TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: June 23, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As June 2026 nears its end, the cyber threat landscape shows no sign of abating, with threat actors deploying increasingly sophisticated and coordinated tactics across highly interconnected digital environments. Conventional defence models continue to be tested as adversaries exploit systemic vulnerabilities at scale. Organisations must reinforce foundational security controls, adopt layered defence strategies, and embed forward-looking intelligence into operational frameworks to sustain resilience and competitive advantage.

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

TATA COMMUNICATIONS

Microsoft’s June Patch addresses 200 flaws, including three publicly disclosed zero-days

Microsoft's June 2026 Patch Tuesday released security updates for 200 vulnerabilities across Windows and its broader product ecosystem, including Office, Azure, Exchange Server, Hyper-V, and developer tools. Of the 33 Critical-rated flaws, 28 are remote code execution vulnerabilities, and the release also covers 65 elevations of privilege, 19 security feature bypasses, and 30 information disclosure issues.

The update patches three publicly disclosed zero-day vulnerabilities, none known to be actively exploited at release. Included are GreenPlasma (CVE-2026-45586), a Windows CTFMON privilege escalation granting SYSTEM access; the HTTP/2 Bomb (CVE-2026-49160), a denial-of-service flaw causing server resource exhaustion; and YellowKey (CVE-2026-50507), a BitLocker bypass allowing physical access to encrypted drives.

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

Source - https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2026-patch-tuesday-fixes-3-zero-day-200-flaws/

TATA COMMUNICATIONS

Ivanti patches severe Sentry vulnerabilities, enabling remote root-level code execution

Ivanti has released patches addressing two critical vulnerabilities in its Sentry secure mobile gateway solution, formerly known as MobileIron Sentry, including a maximum-severity flaw enabling remote attackers to execute code with root privileges. The first, tracked as CVE-2026-10520, stems from an OS command injection weakness, whilst the appliance itself secures traffic between back-end corporate systems and remote mobile devices.

The second flaw, CVE-2026-10523, is a critical authentication bypass exploitable remotely by unauthenticated attackers to create rogue administrative accounts and gain full administrative access. Ivanti patched both issues with the release of Sentry versions R10.5.2, R10.6.2, and R10.7.1, stating it had no evidence of exploitation in the wild and advising administrators to upgrade promptly.

ATTACK TYPE	Malware, Cyber-espionage	**SECTOR**	Healthcare, Tourism, IT, Government, Business, BFSI, Aviation, Automobile, Broadcast Media Production, Retail and Distribution, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Ivanti

Source - https://www.bleepingcomputer.com/news/security/new-max-severity-ivanti-sentry-flaw-allows-code-execution-as-root/

TATA COMMUNICATIONS

Iran-nexus BLUERABBIT backdoor combines data theft, file encryption, and disk wiping

BLUERABBIT is a Golang-based backdoor attributed to a likely Iran-nexus threat actor, first observed in mid-to-late March 2026 and suspected of targeting Israeli entities. According to the Google Threat Intelligence Group, the malware is linked to the same activity cluster previously responsible for BLUEWIPE and SEWERGOO in June 2025. Critically, configuration items, including C2 addresses and credentials, are AES-protected within the binary.

Rather than relying on conventional HTTP callbacks, the malware leverages RabbitMQ for tasking, Redis for state management, and MinIO for bulk data exfiltration. Before destruction begins, it takes ownership of critical boot files and modifies the registry to disable automatic recovery, establishing persistence through a scheduled task named OneDrive Update that deliberately impersonates a legitimate Microsoft service.

ATTACK TYPE	Malware, Cyber-espionage, APT	**SECTOR**	Healthcare, BFSI, IT, Government
REGION	Israel	**APPLICATION**	Windows

Source - https://cyberpress.org/bluerabbit-targets-windows-files/

TATA COMMUNICATIONS

Data extortion actor Pink deploys evasive phishing kits to defeat MFA and passkeys

Pink follows a faster, stealthier credential-driven model built around vishing, evasive phishing kits, and targeted attacks against high-value organisations. The group impersonates internal IT support, luring targets into surrendering credentials on phishing sites before exfiltrating data from SharePoint and OneDrive. Extortion demands are then distributed via compromised emails and internal Teams messages, accompanied by a 72-hour communication deadline.

Pink's two phishing kits target Microsoft Entra ID and Okta environments, employing extensive sandbox evasion and backend-controlled access gates that withhold content until operators manually authorise each session. Operating real-time command-and-control connections, the kits defeat push-based MFA through authenticator number-matching and attempt passkey subversion by socially engineering targets into surrendering recovery words or registering attacker-controlled credentials on their devices.

ATTACK TYPE	Cyber-espionage	**SECTOR**	Healthcare, BFSI, Construction, IT, Transportation, Logistics and Shipping
REGION	Japan, the UK, Ireland, the United States	**APPLICATION**	Microsoft SharePoint Server, OneDrive, Microsoft Office 365, Microsoft Teams, Microsoft Entra, Okta

Source - https://socradar.io/blog/pink-data-extortion-group-phishing-kits/

TATA COMMUNICATIONS

Token forging flaw in SimpleHelp grants attackers privileged remote management access

The vulnerability resides within SimpleHelp's single sign-on mechanism, where identity tokens submitted during OIDC login are accepted without verifying their cryptographic signature. Consequently, a remote attacker can construct an altered token to spoof an identity and obtain a fully authenticated technician session. In vulnerable configurations, this also allows adversaries to circumvent multi-factor authentication protections entirely, undermining a critical security layer.

Once inside, an attacker gains highly privileged capabilities, as a newly created technician account can execute malicious scripts and remote into managed endpoints by default. Because technicians can self-register their own MFA method on first login, attackers bypass existing validation policies. Shodan data revealed internet exposure surging from roughly 3,400 servers to nearly 14,000 active instances.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Tourism, Manufacturing, IT, Government, Defence, Business, BFSI, Aviation, Retail and Distribution, Telecommunications, Logistics and Shipping
REGION	Global	**APPLICATION**	SimpleHelp RMM, Apple macOS, Windows, Linux

Source - https://securityonline.info/simplehelp-authentication-bypass/

TATA COMMUNICATIONS

Injection vulnerability in Microsoft Teams for Android risks confidential data exposure

Microsoft has disclosed a high-severity vulnerability, CVE-2026-42835, carrying a CVSS v3.1 score of 8.1, affecting the Teams application for Android. Classified under CWE-74, the flaw stems from insufficient filtering of user input before it is passed to downstream components, enabling an authenticated attacker to inject malicious control sequences into communication workflows. Notably, exploitation requires no user interaction.

The attack vector is network-based, the exploitation complexity is low, and only minimal privileges are required, making the flaw attractive to adversaries who already hold limited access. A successful attack could expose message contents, authentication tokens, and service data. Microsoft has released fixes, urging organisations to deploy updates promptly and tighten mobile device management monitoring for anomalies.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, Tourism, BFSI, IT, Government, Business, Aviation, Automobile, Broadcast Media Production, Retail and Distribution, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Android, Microsoft Teams

Source - https://1275.ru/vulnerability/uyazvimost-v-microsoft-teams-dlya-android-pozvolyaet-raskryvat-konfidentsialnye-dannye-cve-2026-42835-s-otsenkoy-8-1_28599

TATA COMMUNICATIONS

MLTBackdoor uses ClickFix lures and DLL sideloading to evade detection and analysis

Threat analysts have identified MLTBackdoor, a newly discovered backdoor assessed as likely linked to a ransomware-related threat actor. Victims are lured from an automotive-themed webpage into running commands that fetch a disguised archive from a DGA-generated domain, decrypt an RC4-protected payload, and install the malware through DLL sideloading using the signed Microsoft Defender binary mpextms.exe. A single generated domain handled both delivery and command-and-control traffic.

The malware resists detection using heavy LLVM-based obfuscation, mixed boolean-arithmetic, control-flow flattening, API hashing, and Hell's Gate-style indirect system calls, with roughly 95% of the code comprising junk mathematical operations. Rather than exiting when detecting analysis environments, it performs ten anti-analysis checks, then reports the results to operators and includes a Beacon Object File loader expanding post-exploitation capability in memory.

ATTACK TYPE	Malware	**SECTOR**	IT, Healthcare, Financial Services, Manufacturing, Government, Transportation, Education, Energy, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Windows Defender

Source - https://www.zscaler.com/blogs/security-research/technical-analysis-mltbackdoor

TATA COMMUNICATIONS

CISA urges immediate patching of exploited Chrome engine and Cisco SD-WAN flaws

CISA expanded its Known Exploited Vulnerabilities catalogue following evidence of active real-world targeting. The first addition, CVE-2026-11645, a Google Chromium V8 engine out-of-bounds flaw, allows remote threat actors to achieve code execution by luring victims to a crafted malicious HTML page, escaping the browser sandbox and posing a significant risk to enterprise endpoints.

The second addition, CVE-2026-20245, carries a CVSS score of 7.8 and affects Cisco Catalyst SD-WAN Manager components. Stemming from improper input encoding within the command-line interface, the flaw enables a local authenticated attacker to supply a crafted file and execute arbitrary commands as root. Early investigations revealed limited real-world cases where adversaries pushed unauthorised configuration changes directly to edge hardware.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Google ChromeOS, Cisco SD-WAN, Google Chrome

Source - https://securityonline.info/cisa-active-exploit-catalog-additions/

INTRODUCTION | GREENPLASMA AND YELLOWKEY ZERO-DAYS AMONG 200 FLAWS FIXED IN JUNE PATCH | IVANTI URGES URGENT PATCHING AS CRITICAL SENTRY GATEWAY FLAWS ARE DISCLOSED | STEALTHY BLUERABBIT BACKDOOR BLENDS C2 WITH ENTERPRISE MESSAGING TOOLS | VOICE PHISHING CREW IMPERSONATES IT, TARGETING ENTERPRISE CREDENTIALS AND DATA | CRITICAL SIMPLEHELP FLAW LETS ATTACKERS FORGE TOKENS AND SEIZE TECHNICIAN CONTROL | HIGH-SEVERITY TEAMS FLAW ON ANDROID EXPOSES SENSITIVE DATA THROUGH INJECTION | MLTBACKDOOR ABUSES CLICKFIX SOCIAL ENGINEERING AND BEACON OBJECT FILE LOADING | CISA FLAGS EXPLOITED CHROME AND CISCO SD-WAN FLAWS FOR URGENT PATCHING | ORACLE ISSUES EMERGENCY ALERT AS PEOPLESOFT ZERO-DAY DRIVES MASS DATA THEFT | NEW OP-512 CLUSTER DEPLOYS CUSTOM WEB SHELLS AGAINST LEGACY IIS SERVERS

TATA COMMUNICATIONS

ShinyHunters exploits Oracle PeopleSoft RCE flaw to breach organisations globally

Oracle released an out-of-band security alert for CVE-2026-35273, a critical unauthenticated remote code execution flaw carrying a CVSS score of 9.8, affecting PeopleSoft Enterprise PeopleTools versions 8.61 and 8.62. Mandiant attributed active exploitation to UNC6240, also known as ShinyHunters, observing attacks between 27 May and 9 June 2026 — predating Oracle's advisory and confirming zero-day exploitation.

The campaign heavily targeted higher education, with 68% of 100+ notified organisations being universities and colleges. After gaining initial access, attackers deployed a customised version of the MeshCentral remote monitoring platform, disguised as legitimate Microsoft Azure services, to establish persistence. The University of Nottingham was among the first confirmed victims, with attackers claiming theft of 40GB of personal data.

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

Source - https://cloud.google.com/blog/topics/threat-intelligence/shinyhunters-targets-education-sector-oracle-exploit

TATA COMMUNICATIONS

OP-512 threat actor exploits end-of-life IIS servers for stealthy espionage operations

Threat researchers assessed with moderate to high confidence that OP-512 conducted espionage through a compromised IIS web server, targeting an organisation whose sector and geography aligned with China-linked intelligence priorities. It is the fourth such cluster after CL-STA-0048, DragonRank, and GhostRedirector to single out IIS web servers over the past twelve months, underscoring a persistent focus on this technology across the espionage ecosystem.

The attacker targeted a legacy server running Windows Server 2016 with end-of-life .NET Framework 4.0, using the worker process to drop a web shell into the upload directory. A self-reporting mechanism then transmitted the shell's location via DNS query, with an HTTP request as a fallback. OP-512 subsequently attempted to escalate privileges to the SYSTEM level using the Potato Suite.

ATTACK TYPE	Cyber-espionage, APT	**SECTOR**	IT, Government, Telecommunications
REGION	Global	**APPLICATION**	Microsoft Windows Server 2016, Microsoft .NET Framework, Microsoft Internet Information Services (IIS)

Source - https://thehackernews.com/2026/06/new-threat-cluster-op-512-targets.html

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