cloud-security/silent-twinloot-threat-operates-microsoft-cloud

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