TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: July 14, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As July 2026 progresses, the cyber threat landscape shows no sign of easing, with threat actors deploying ever more sophisticated and coordinated tactics across highly interconnected digital environments. Traditional defence models are being tested as adversaries exploit systemic weaknesses at scale. To sustain resilience and competitive advantage, organisations must strengthen foundational security controls, adopt layered defence strategies, and embed forward-looking intelligence throughout their operational frameworks.

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

TATA COMMUNICATIONS

State-linked actor wields modular C2 framework against government and IT targets

The attack chain begins with SysAid's software update feature, which the adversary abuses to initiate a DLL side-loading sequence that executes a trojanised uxtheme.dll containing the Cavern Agent. The agent then loads a standalone communication module to contact its command-and-control server, fetching additional post-exploitation modules on the fly over HTTPS or WebSocket.

Researchers uncovered five distinct DLL modules supporting file operations, SQL database manipulation, Active Directory reconnaissance, network scanning, and SOCKS5 tunnelling. A defining trait is the framework's use of three different .NET compilation targets, whereby the compilation format itself becomes an anti-analysis layer, forcing reverse engineers into multiple toolsets and metadata-reconstruction workflows alongside per-module isolation.

ATTACK TYPE	Malware, Cyber-espionage, APT	**SECTOR**	Government, IT Services and Consulting
REGION	Middle East, Israel	**APPLICATION**	Microsoft Active Directory Services, Microsoft SQL Server, Windows

Source - https://thehackernews.com/2026/07/iran-linked-hackers-use-new-cavern-c2.html

TATA COMMUNICATIONS

Microsoft patches critical flaw, allowing low-privileged users to seize tenant-wide control

Classified under CWE-862, the flaw stems from the system failing to verify correctly whether a user is authorised to perform a given operation, thereby allowing a remote attacker to elevate their privileges. Its CVSS 3.1 vector confirms network access, low attack complexity, low privileges required, and no user interaction, whilst a changed security scope lets attackers affect resources beyond their initial access zone.

With high impact on both confidentiality and integrity, an attacker could read and alter any emails, calendars, and contacts across the organisation, sending messages impersonating executives or destroying critical data. Exploitation could enable malicious mailbox forwarding rules, establish persistence to survive service restarts, and ultimately facilitate ransomware deployment through phishing emails bearing a trusted sender's signature.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, BFSI, IT, Government, Aerospace, Business, Airlines, Automobile, Retail and Distribution, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Microsoft Exchange Server

Source - https://1275.ru/vulnerability/kriticheskaya-uyazvimost-v-microsoft-exchange-online-otkryvaet-put-k-polnomu-kontrolyu-nad-korporativnoy-pochtoy_31447

TATA COMMUNICATIONS

Bad Epoll kernel bug enables reliable privilege escalation with no available workaround

Bad Epoll is a use-after-free bug in which two parts of the kernel attempt to clean up the same internal object simultaneously, one freeing the memory while the other is still writing to it. That brief collision allows an attacker to corrupt kernel memory and climb from a normal account up to root.

The collision window spans only about six machine instructions, so a random attempt rarely lands within it. However, the researcher's exploit widens that window and retries without crashing, reaching root roughly 99% of the time on tested systems. More concerning still, it can be triggered from inside Chrome's renderer sandbox and can reach Android.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, BFSI, IT, Government, Aerospace, Business, Airlines, Automobile, Retail and Distribution, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Linux

Source - https://thehackernews.com/2026/07/new-bad-epoll-linux-kernel-flaw-lets.html

TATA COMMUNICATIONS

Avalon framework uses MSBuild and ISO files before the CrownX ransomware deployment

Documented by Cyber analysts on 2 July 2026, the intrusion began with a spoofed legal-document email directing victims to a password-protected archive hosted on Proton Drive. Inside sat an ISO image containing a document-themed shortcut that, rather than opening a PDF, launched cmd.exe to copy and execute a disguised MSBuild project holding inline C# and an encrypted managed stage.

Before encryption, Avalon operates as a central post-exploitation framework, interfering with Event Tracing for Windows and AMSI inspection before mapping its next payload directly into memory. It harvests browser credentials, wallets, and remote-access material, prepares lateral movement, and sabotages recovery by deleting shadow copies and targeting Windows Recovery Environment paths ahead of CrownX deployment.

ATTACK TYPE	Ransomware, Malware	**SECTOR**	Business, IT Services and Consulting
REGION	Global	**APPLICATION**	Chromium, Mozilla Firefox, Windows, Microsoft Teams, Slack, Discord

Source - https://trojan-killer.net/avalon-crownx-ransomware-msbuild-cleanup/

TATA COMMUNICATIONS

SharkLoader malware targets government and diplomatic networks via software disguises

The StrikeShark cluster does not rely on a single-entry point, exploiting known flaws in software such as Microsoft Exchange, SharePoint, Fortinet appliances, and Cisco IOS XE, whilst also distributing droppers disguised as Cisco AnyConnect and Google Update. Once launched, these fake installers quietly plant the loader while the victim believes legitimate software is being updated.

SharkLoader abuses DLL sideloading, hijacking the genuine Windows binary SystemSettings.exe to load a malicious SystemSettings.dll, ensuring security tools relying on file reputation flag nothing unusual. It further hooks numerous Windows API calls, redirects them to dynamically generated system calls, tampers with Event Tracing for Windows logging, and spoofs parent process IDs to blend into normal activity.

ATTACK TYPE	Malware	**SECTOR**	Government, Software Development
REGION	Colombia, Indonesia, Lebanon, Nepal, North Macedonia, Serbia, Syria, Taiwan	**APPLICATION**	Microsoft Exchange Server, Microsoft SharePoint Server, Cisco iOS, Windows, Cisco iOS XE, F5 BIG-IP, Zimbra Collaboration, Fortinet

Source - https://cybersecuritynews.com/hackers-use-fake-cisco-anyconnect-and-google-update-installers/

TATA COMMUNICATIONS

Agentic JADEPUFFER ransomware uses a language model to breach production database

Researchers identified JADEPUFFER as an agentic threat actor executing the first documented end-to-end extortion campaign driven entirely by a large language model. Exploiting CVE-2025-3248, a missing-authentication flaw in Langflow's code validation endpoint, the agent achieved unauthenticated remote code execution, then swept the host for cloud credentials, cryptocurrency wallets, and database configurations without human oversight.

Demonstrating machine-speed troubleshooting, the agent accessed a MinIO instance using default credentials, extracted access keys, and then compromised an Alibaba Nacos service by exploiting an authentication bypass and forging tokens. It ultimately encrypted 1,342 Nacos configurations using a randomly generated AES key that was never saved, rendering the data permanently unrecoverable even after payment.

ATTACK TYPE	Ransomware, Malware	**SECTOR**	IT Services and Consulting
REGION	Global	**APPLICATION**	Apple macOS, PostgreSQL, Windows, Linux

Source - https://cyberpress.org/jadepuffer-breaches-production-database/

TATA COMMUNICATIONS

Anubis ransomware exploits CitrixBleed 2 and legitimate remote administration tools

Initial access generally fell into two categories: valid VPN credential use and exploitation of CitrixBleed 2, a pre-authentication memory disclosure vulnerability that can expose session material from affected NetScaler appliances, enabling session hijacking and multi-factor authentication bypass. Malicious VPN authentication was then followed by RDP and SMB activity, leading to credential access, PsExec service creation, and RMM deployment.

A defining pattern was the deployment of legitimate RMM tools for persistent access, including ScreenConnect, Zoho Assist, MeshAgent, Remotely, UltraVNC, and Total Software Deployment, which provided interactive access, file transfer, and service-based persistence whilst blending in with software commonly used by IT teams. Some intrusions also involved CloudFlare tunnels and SSH-based SOCKS tunnelling to establish alternate egress paths.

ATTACK TYPE	Cybercrime, Ransomware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Windows Defender, Microsoft Edge, Citrix NetScaler, Windows, Linux, Google Chrome, Synology, ULTRA VNC, ScreenConnect

Source - https://arcticwolf.com/resources/blog/citrixbleed-2-to-cloudflared-the-tools-and-techniques-behind-anubis-ransomware-attacks/

TATA COMMUNICATIONS

Citrix urges urgent NetScaler upgrades after six vulnerabilities threaten enterprise gateways

Citrix released security updates addressing multiple flaws in NetScaler ADC and NetScaler Gateway that could be exploited to facilitate arbitrary file reads or trigger denial-of-service conditions. The most severe, including CVE-2026-8451, CVE-2026-8452, and CVE-2026-8655, each carry a CVSS score of 8.8 and affect appliances configured as SAML IDP, Gateway, AAA virtual server, or specific load-balancing deployments.

Cyber researchers reported that CVE-2026-8451 stems from how NetScaler parses SAML authentication requests, sharing the same root cause as an earlier March 2026 flaw and resulting in out-of-bounds memory reads. Researchers cautioned that memory management remains fragile within these appliances, warning that even accidental misconfiguration could expose leaked memory to attackers.

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

Source - https://thehackernews.com/2026/07/citrix-patches-six-netscaler-flaws.html

TATA COMMUNICATIONS

Critical Oracle E-Business Suite flaw enables full unauthenticated remote system takeover

Threat actors are actively exploiting CVE-2026-46817, with live attack activity captured across honeypot infrastructure over the weekend of 27–28 June 2026. Residing in the Oracle Payments product, the flaw allows an unauthenticated attacker with network access via HTTP to fully compromise confidentiality, integrity, and availability. Affected versions span Oracle E-Business Suite 12.2.3 through 12.2.15.

The captured attack traffic revealed targeted POST requests to the Oracle iPayment file transmission endpoint, submitting a crafted XML delivery payload. Notably, no public proof-of-concept code exists, indicating the threat actor may be operating with privately developed exploit capabilities. Oracle addressed the vulnerability in its May 2026 Critical Security Patch Update, urging customers to apply the fix immediately.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Oracle, Oracle E-Business Suite

Source - https://www.cryptika.com/hackers-exploiting-critical-oracle-e-business-suite-vulnerability-actively-in-attacks/

TATA COMMUNICATIONS

Zero-Click prompt injection turns popular AI coding assistant into a remote attack vector

The two vulnerabilities, collectively named DuneSlide, carry a CVSS score of 9.8 and exploit weaknesses in Cursor's sandboxed command-execution model, designed to run terminal commands without user approval. Crucially, exploitation requires no direct user interaction — merely a benign prompt that processes attacker-controlled content from sources such as malicious MCP servers or compromised web results.

The first flaw manipulates the working directory parameter, which Cursor fails to validate when the LLM sets it dynamically, enabling arbitrary file writes that can disable sandbox protections. The second exploits symlink resolution failures, allowing attackers to overwrite protected binaries and achieve sandbox escape. Fixes were rolled out in Cursor version 3.0.

ATTACK TYPE	Vulnerability	**SECTOR**	IT Services and Consulting, Software Development
REGION	Global	**APPLICATION**	Apple macOS, Windows, Linux, Cursor IDE

Source - https://gbhackers.com/critical-cursor-ide-flaws/

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