TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: August 18, 2026

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

The cyber threat landscape continues to evolve in August 2026, with threat actors mounting ever more sophisticated and tightly coordinated campaigns across deeply interconnected digital environments. Conventional defence models are being pushed to their limits as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now hinges on organisations reinforcing foundational security controls, adopting layered defence strategies, and weaving forward-looking intelligence into every layer of their operational frameworks.

In this fast-shifting environment, the Tata Communications Cyber Threat Intelligence report remains an indispensable resource for security practitioners. Published weekly, it offers 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 — safeguarding the continuity of critical operations at scale.

TATA COMMUNICATIONS

Leaked toolkit exposes Gentlemen intrusion using EtherRAT for stealthy command and control

Researchers have uncovered an exposed open directory on infrastructure linked to an affiliate of The Gentlemen ransomware operation, capturing an active intrusion toolkit mid-campaign. The recovered files reveal an operator preparing long-term access to Windows domains through scheduled tasks, PowerShell, SMB, and WMI, alongside credential theft utilities, privilege-escalation tools, and multiple layered command-and-control channels.

The standout payload, EtherRAT, is a Node.js implant that avoids hardcoding its command server. Instead, it queries an Ethereum smart contract through public RPC services to retrieve active C2 domains, enabling resilient, takedown-resistant infrastructure rotation recorded permanently on-chain. Defenders are urged to monitor for unusual outbound blockchain traffic, suspicious scheduled tasks, and the distinctive polling headers reported by researchers.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, BFSI, Manufacturing, IT, Government, Telecommunications
REGION	UK, Estonia, Netherlands, UAE, United States	**APPLICATION**	Windows, PowerShell

Source - https://hunt.io/blog/the-gentlemen-etherrat-ethereum-smart-contract-c2

TATA COMMUNICATIONS

New backdoors target government agencies for credential theft and covert surveillance

Security researchers have uncovered an ongoing cyber-espionage campaign targeting government and public-sector organisations across Central Asia and Syria, active since January 2025. The operation deploys two previously undocumented backdoors, OctLurk, and SilkLurk, alongside a proxy utility named LurkProxy. Delivered via DLL side-loading, scheduled tasks, and services, each loader is customised per victim and decrypts its payload using machine-specific information.

Both backdoors operate largely in memory and use heavy obfuscation to frustrate sandbox analysis and reverse engineering. They download modular plugins enabling credential dumping, keylogging, network reconnaissance, document collection, remote access, and browser password theft over encrypted channels. LurkProxy, meanwhile, quietly tunnels traffic to sustain access. Organisations should audit installed software and investigate unusual remote sessions and process behaviour.

ATTACK TYPE	Malware, Cyber-espionage	**SECTOR**	Healthcare, Government, Education, Energy, Facilities Services, Logistics and Shipping
REGION	India, Indonesia, United States	**APPLICATION**	Microsoft Windows Defender, 7-Zip, Mozilla Firefox, MySQL, Windows, Google Chrome, PowerShell, NVIDIA, Telegram

Source - https://www.microsoft.com/en-us/security/blog/2026/06/24/stealc-and-amadey-breaking-down-infostealers-and-the-cybercrime-services-that-deliver-them/

TATA COMMUNICATIONS

Cisco issues fixes for critical vulnerabilities affecting SD-WAN and IOS XE software

Cisco has released a batch of security updates addressing multiple vulnerabilities across IOS, IOS XE, Catalyst SD-WAN, and Integrated Management Controller software. The most severe are three Catalyst SD-WAN flaws — CVE-2026-20303, CVE-2026-20304, and CVE-2026-20310 — each rated 9.9 and rooted in improper input validation, access control, and link resolution, alongside a critical IOS XE injection vulnerability, CVE-2026-20272, scoring 9.8.

The broader release, published on 5 August 2026, spans further weaknesses including argument injection, denial of service, improper access control, flawed resource handling, and cleartext storage of sensitive information. Cisco discovered the issues during internal reviews and reports no known exploitation. With no workarounds for the hardening advisories, customers are strongly urged to apply the fixed releases promptly.

ATTACK TYPE	Vulnerability	**SECTOR**	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	**APPLICATION**	Cisco iOS, Cisco SD-WAN, Cisco IOS XE, Cisco Integrated Management Controller (IMC), Cisco ISE, Cisco Catalyst

Source - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xmcp-thbAr34t

TATA COMMUNICATIONS

Trojanised apps deploy SparkKitty malware to steal cryptocurrency recovery phrases

SparkKitty is a cross-platform information-stealing malware targeting both Android and iOS devices, designed primarily to harvest cryptocurrency wallet seed phrases from screenshots and images stored in device galleries. First identified by Kaspersky and publicly disclosed in 2025, it evolved from the earlier SparkCat family, using optical character recognition to locate sensitive text hidden within saved photographs.

The malware spread through both official app stores and sideloaded applications, disguised as cryptocurrency, messaging, gambling, and modified social media apps. Once granted photo-library access, it silently uploads images to attacker-controlled servers, exposing not only wallet credentials but also passwords and identity documents. Users are advised to avoid storing sensitive screenshots and scrutinise app permissions carefully before granting them.

ATTACK TYPE	Malware	**SECTOR**	BFSI, Cryptocurrency
REGION	Global	**APPLICATION**	Android, Apple iOS

Source - https://zimperium.com/blog/mobile-threat-watch/sparkkitty-malware-targets-mobile-users-with-stealthy-data-theft

TATA COMMUNICATIONS

Microsoft patches Teams cloud flaws including a maximum severity privilege escalation bug

Microsoft has addressed three security vulnerabilities affecting the cloud version of Microsoft Teams, comprising two critical elevation of privilege flaws and one spoofing issue. The most severe, CVE-2026-65667, carries a maximum CVSS score of 10.0 and stems from a missing authorisation check that could let an unauthenticated attacker escalate privileges across a network without any prior access.

The remaining flaws include CVE-2026-62896 (CVSS 9.6), an improper authentication weakness allowing an authenticated attacker to elevate privileges, and CVE-2026-62918 (CVSS 7.5), which is a signature verification flaw enabling network-based message spoofing. Microsoft has fully mitigated all three issues within its own cloud infrastructure, so customers are not required to take any action or deploy patches themselves.

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

Source - https://1275.ru/vulnerability/uyazvimosti-v-microsoft-teams-pozvolyayut-povysit-privilegii-i-podmenit-dannye_34100

TATA COMMUNICATIONS

Critical ManageEngine ADAudit Plus flaw allows attackers seize servers without credentials

A maximum-severity vulnerability, tracked as CVE-2026-6516, has been disclosed in ZohoCorp's ManageEngine ADAudit Plus, an Active Directory auditing solution. Rated CVSS 10.0, the flaw stems from insufficient input validation in the agent API, enabling authentication bypass and OS command injection. It affects all builds prior to 8606, exposing organisations to unauthenticated remote code execution across their environments.

An attacker requires only network access to a vulnerable agent to execute arbitrary commands and seize full control of the host, without any credentials or user interaction. Although no active exploitation has yet been reported, the flaw's simplicity makes it an attractive target. ZohoCorp urges administrators to upgrade to build 8606 immediately and update all affected agents.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, BFSI, IT, Government, Education
REGION	North America, Australia, Europe, UK, China, Netherlands, Qatar, Turkey, United States	**APPLICATION**	Zoho ManageEngine ServiceDesk Plus, Zoho ADSelfService Plus

Source - https://1275.ru/vulnerability/kriticheskaya-uyazvimost-v-manageengine-adaudit-plus-ugrozhaet-udalyonnym-zahvatom-sistem_33341

TATA COMMUNICATIONS

DevMan RaaS operation matures into a fully managed platform for criminal affiliates

Researchers have detailed how Funky Mantis, publicly tracked as DevMan, evolved from a basic ransomware platform into a mature ransomware-as-a-service ecosystem by early 2026. The group operates a centralised web portal that consolidates payload generation, affiliate management, victim negotiations, revenue tracking, and extortion support, effectively packaging the entire attack lifecycle into a single administered service.

Evidence drawn from successive portal versions, private communications, and a Windows encryptor reveals structured workflows, including access distribution, country-specific target networks, and strict completion deadlines for affiliates. The operation struck healthcare, critical infrastructure, and commercial and public-sector organisations. Defenders are advised to focus on attacker behaviours — access, privilege escalation, lateral movement, and backup hygiene — rather than individual indicators alone.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, BFSI, IT, Business
REGION	Brazil, Chile, China, France, Italy, Morocco, Norway, Philippines, United States	**APPLICATION**	Microsoft Windows Defender, VMware ESXi, Windows, Linux, Fortinet VPN, Fortinet

Source - https://thehackernews.com/2026/07/devman-raas-portal-centralizes-payload.html

TATA COMMUNICATIONS

Interlock group abuses Volatility3 and WinPmem to steal credentials from victim memory

Sophos incident responders have detailed a March 2026 ransomware intrusion in which the Interlock group, tracked as GOLD EMBRACE, abused legitimate digital forensics tools to steal credentials. The attack began with a ClickFix-style lure when an employee searched ChatGPT for Dynamics 365 and was redirected to a compromised website, then tricked into running a malicious command.

Attackers deployed WinPmem to capture system memory, then ran Volatility3 to extract NTLM hashes and cached credentials. The intrusion progressed through LDAP reconnaissance, Kerberoasting, NTLM downgrade attacks, and lateral movement to domain controllers, ending in data exfiltration, hypervisor lockout, and ransomware deployment. Organisations are urged to investigate any unsanctioned use of forensic utilities across their environments.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare, IT, Education, BFSI
REGION	North America, Europe	**APPLICATION**	Microsoft Windows Defender, Windows

Source - https://securityonline.info/interlock-ransomware-volatility3/

TATA COMMUNICATIONS

Trojanised Zoom installer drops cross-platform spyware on Mac and Windows machines

Security researchers have uncovered a malware campaign distributing a fake Zoom installer named ZoomMeetings, which targets both macOS and Windows through an unusual cross-platform .NET-based downloader. Once executed, it detects the victim's operating system and architecture, then retrieves and runs platform-specific payloads from attacker-controlled infrastructure, while quietly installing the genuine Zoom application to preserve the deception.

The second-stage payload is a customised build of Overlord, an open-source WebSocket-based remote access trojan compiled with obfuscation to hinder analysis. It provides extensive surveillance, persistence, remote administration, and data theft, including keylogging, screen and webcam capture, and microphone access. Organisations are advised to block unsigned binaries executing from temporary directories and monitor for unauthorised persistence mechanisms.

ATTACK TYPE	Malware	**SECTOR**	Healthcare, Tourism, Manufacturing, IT, Government, Defence, Business, BFSI, Retail and Distribution, Telecommunications, Logistics
REGION	Global	**APPLICATION**	Apple macOS, Windows, Microsoft Teams, Zoom

Source - https://cyberpress.org/fake-zoom-installer-delivers-overlord-rat/

TATA COMMUNICATIONS

Severe Linux IPv6 Fraggap bug enables privilege escalation for unprivileged local users

CVE-2026-53362, dubbed the Fraggap vulnerability, is a high-severity flaw in the Linux kernel's IPv6 UDP networking stack. It stems from incorrect buffer size accounting in the __ip6_append_data function when handling paged allocations involving the MSG_MORE and MSG_SPLICE_PAGES flags. The miscalculation produces an out-of-bounds write that corrupts adjacent kernel memory structures, specifically the trailing region.

An unprivileged local user can trigger the flaw through UDPv6 sockets, potentially causing kernel crashes, denial-of-service conditions or privilege escalation. Red Hat has warned that an attacker inside a container could exploit it to escape to the host and gain root access. Administrators are strongly advised to apply the available kernel updates across all affected systems without delay.

ATTACK TYPE	Vulnerability	**SECTOR**	Healthcare, BFSI, Manufacturing, Government, IT Services and Consulting, Telecommunications
REGION	Global	**APPLICATION**	Linux

Source - https://securityonline.info/fraggap-linux-kernel-cve-2026-53362/

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