

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: October 13, 2026



THREAT INTELLIGENCE ADVISORY REPORT

With October 2026 well underway, the cyber threat landscape shows no sign of relenting, as threat actors devise increasingly sophisticated and tightly coordinated campaigns across deeply interconnected digital environments. Conventional defence models are being outpaced as adversaries exploit systemic weaknesses with growing speed and precision. Sustaining resilience and competitive advantage now rests on organisations strengthening foundational security controls, adopting layered defence strategies, and weaving forward-looking intelligence throughout their operational frameworks.

In this fast-moving environment, the Tata Communications Cyber Threat Intelligence report remains an indispensable resource for security practitioners. Issued weekly, it offers sharp, timely analysis of emerging threat campaigns, evolving attacker methodologies, and sector-specific risk exposures. By translating intelligence into practical defence guidance, it helps security teams anticipate, counter, and contain threats with confidence, safeguarding critical operations at scale.

INTRODUCTION

OROVA RANSOMWARE
GROUP HITS LINUX AND
ESXI SERVERS WITH
DOUBLE EXTORTION

ATTACKERS EXPLOIT
CRITICAL FORTIMAIL
ZERO-DAY TO PLANT
FILES ON EMAIL
GATEWAYS

MIDNIGHT BLIZZARD'S
CAPTIVECRUNCH
CAMPAIGN STEALS
MICROSOFT 365
CREDENTIALS VIA HOTEL
WI-FI

STOLEN SERVICE
PRINCIPALS LET
JADEPUFFER DELETE
AZURE CLOUD
RESOURCES IN MINUTES

ATTACKERS EXPLOIT
CISCO SD-WAN FLAW TO
SEIZE ADMINISTRATIVE
API ACCESS REMOTELY

WINDOWS
CLOSEDQUORUM
MALWARE LETS AI
MODELS DECIDE ITS NEXT
ATTACK MOVE

DEVELOPERS TARGETED
AS NEW WEASELBISCUIT
INFESTEALERS LURKS
INSIDE NPM PACKAGES

NEW MALWARE WAVE
BUILDS AI DIRECTLY INTO
ITS CORE TO ADAPT
DYNAMICALLY

ANDROID BANKING
TROJAN RATHAT USES
GENAI TO HIJACK
PHONES AND DRAIN
ACCOUNTS

NIE OPERATOR WIRES
COMMERCIAL AI MODELS
INTO LIVE
CYBERESPIONAGE
OPERATIONS

New OROVA ransomware targets Linux and VMware ESXi with double-extortion tactics

OROVA is an emerging ransomware operation targeting Linux servers and VMware ESXi hypervisors through a double-extortion model that pairs file encryption with data theft and threatened public disclosure. SonicWall analysed its ELF encryptor, which enumerates running virtual machines via the ESXi command line and force-kills them before encrypting files with a modern Curve25519 and ChaCha20 cryptographic stack.

Since its leak site surfaced in August 2026, OROVA has claimed 45 victims in manufacturing, healthcare, technology, and financial services across six countries, including the United States, Hong Kong, and Taiwan. Its abuse of valid account credentials and destruction of recovery mechanisms deepen operational disruption and raise extortion risk. Organisations should enforce multi-factor authentication and maintain tested offline backups.

ATTACK TYPE	Ransomware, Emerging Threats	SECTOR	IT, Healthcare, BFSI, Manufacturing, Government, Energy, Defence Industry, Real Estate, FnB Service, Hospitality, Retail and Distribution
REGION	Japan, Brazil, Egypt, Taiwan, United States, Hong Kong	APPLICATION	VMware ESXi, Linux

Source - <https://cyberxtron.com/resources/blogs/orova-ransomware---a-rapidly-expanding-double-extortion-operation-with-growing-reach--8118>

CISA warns of FortiMail path traversal flaw enabling unauthenticated arbitrary file writes

A critical vulnerability in Fortinet FortiMail, the vendor's email security gateway, is being actively exploited in the wild. Tracked as CVE-2026-104286 (CVSS 9.8), the flaw combines path traversal with improper NULL-byte neutralisation within the Identity-Based Encryption feature of the web interface. It allows an unauthenticated remote attacker to write arbitrary files via specially crafted HTTP or HTTPS requests.

Attackers have been observed dropping webshells and malicious binaries, modifying system files, and establishing persistence on exposed appliances. CISA added the flaw to its Known Exploited Vulnerabilities catalogue on 1 October 2026, setting a tight remediation deadline for federal agencies. Organisations should upgrade to fixed FortiMail builds immediately or apply Fortinet's workaround and hunt for indicators of prior compromise.

ATTACK TYPE	Vulnerability	SECTOR	IT, Healthcare, Construction, Government, Transportation, ONGC, BFSI, Aviation, Automobile, Retail and Distribution, Telecommunications
REGION	Global	APPLICATION	Fortinet

Source - <https://socradar.io/blog/fortimail-zero-day-under-active-exploitation/>

Midnight Blizzard hackers hijack hotel Wi-Fi portals to steal Microsoft 365 credentials

Microsoft Threat Intelligence has detailed CaptiveCrunch, a credential-theft campaign run by Storm-2945, a sub-cluster of the state-linked actor Midnight Blizzard. The operators compromise shared captive-portal infrastructure used by hotels and conference centres, then manipulate DNS and HTTP traffic to redirect connecting travellers towards attacker-controlled Microsoft 365 phishing pages and Entra ID device-code authentication prompts.

A separate route uses ClickFix lures disguised as software updates to deliver two custom strains: CornFlake, a Go-based Windows RAT providing persistent access, and ChocoShell, a PowerShell infostealer. Together they harvest credentials, session tokens, browser data, and host information. Because stolen Microsoft 365 tokens can outlive password resets, organisations should rotate credentials, revoke sessions, and treat untrusted Wi-Fi cautiously.

ATTACK TYPE	Social Engineering, Phishing	SECTOR	Hospitality
REGION	India, Saudi Arabia, United States	APPLICATION	Microsoft Windows Defender, Android, Microsoft Outlook, Mozilla Firefox, Windows, Microsoft Office 365, Google Chrome, Microsoft Entra

Source - <https://www.zscaler.com/blogs/security-research/captivecrunch-midnight-blizzard-weaponizes-hotel-wi-fi-captive-portals>

JADEPUFFER (Storm-3168) expands agentic ransomware activity to Azure cloud resources

Microsoft has detailed a destructive Azure campaign by JADEPUFFER, which it tracks as Storm-3168. Using two compromised service principals within a single tenant, the actor performed extensive cloud reconnaissance before rapidly deleting Azure Storage Accounts, Key Vaults, Function Apps, and App Service resources. It also targeted recovery controls, harvested storage access keys, and attempted to destroy SQL databases.

Sysdig first documented JADEPUFFER's agentic ransomware operations in Langflow and database environments; this move into cloud infrastructure marks a significant expansion. The automated sequence unfolded in minutes, far outpacing typical human response times, and only pre-configured resource locks withstood deletion. Organisations are urged to secure service principal credentials, enforce least privilege, and apply protective resource locks.

ATTACK TYPE	Ransomware, Emerging Threats	SECTOR	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	APPLICATION	Docker, WordPress, Linux, Microsoft Azure, Langflow

Source - <https://securityonline.info/jadepuffer-azure-attack/>

CISA adds actively exploited Cisco SD-WAN authentication bypass flaw (CVSS 9.8) to its KEV catalogue

CISA has added CVE-2026-76504 (CVSS 9.8), a critical authentication bypass vulnerability in Cisco Catalyst SD-WAN Manager, to its Known Exploited Vulnerabilities catalogue. The flaw stems from improper handling of URI encoding in an HTTP request, allowing an unauthenticated remote attacker to bypass authentication rules and reach a restricted API endpoint with the privileges of the administrator user.

Cisco confirmed it had become aware of active exploitation in September 2026. The flaw affects all Catalyst SD-WAN Manager deployments regardless of configuration, and no workarounds are available. Federal agencies were ordered to remediate by 3 October 2026. Administrative access to the central manager risks unauthorised configuration changes across every connected branch, so organisations should upgrade and check for signs of compromise immediately.

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

Source - <https://www.cisa.gov/news-events/alerts/2026/09/30/cisa-adds-one-known-exploited-vulnerability-catalog>

New AI-driven CLOSEDQUORUM malware lets LLMs choose its next attack step and reports back via Discord

Cisco Talos has documented CLOSEDQUORUM, the first publicly reported Windows implant to delegate tactical command-and-control decisions to commercial large language models rather than a human operator. After infecting a host, the Go-based malware queries up to four AI providers (DeepSeek, Qwen, Mistral, and Gemini), sending basic system details and letting the models select its next action.

When the models choose theft, the implant simultaneously dumps LSASS memory, harvests browser credentials, and extracts cryptocurrency wallet data, before establishing persistence through Registry Run keys, scheduled tasks, and WMI. Stolen material is encrypted and exfiltrated via a Discord webhook. Talos has not confirmed any in-the-wild deployment, and the publicly distributed build is non-functional, containing placeholder credentials.

ATTACK TYPE	Malware	SECTOR	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	APPLICATION	Microsoft Edge, Mozilla Firefox, Windows, Google Chrome

Source - <https://blog.talosintelligence.com/the-closed-quorum-inside-the-first-reported-autonomous-ai-c2-implant/>

New WeaselBiscuit JavaScript infostealer spreads through malicious npm packages, with potential DPRK links

Researchers have identified WeaselBiscuit, a previously undocumented JavaScript infostealer distributed through a cluster of malicious npm packages. Once a package is imported, a loader retrieves the main payload from an Npoint.io dead drop and executes it directly in memory. The malware harvests Chrome extension storage across Windows, macOS, and Linux. On Windows, it can capture clipboard contents and keystrokes when instructed.

By targeting extension storage, WeaselBiscuit can expose sensitive cryptocurrency wallet and other extension-related data. Its Npoint dead-drop pattern, nested geolocation lookups, and control-plane design closely mirror the DPRK-associated BeaverTail and OtterCookie families, though researchers stress this attribution remains a working hypothesis. Organisations should vet third-party npm dependencies carefully, monitor for suspicious Node.js activity, and block the identified indicators.

ATTACK TYPE	Malware, Supply Chain, Emerging Threats	SECTOR	Business, IT, Cryptocurrency
REGION	Global	APPLICATION	Apple macOS, Windows, Linux, Google Chrome, Node Package Manager (npm)

Source - <https://opensourcemalware.com/blog/introducing-weaselbiscuit>

Attackers embed AI models inside malware, creating adaptive threats that evade detection

Researchers have outlined the emerging AI-Killchain, a shift in which threat actors embed AI models directly into malware rather than merely using them for support. This integration enables dynamic command generation, adaptive execution, automated data collection, and AI-assisted attack development, allowing malicious code to alter its behaviour at runtime instead of relying on fixed, pre-written logic.

Emerging families illustrate the breadth of this trend across Windows, Android, and cloud environments. XillenStealer harvests data, PromptSpy hijacks Android devices, PromptLock demonstrates AI-generated ransomware, SesameOp abuses the OpenAI API as a covert command channel, and LAMEHUG generates Windows commands on the fly. This move towards adaptive threats complicates traditional detection, analysis, and incident-response processes, demanding behaviour-based defensive strategies.

ATTACK TYPE	Information Gathering, Cyber Crime, Malware, Mobile, Cyberespionage, APT, Emerging Threats	SECTOR	IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications
REGION	Global	APPLICATION	Android, Windows, GitHub, Anthropic Claude Code, Hugging Face Transformers, Google Gemini

Source - <https://rt-solar.ru/solar-4rays/blog/6886/>

Suspected China-linked actors deploy RatHat Android trojan that uses AI navigation and ADB persistence

Researchers have uncovered RatHat, an Android banking trojan distributed through smishing, malvertising, and deceptive download pages. After tricking victims into granting Accessibility access, it uses synthetic taps to enable Developer Options and Wireless Debugging and then pairs with the device's own ADB daemon to break out of the app sandbox and gain shell-level privileges without an external computer.

Unusually, RatHat serialises the live Accessibility tree into XML and queries a generative AI assistant to navigate unfamiliar interfaces in real time, making automation harder to detect. It steals banking credentials, OTPs, PINs, and personal data via fake overlays, and can reinstall itself after removal. Tentatively linked to China-based operators, it has been observed across multiple regions worldwide.

ATTACK TYPE	Malware, Mobile, Emerging Threats	SECTOR	BFSI, Cryptocurrency
REGION	Europe, South Asia, Latin America	APPLICATION	Android, Microsoft Edge, Opera Browser, Google Chrome

Source - <https://zimperium.com/blog/rathat-ai-powered-mobile-threat-is-here-for-your-credentials-bank-accounts>

Nie AI framework turns commercial chatbots into automated agents for cyber intrusions

Researchers have uncovered a campaign in which a Chinese-speaking operator, with the recurring handle Nie, used an AI orchestration framework named SecFlow to automate intrusions against systems belonging to government, political, education, healthcare, and industrial organisations in Asia. SecFlow converted high-level objectives into discrete tasks, assigning them to interchangeable AI workers based on Claude, Qwen, and DeepSeek models.

Alongside the AI workers, the operator deployed custom webshells, conventional exploitation tools, and a Go-based implant named SecBox. Confirmed activity included command execution, credential theft, database access, and the collection of government, health-related, and student information. Model requests were routed through private proxy relays, and the AI agents ran with their approval checks disabled. Organisations should monitor for the published indicators and harden exposed applications promptly.

ATTACK TYPE	Vulnerability, Breaches, Malware, Cyberespionage	SECTOR	Healthcare, Government, Education
REGION	Global, China, Indonesia, Taiwan, Vietnam	APPLICATION	Microsoft SQL Server, Oracle Database, Windows, Linux, Apache Tomcat, Nexus Repository

Source - <https://hunt.io/blog/chinese-operator-secflow-claude-qwen-deepseek-asia>

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.