TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: July 28, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As July 2026 is coming towards an end, the cyber threat landscape continues to intensify, with threat actors orchestrating increasingly sophisticated and coordinated campaigns across deeply interconnected digital environments. Conventional defence models are under mounting strain as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now demands that organisations reinforce foundational security controls, embrace layered defence strategies, and embed forward-looking intelligence across every layer of their operational frameworks.

Amid this evolving environment, the Tata Communications Cyber Threat Intelligence report continues to serve as an indispensable resource for security practitioners. Published weekly, it delivers sharp, timely analysis of emerging threat campaigns, evolving attacker methodologies, and sector-specific risk exposures. By translating intelligence into practical defence guidance, it equips security teams to anticipate, counter, and contain threats with confidence — protecting the continuity of critical operations at scale.

TATA COMMUNICATIONS

Record-breaking Microsoft update patches numerous security flaws and three zero-days

Microsoft's July 2026 Patch Tuesday has addressed a record haul of vulnerabilities spanning Windows, Office, Azure, Exchange Server, Visual Studio and numerous other products. The release, among the largest the company has issued, includes three zero-day flaws: two already exploited in attacks and one publicly disclosed ahead of a fix. Microsoft attributed the surge partly to AI-driven vulnerability discovery.

The two exploited zero-days affect Active Directory Federation Services and SharePoint Server, and both have been added to CISA's Known Exploited Vulnerabilities catalogue. Successful exploitation across the wider release could enable remote code execution, privilege escalation, information disclosure, security feature bypass and unauthorised access. Administrators are urged to apply the updates promptly, prioritising internet-facing identity and collaboration systems.

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-july-2026/v

INTRODUCTION | MICROSOFT JULY PATCH TUESDAY FIXES RECORD HAUL OF FLAWS AND THREE ZERO-DAYS | CISA WARNS OF ACTIVE EXPLOITATION TARGETING SONICWALL SMA1000 APPLIANCES | SHADOWRECRUIT CAMPAIGN ABUSES CONTROLR AND GOOGLE SHEETS TO SPY ON JOB SEEKERS | CERT-IN WARNS OF CRITICAL FILE UPLOAD FLAW IN POPULAR JOOMLA PAGE BUILDER | TELEPUZ USES POWERSHELL DELIVERY AND STEALTHY CHANNELS TO EVADE DETECTION | WORLDLEAKS ABANDONS RANSOMWARE ENCRYPTION FOR A PURE DATA THEFT EXTORTION MODEL | CLICKFIX WEAPONISES CLAUDE SHARED CHATS TO DELIVER CREDENTIAL-STEALING MACOS MALWARE | EVEREST RANSOMWARE ENCRYPTOR USES STEALTH AND NETWORK TRICKS TO MAXIMISE DAMAGE | CURSOR IDE EXECUTES HIDDEN GIT BINARY FROM REPOSITORIES WITHOUT USER APPROVAL | ESPIONAGE OPERATION USES TELEGRAM BOTS TO BACKDOOR GOVERNMENT COMPUTER SYSTEMS

TATA COMMUNICATIONS

CISA flags actively exploited SonicWall SMA1000 flaws and orders urgent federal patching

The US Cybersecurity and Infrastructure Security Agency has added two SonicWall SMA1000 vulnerabilities, CVE-2026-15409 and CVE-2026-15410, to its Known Exploited Vulnerabilities catalogue after confirming active exploitation. The critical server-side request forgery flaw carries a CVSS score of 10.0, while the high-severity code injection flaw scores 7.2. Models 6210, 7210 and 8200v are affected, having been exploited as zero-days.

SonicWall has released emergency hotfixes and is urging customers to upgrade immediately, warning that patching alone may not suffice. Administrators are advised to review logs for indicators of compromise and reset credentials where necessary. Federal civilian agencies must remediate affected systems by 17 July 2026 under Binding Operational Directive 26-04, reflecting the appliances' history as attacker targets.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Hospitality, Manufacturing, IT, Government, Business, BFSI, Aviation, Retail and Distribution, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Sonicwall SMA, Sonicwall Firewall

Source - https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-sma1000-flaws-exploited-in-zero-day-attacks-patch-now/

TATA COMMUNICATIONS

ShadowRecruit targets job seekers using fake recruitment documents and SheetAgent RATs

Security researchers have uncovered Operation ShadowRecruit, a multi-stage malware campaign targeting Indian government job seekers through fake Cabinet Secretariat recruitment notices. Victims receive a ZIP archive containing a disguised shortcut file that triggers a PowerShell downloader and a .NET loader. These components ultimately deploy a custom remote access trojan while a decoy document distracts the target.

The operation abuses legitimate ControlR remote management software to establish persistent access, alongside a bespoke trojan dubbed SheetAgent that uses Google Sheets as a covert command-and-control channel. Embedded credentials let it read attacker instructions and return stolen data. Researchers attribute the campaign with moderate confidence to APT36, citing tradecraft matching the group's previous espionage operations.

ATTACK TYPE	Malware, Cyber-espionage	**SECTOR**	Government, Education, IT Services and Consulting
REGION	India	**APPLICATION**	Windows

Source - https://www.seqrite.com/blog/operation-shadowrecruit-a-recruitment-themed-malware-campaign-leveraging-controlr-and-google-sheets-to-target-indian-job-seekers/

TATA COMMUNICATIONS

Unpatched Joomla sites face full compromise through critical SP Page Builder upload flaw

CERT-In has issued Vulnerability Note CIVN-2026-0364 warning of a critical flaw in JoomShaper's SP Page Builder extension for Joomla. Tracked as CVE-2026-48908 and carrying a maximum CVSS score of 10.0, the vulnerability allows unauthenticated attackers to upload malicious PHP files through an unprotected icon-upload endpoint, enabling remote code execution. All versions up to and including 6.6.1 are affected.

Successful exploitation could grant attackers complete control of affected websites, allowing web shells, data theft or defacement. The flaw is being actively exploited in the wild and has been added to the Known Exploited Vulnerabilities catalogue. JoomShaper has resolved the issue in version 6.6.2, and administrators are urged to update immediately and audit sites for compromise.

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

Source - https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2026-0364

TATA COMMUNICATIONS

TELEPUZ malware uses PowerShell and resilient fallback channels for persistent access

Security researchers have detailed TELEPUZ, a modular Windows backdoor active since late April 2026 and spreading rapidly through malware-as-a-service operations. Infections begin with a social-engineering lure that tricks users into running a PowerShell command, which downloads a disguised DLL. The library then registers a service and drops additional files across common user directories to establish persistence.

Once installed, TELEPUZ elevates its privileges, disables security monitoring and harvests credentials, browser cookies and other confidential data. Extensive anti-analysis and sandbox-evasion checks help it avoid detection, while fallback command channels hidden within Telegram, Steam and a blockchain smart contract ensure resilient operator control. The threat exposes organisations to credential theft, financial fraud and operational disruption.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, BFSI, IT, Government, Education
REGION	Global	**APPLICATION**	Microsoft Edge, Google Chrome OS, Windows, Google Chrome, PowerShell

Source - https://www.elastic.co/security-labs/telepuz-maas-malware-clickfix

TATA COMMUNICATIONS

WorldLeaks EaaS steals corporate data and threatens leaks to pressure victims into paying

WorldLeaks is an active Extortion-as-a-Service operation that emerged in January 2025 as a rebrand of the Hunters International ransomware group. Rather than encrypting files for ransom, it has pivoted to a data extortion model, stealing sensitive information and threatening to publish it unless victims pay. Affiliates are supplied with a custom tool that automates data exfiltration.

The group targets organisations across numerous industries, gaining access through phishing, stolen credentials, vulnerable public-facing applications and compromised VPNs lacking multi-factor authentication. Once inside, it deploys sophisticated infrastructure to intensify pressure, including dedicated leak sites, victim portals and a journalist platform offering early access to stolen files. Since launch, WorldLeaks has claimed well over one hundred victims worldwide.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Manufacturing, IT, Government, Transportation, Education, Energy, Hospitality
REGION	North America, South America, Europe, Africa, India, Asia	**APPLICATION**	Windows, Sonicwall SMA, PowerShell

Source - Threat Intel Team Internal Research

TATA COMMUNICATIONS

ClickFix campaign abuses Claude shared chats to spread new macOS information stealer

A sophisticated ClickFix campaign has abused Claude's legitimate chat-sharing feature to distribute MacSync Stealer targeting macOS users. Uncovered by Zscaler, the operation used paid search advertising to lure people seeking Claude towards shared chat links hosted on the platform's genuine domain. Posing as Apple Support, the fake conversations instructed victims to paste an obfuscated command into Terminal.

Executing the command triggered a multi-stage infection chain that quietly fetched further payloads while concealing its activity. Deployed via AppleScript, MacSync Stealer harvested credentials, browser data, cryptocurrency wallets and developer keys before erasing its traces. Anthropic confirmed its platform was not compromised and has removed the offending chats, but researchers urge users never to paste unfamiliar Terminal commands.

ATTACK TYPE	Information gathering, Social engineering, Cybercrime, Malware	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Apple macOS, Microsoft Edge, Apple Safari, Chromium, Opera Browser, Google Chrome, Telegram, Anthropic Claude

Source - https://cybersecuritynews.com/shared-claude-chats-macsync-stealer/

TATA COMMUNICATIONS

Everest ransomware uses Wake-on-LAN and ConfuserEx to maximise enterprise encryption

Security researchers have analysed a newly discovered Everest ransomware encryptor, a ConfuserEx-protected .NET binary engineered to frustrate detection and analysis. Although its code declares RSA-4096 and AES-256, the malware quietly downgrades to RSA-1024 and AES-128-CBC at runtime. Extensive obfuscation, encrypted strings and hundreds of runtime decryption routines significantly complicate both static analysis and automated defence.

Before encrypting, Everest weakens its host extensively, sabotaging recovery options, disabling security controls, re-enabling the legacy SMBv1 protocol and continuously terminating security, backup, database and analysis tools. Unusually, it broadcasts Wake-on-LAN packets to rouse dormant machines, widening its reach before encrypting local and network-accessible files. Researchers note this noisy sequence offers defenders a valuable detection opportunity.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, Manufacturing, Government, IT Services and Consulting
REGION	North America, Europe, Asia	**APPLICATION**	Microsoft Excel, Microsoft Exchange Server, Microsoft IIS, OneNote, Outlook, PowerPoint, Microsoft SQL Server, Microsoft Visio, Microsoft Word, Mozilla Firefox, Mozilla Thunderbird, MySQL, Oracle Database, Windows, Google Chrome

Source - https://gbhackers.com/everest-ransomware-attack/

TATA COMMUNICATIONS

Cursor zero-day runs malicious git binary automatically when developers open a repository

A zero-day vulnerability in the AI-powered Cursor code editor allows a malicious git.exe file planted in a repository's root to execute automatically on Windows. Discovered by Mindgard in December 2025, the flaw stems from Cursor's Git binary discovery process, which scans the active workspace and runs the file without any prompts, warnings, or user approval.

Exploitation grants arbitrary code execution under the logged-in user's privileges, potentially delivering ransomware, keyloggers, or credential harvesters. Mindgard demonstrated the issue using a renamed Calculator binary, which relaunched repeatedly while the project stayed open. The flaw remains unpatched. Administrators are advised to restrict binary execution from developer workspaces using AppLocker and avoid opening untrusted repositories.

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

Source - https://securityonline.info/cursor-zero-day-vulnerability/

INTRODUCTION | MICROSOFT JULY PATCH TUESDAY FIXES RECORD HAUL OF FLAWS AND THREE ZERO-DAYS | CISA WARNS OF ACTIVE EXPLOITATION TARGETING SONICWALL SMA1000 APPLIANCES | SHADOWRECRUIT CAMPAIGN ABUSES CONTROLR AND GOOGLE SHEETS TO SPY ON JOB SEEKERS | CERT-IN WARNS OF CRITICAL FILE UPLOAD FLAW IN POPULAR JOOMLA PAGE BUILDER | TELEPUZ USES POWERSHELL DELIVERY AND STEALTHY CHANNELS TO EVADE DETECTION | WORLDLEAKS ABANDONS RANSOMWARE ENCRYPTION FOR A PURE DATA THEFT EXTORTION MODEL | CLICKFIX WEAPONISES CLAUDE SHARED CHATS TO DELIVER CREDENTIAL-STEALING MACOS MALWARE | EVEREST RANSOMWARE ENCRYPTOR USES STEALTH AND NETWORK TRICKS TO MAXIMISE DAMAGE | CURSOR IDE EXECUTES HIDDEN GIT BINARY FROM REPOSITORIES WITHOUT USER APPROVAL | ESPIONAGE OPERATION USES TELEGRAM BOTS TO BACKDOOR GOVERNMENT COMPUTER SYSTEMS

TATA COMMUNICATIONS

New malware suite abuses Telegram to breach and control government computer systems

Security researchers have uncovered a targeted espionage campaign against government entities, attributed with moderate-to-high confidence to a threat actor operating from East Asia. The operation deploys three previously undocumented malware families — TELESHIM, MIXEDKEY and BINDCLOAK — through a multi-stage attack chain. Initial access begins with a weaponised ISO file that sideloads a malicious DLL via a legitimate signed executable.

The first-stage TELESHIM backdoor abuses Telegram's Bot API for command-and-control, allowing malicious traffic to blend with legitimate communications. Both TELESHIM and MIXEDKEY employ heavy code obfuscation and anti-analysis defences, while environmental keying ties execution to each victim machine. Organisations are urged to monitor for the reported indicators and scrutinise ISO-based lures referencing government or energy-sector themes.

ATTACK TYPE	Malware, Cyber-espionage	**SECTOR**	Healthcare, Government, Defence, BFSI
REGION	Middle East, East Asia	**APPLICATION**	Windows

Source - https://cyberpress.org/teleshim-targets-middle-east-governments/

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