

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: October 27, 2026



THREAT INTELLIGENCE ADVISORY REPORT

As October 2026 draws to a close, the cyber threat landscape remains as relentless as ever, with threat actors engineering increasingly sophisticated and tightly coordinated campaigns across deeply interconnected digital environments. Traditional defence models are struggling to keep pace as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now depends on organisations reinforcing foundational security controls, adopting layered defence strategies, and embedding forward-looking intelligence throughout their operational frameworks.

In this fast-evolving environment, the Tata Communications Cyber Threat Intelligence report remains 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 turning intelligence into practical defence guidance, it equips security teams to anticipate, counter, and contain threats with confidence — preserving the continuity of critical operations at scale.

CERT-In warns attackers weaponise AI tools to compromise ICT systems at speed

Indian Computer Emergency Response Team (CERT-In) has issued a critical advisory, CIAD-2026-0049, formally classifying autonomous AI agents as an active attack surface. It details two incident categories: AI agents under research and evaluation that exceeded their authorised scope and reached the live systems of Indian organisations, and financially motivated actors abusing open-source agentic AI frameworks against Indian ICT assets.

The incidents stemmed from conventional lapses, including exposed credentials, insecure APIs, and excessive cloud permissions. Operating at machine speed, the agents exploited these gaps faster than human attackers, compressing the time from initial access to impact into hours, while incomplete remediation enabled repeat attacks. CERT-In urges organisations to secure credentials, enforce least privilege, restrict access, and strengthen real-time detection.

ATTACK TYPE	Cyber Crime, Breaches, Misconfiguration, Emerging Threats	SECTOR	BFSI, IT Services and Consulting
REGION	India	APPLICATION	Apple macOS, Windows, Linux

Source - CERT-In Advisory CIAD-2026-0049

Android banking GhostBat RAT evolves to steal PINs from 60 genuine financial apps

Researchers have detailed an evolved variant of GhostBat RAT, an Android banking trojan operating within the broader GhostX ecosystem and targeting users in India. Distributed through mParivahan and eChallan-themed smishing campaigns, the malware abuses Android Accessibility Services via a transparent Ghost Overlay technique to capture PINs entered in legitimate apps, including Google Pay and MobiKwik.

A separate keylogging feature monitors 60 banking, UPI, wallet, fintech, and payment applications for PIN-like input. Alongside this, evolving loaders, Firebase-based dynamic configuration, SMS collection, and call-forwarding manipulation strengthen its credential-theft and remote-control capabilities. Users should avoid installing applications from links in unsolicited messages, scrutinise accessibility permission requests, and rely only on official app stores for downloads.

ATTACK TYPE	Cyber Crime, Phishing, Malware, Mobile	SECTOR	Government, BFSI
REGION	India	APPLICATION	Android

Source - <https://cybersecuritynews.com/ghostbat-android-malware/>

Attackers chain Fortinet flaws to plant stealthy memory-resident implant on firewalls

Palo Alto Networks’ Unit 42 has detailed a multistage intrusion against a telecommunications managed service provider, tracked as CL-STA-0954. The attackers first exploited CVE-2024-47575, known as FortiJump, against a central FortiManager appliance, stealing configurations, credentials, and cryptographic trust material tied to more than 500 managed FortiGate firewalls. They then registered a rogue virtual appliance and exfiltrated a configuration archive.

Following an extended dwell period, the attackers exploited CVE-2025-61624, a FortiOS path-traversal flaw, to deploy PEERSTITCH, a memory-resident ARM64 implant. By patching the logging and VPN daemons in memory, it intercepts traffic data, suppresses security checks, and leaves no files on disk. Critically, patching alone cannot evict the intruders; organisations must rotate all stolen cryptographic material.

ATTACK TYPE	Vulnerability, Cyber Crime, Breaches, Malware	SECTOR	Telecommunications
REGION	Global	APPLICATION	Linux, FortiManager, Node.js, FortiOS, FortiGate

Source - <https://unit42.paloaltonetworks.com/fortimanager-cve-2024-47575-peerstitch-malware/>

Gentlemen RaaS affiliate Azazel harvests CI/CD secrets and weaponises AI tooling in attacks

The Gentlemen ransomware-as-a-service ecosystem relies on compromised credentials, exposed services, data exfiltration, security tool disruption, and ransomware deployment. Investigating exposed infrastructure, CloudSEK uncovered an affiliate known as Azazel who operated an independent leak site, LEAKNED, diverting extortion proceeds from the operators. Most victims were breached through extensive CI/CD secret harvesting, chiefly from GitLab variable stores and repository history.

In a previously unreported technique, Azazel registered a reverse shell as a callable tool within an AI assistant via the Model Context Protocol, turning the assistant into a command channel. Separately, CloudSEK's analysis of 15 ransomware incidents identified recurring techniques involving VPN access, RDP lateral movement, EDR impairment, backup disruption, and ransomware deployment. Organisations should urgently secure their pipeline secrets.

ATTACK TYPE	Information Gathering, Ransomware, Breaches, Malware	SECTOR	IT, Healthcare, BFSI, Pharmaceuticals, Manufacturing, Government, Logistics and Shipping
REGION	Global	APPLICATION	Microsoft Defender, Microsoft Active Directory Services, Microsoft SQL Server, PostgreSQL, Kubernetes, Windows, Redis, FileZilla, Fortinet FortiGate SSL VPN

Source - <https://www.cloudsek.com/blog/caught-in-4k-the-gentlemen-files>

Japan confronts breach surge as attackers exploit APIs and critical vulnerabilities

Japan has been contending with a sustained wave of cyber incidents since late September 2026, involving data exposure, API abuse, vulnerability exploitation, and ransomware. More than 20 organisations have disclosed breaches, including car-sharing service Times Car, restaurant operator Monogatari Corporation, JR East, Tokyo Metro, and government infrastructure. The Times Car breach alone exposed roughly 6.6 million customer accounts.

In an alert issued on 8 October, JPCERT/CC highlighted attackers reverse-engineering mobile apps to abuse hidden API endpoints and exploit the critical Metabase SQL injection vulnerability (CVE-2026-72898). These incidents underscore the need for stronger access controls, timely patching, and continuous monitoring. Investigations by authorities remain ongoing, with no link yet confirmed between the reported incidents.

ATTACK TYPE	Social Engineering, Vulnerability, Cyber Crime, Ransomware, Breaches	SECTOR	IT, Government, Transportation, Hospitality
REGION	Japan	APPLICATION	Apple macOS, Windows, Linux, Metabase

Source- <https://www.cybersecurityintelligence.com/blog/japan-declares-emergency-as-it-falls-under-sustained-cyber-attack-9821.html>

New macOS GhostProfile malware clones browser profiles to hijack victims' login sessions

Researchers have disclosed GhostProfile, a macOS malware implant that clones a victim's browser profile and remotely operates a concealed copy of Chrome or Firefox. By copying browser cookies into a separate, disposable environment, it lets an operator interact with online services using the victim's existing authenticated sessions, without a fresh login.

The implant controls the ghost browser through the Chrome DevTools Protocol and WebDriver BiDi, concealing the window by moving it far off-screen. Notably, researchers caution that success depends on each service's session handling, and device-bound protections may still apply. Organisations should monitor for browsers launched with remote-debugging flags or unusual profile paths, and prioritise phishing-resistant, session-aware authentication controls.

ATTACK TYPE	Malware, Emerging Threats	SECTOR	IT, Healthcare, Government, Transportation, Military, Energy, BFSI, Automobile, Retail and Distribution, Telecommunications, Logistics
REGION	Global	APPLICATION	Apple macOS, Mozilla Firefox, Google Chrome

Source - <https://cybersecuritynews.com/ghostprofile-macos-malware/>

ICMacOS upgrades into backdoor, offering attackers interactive remote command execution

ICMacOS, also known as Icarus macOS, is a macOS malware family that researchers at SOCRadar have observed evolving from an information stealer into a persistent remote access trojan. Sold under a subscription model by the Russian-speaking actor GlowComa, it spreads through ClickFix social-engineering pages that trick victims into pasting malicious commands into Terminal, before deploying a Go-based Mach-O payload.

Earlier versions displayed a fake system dialog to capture the login password and decrypt the Keychain. The newer build adds LaunchAgent persistence under an Apple-like name, a fallback restart mechanism, and an interactive WebSocket command channel enabling real-time remote shell execution. With browser, developer, and cloud credentials at risk, users should never paste untrusted commands into Terminal.

ATTACK TYPE	Information Gathering, Malware	SECTOR	IT, Healthcare, Government, Transportation, Military, Energy, BFSI, Automobile, Retail and Distribution, Telecommunications, Logistics
REGION	Global	APPLICATION	Apple macOS

Source - <https://cybersecuritynews.com/icmacos-malware-evolves/>

Critical FortiClient EMS zero-day flaw under active attack as public exploit emerges

Fortinet has released emergency hotfixes for CVE-2026-35616 (CVSS 9.1), a critical pre-authentication API access control flaw in FortiClient EMS that is being actively exploited in the wild. Classified as improper access control (CWE-284), it allows unauthenticated attackers to bypass API authentication using crafted requests, execute arbitrary commands, and escalate privileges. Affected versions include FortiClient EMS 7.4.5 and 7.4.6.

Attackers have exploited the flaw since 31 March 2026, and it now sits in CISA’s Known Exploited Vulnerabilities catalogue. A public proof-of-concept exploit has since been released, sharply increasing the risk of opportunistic attacks. Organisations running affected versions should deploy the hotfix immediately or upgrade to the fixed release, 7.4.7.

ATTACK TYPE	Vulnerability	SECTOR	IT, Healthcare, Government, Transportation, Military, Aviation, Energy, BFSI, Automobile, Retail and Distribution, Telecommunications, Logistics
REGION	Global	APPLICATION	FortiClient, FortiClient EMS, FortiClient

Source - <https://gbhackers.com/forticlient-ems-authentication-bypass/>

Cisco’s October update fixes 36 flaws including an actively exploited email gateway bug

Cisco’s October 2026 security updates address 36 vulnerabilities across products including Secure Email Gateway, License On-Prem, NX-OS, APIC, Meraki, Finesse, and Nexus 9000 Series Fabric Switches in ACI Mode. The flaws span remote code execution, authentication and authorisation weaknesses, memory-safety issues, injection, path traversal, denial-of-service, and server-side request forgery, with several rated critical, scoring between 9.8 and 10.0.

One of the greatest concerns is CVE-2026-76519 (CVSS 9.8), a critical arbitrary file write flaw in the Secure Email Gateway’s Advanced Malware Protection feature. By sending a crafted email attachment, an unauthenticated remote attacker can write files and execute commands as root. Cisco confirms active exploitation, and CISA has added it to its KEV catalogue. Administrators should patch without delay.

ATTACK TYPE	Vulnerability	SECTOR	IT, Healthcare, Government, Transportation, Military, Aviation, Energy, BFSI, Automobile, Retail and Distribution, Telecommunications
REGION	Global	APPLICATION	Cisco Application Policy Infrastructure Controller (APIC), Cisco NX-OS, Cisco switches, Cisco Meraki MT, Cisco Meraki MS

Source - <https://cybersecuritynews.com/cisco-secure-email-gateway-0-day-vulnerability/>

Qilin and Settra weaponise PAN-OS VPN flaw for stealthy corporate network access

The US Cybersecurity and Infrastructure Security Agency (CISA) has added CVE-2026-0257 to its Known Exploited Vulnerabilities catalogue, confirming active exploitation of an authentication bypass flaw in Palo Alto Networks PAN-OS GlobalProtect and Prisma Access. Now rated high severity (CVSS 7.8), the vulnerability lets attackers submit crafted cookies to bypass authentication, defeat multi-factor controls, and establish unauthorised VPN sessions.

Exploitation has been linked to the Qilin and Settra ransomware operations, with observed campaigns involving repeated probing and attempts to reach internal networks. Associated post-compromise activity has featured Cobalt Strike, BloodHound, and SharpHound, raising the prospect of credential theft, internal reconnaissance, lateral movement, data exfiltration, and ransomware deployment. Organisations should upgrade PAN-OS immediately and terminate all active GlobalProtect sessions.

ATTACK TYPE	Vulnerability	SECTOR	IT, Healthcare, Government, Transportation, Military, Aviation, Energy, BFSI, Automobile, Retail and Distribution, Telecommunications
REGION	Global	APPLICATION	Palo Alto Networks GlobalProtect, Palo Alto Networks PAN-OS, Palo Alto, Prisma Access

Source - <https://cybersecuritynews.com/palo-alto-globalprotect-flaw-vpn-access/>

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



All content is provided AS IS and for information purposes only. Tata Communications does not make any representations or warranties of any kind, including completeness, adequacy or accuracy of such information and disclaims all liability in connection with the use of this information. The information contained herein should not be construed as a substitute for professional advice.