

# YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: October 6, 2026



# THREAT INTELLIGENCE ADVISORY REPORT

As October 2026 begins, the cyber threat landscape remains as unrelenting 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 every layer of 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 — protecting the continuity of critical operations at scale.

[INTRODUCTION](#)[SHINYHUNTERS RENEWS  
PEOPLESOFT ATTACKS  
AND BREACHES A RIVAL  
RANSOMWARE GANG](#)[WEAPONISED FAKE JOB  
TERRAFORM FILES  
DELIVER STEALTHY  
MACOS ARM BACKDOORS](#)[CYBERCRIMINAL TAJIN  
GROUP USES NFC RELAY  
AND STOLEN CARDS TO  
LAUNDER ILLICIT FUNDS](#)[ACTIVELY EXPLOITED F5  
FLAW LETS ATTACKERS  
SEIZE BIG-IP ACCESS  
MANAGEMENT SYSTEMS](#)[CHECK POINT URGES  
URGENT PATCHING AS  
CRITICAL CVSS 9.8  
FLAWS COME UNDER  
ATTACK](#)[WATERPLUM GROUP  
WEAPONISES FAKE  
CODING TESTS TO  
HIJACK DEVICES AND  
STEAL CRYPTO](#)[FERAL WOLF EXPLOITS  
CONFLUENCE AND 1C  
FLAWS TO DELIVER  
GENIELOCKER  
RANSOMWARE](#)[KONNI HACKERS TARGET  
DIPLOMATS WITH  
VELVETCAKE VIA FAKE  
PDF SHORTCUT LURES](#)[SECTOPRAT HIDES INSIDE  
TAMPERED AUDIO  
SOFTWARE TO STEAL  
CREDENTIALS AND  
CRYPTO DATA](#)[CARBONATO BOTNET  
IMPLANTS AI AGENTS ON  
EXPOSED DOCKER  
HOSTS TO STEAL API  
KEYS](#)

# ShinyHunters (UNC6240) renews PeopleSoft exploitation following Clop leak site breach

Google Threat Intelligence Group have observed the ShinyHunters cluster, tracked as UNC6240, renewing mass exploitation of CVE-2026-35273, a critical unauthenticated remote code execution flaw in Oracle PeopleSoft. The group defeats web application firewall rules by URL-encoding the blocked PSEMHUB endpoint path, then deploys JSP web shells, the SIDEYE backdoor, Neo-reGeorg tunnelling and MeshAgent for persistent access.

Notably, the campaign targets organisations that deployed firewall rules but never applied Oracle's patch, underscoring that WAF mitigation alone is inadequate. The group also breached rival ransomware gang Clop's leak site via a Grav CMS path traversal flaw, and claimed unauthorised activity against a US government jobs portal. Organisations must apply the update immediately and rotate exposed credentials.

|             |                                     |             |                                                           |
|-------------|-------------------------------------|-------------|-----------------------------------------------------------|
| ATTACK TYPE | Vulnerability, Cybercrime, Breaches | SECTOR      | Healthcare, Government, Transportation, Education, IT     |
| REGION      | Global                              | APPLICATION | Oracle WebLogic Server, Windows, Linux, Oracle PeopleSoft |

Source - <https://cloud.google.com/blog/topics/threat-intelligence/shinyhunters-renewed-mass-exploitation-campaign-targeting-oracle-peoplesoft/>

# TraderTraitor threat actor uses Terraform repositories to plant macOS ARM64 backdoors

The North Korea-linked threat actor Jade Sleet, also tracked as TraderTraitor and UNC4899, has expanded its targeting through fake job-interview repositories containing weaponised Terraform projects. A malicious dependency lock file points to a typosquatted provider registry, so that when a developer runs terraform init, the system downloads and executes attacker-controlled modules delivering the FLATROOF and ROOFDECK macOS ARM64 backdoors.

Researchers identified an Indian IT services provider whose DevOps engineer's Apple Silicon MacBook held both implants by 18 March 2026. Written in Rust for ARM64, the pair bypass Gatekeeper and enable persistent access, reconnaissance, browser-data and Keychain theft, command execution and exfiltration. Organisations should audit Terraform lockfiles for untrusted registries and restrict developer cloud credentials accordingly.

|             |                                           |             |                                                                                                  |
|-------------|-------------------------------------------|-------------|--------------------------------------------------------------------------------------------------|
| ATTACK TYPE | Social Engineering, Malware, Supply Chain | SECTOR      | IT Services and Consulting                                                                       |
| REGION      | India                                     | APPLICATION | Apple macOS, Apple Safari, Mozilla Firefox, Google Chrome, Amazon Web Services, Telegram, GitHub |

Source - <https://thehackernews.com/2026/09/jade-sleet-linked-to-indian-it-provider.html>

# Financial fraud vendor Tajin exploits Telegram escrow markets for card theft and laundering

A group of researchers has profiled Tajin Group, a third-party vendor operating on Telegram-based Chinese-language guarantee marketplaces. The group has pivoted from Dabai Guarantee to Xinbi Guarantee, demonstrating that such vendors show little loyalty to any single platform. Its activities span financial fraud, money laundering, and the buying and selling of compromised payment-card information, including CVVs.

Observed techniques include ghost-tapping and contactless ATM withdrawals using NFC-relay methods, AI-assisted card-transfer operations, and cash-out schemes routed through UAE payment gateways and UK-based eGift cards. These operations primarily target mainland Chinese citizens and banking infrastructure, exposing financial institutions to fraud and related risks. Institutions are urged to monitor for such activity and strengthen transaction-fraud controls accordingly.

|             |                                                                                                                      |             |                                       |
|-------------|----------------------------------------------------------------------------------------------------------------------|-------------|---------------------------------------|
| ATTACK TYPE | Cybercrime, Phishing                                                                                                 | SECTOR      | BFSI                                  |
| REGION      | UK, Global, China, Malaysia, Philippines, Romania, South Africa, Sri Lanka, United Arab Emirates, Vietnam, Hong Kong | APPLICATION | Apple macOS, Windows, Linux, Telegram |

Source - <https://www.recordedfuture.com/research/tajin-group-gurantee-marketplace>

# F5 BIG-IP APM and DNS flaw under attack enables unauthenticated remote code execution

F5 has disclosed two vulnerabilities affecting BIG-IP APM and BIG-IP DNS, one of which is already under active attack. CVE-2026-94127 (CVSS 9.3) is a critical heap-based buffer overflow that allows unauthenticated remote code execution. It affects only systems where APM is configured as an OAuth authorisation server, with both an access policy and OAuth profile on the same virtual server.

The second flaw, CVE-2026-11622 (CVSS 7.5), can cause excessive memory consumption in DNSSEC-validating resolvers, potentially triggering denial-of-service conditions. Following confirmation of active exploitation, CISA added CVE-2026-94127 to its Known Exploited Vulnerabilities catalogue with a rapid remediation deadline. Organisations are urged to apply the available engineering hotfixes immediately or deploy F5's iRule mitigation until patching is complete.

|             |               |             |                                                                                                                                 |
|-------------|---------------|-------------|---------------------------------------------------------------------------------------------------------------------------------|
| ATTACK TYPE | Vulnerability | SECTOR      | IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications |
| REGION      | Global        | APPLICATION | F5 BIG-IP                                                                                                                       |

Source - <https://cybersecuritynews.com/f5-big-ip-oauth-server-0-day-flaw/>

# Actively exploited Check Point flaws enable pre-authentication CVSS 9.8 code execution

Check Point has released security updates addressing two critical vulnerabilities affecting its Security Gateway, Spark Firewall and Security Management products, both now under active exploitation. CVE-2026-85102 (CVSS 9.8) stems from improper certificate validation during VPN negotiation, allowing an unauthenticated remote attacker to send a malicious certificate and execute arbitrary code on the gateway. Fixes were released on 9 September 2026.

The second flaw, CVE-2026-93616 (CVSS 9.8), is a pre-authentication path-traversal and file-upload vulnerability in the Management web service, letting attackers execute scripts from arbitrary paths and load malicious Java classes. Check Point observed it being exploited as a zero-day since 23 July. CISA has added both flaws to its Known Exploited Vulnerabilities catalogue, urging organisations to patch without delay.

|             |               |             |                                                                                                                                 |
|-------------|---------------|-------------|---------------------------------------------------------------------------------------------------------------------------------|
| ATTACK TYPE | Vulnerability | SECTOR      | IT, Healthcare, BFSI, Manufacturing, Government, Transportation, Education, Energy, Retail and Distribution, Telecommunications |
| REGION      | Global        | APPLICATION | Check Point Firewall, Check Point Management Server, Check Point VPN                                                            |

Source - <https://securityonline.info/checkpoint-vpn-vulnerability-cve-2026-85102/>

# WaterPlum hacker group poses as fake recruiters to infect developer devices worldwide

A joint advisory from authorities in Japan, the United States, Australia and Germany has detailed WaterPlum, a state-sponsored threat group also tracked as Contagious Interview. Posing as recruiters for legitimate AI, cryptocurrency and NFT firms, its operators lure software developers and IT professionals into fake technical interviews, instructing them to download malicious coding assignments that quietly backdoor their devices.

Once installed, remote-access trojans and information stealers grant persistent access, harvesting browser passwords, keystrokes, screenshots, identity documents and cryptocurrency wallet data. Between December 2025 and July 2026, WaterPlum compromised at least 30,000 devices across more than 100 countries, draining over 7,000 wallets of roughly US\$10.71 million. Professionals should treat unsolicited recruiter code with extreme caution and verify approaches independently.

|             |                             |             |                                                                                                                    |
|-------------|-----------------------------|-------------|--------------------------------------------------------------------------------------------------------------------|
| ATTACK TYPE | Social Engineering, Malware | SECTOR      | BFSI, Business, IT Services and Consulting, Staffing and Recruiting, Software Development, Trading, Cryptocurrency |
| REGION      | Global                      | APPLICATION | Apple macOS, Windows, Linux, VS Code, Node Packag Manager (npm)                                                    |

Source - <https://securityonline.info/waterplum-cyber-actor-group/>

# Feral Wolf deploys GenieLocker ransomware and backdoors against Russian organisations

Researchers have detailed Feral Wolf, a financially motivated group that targeted Russian organisations across retail, construction, manufacturing and IT between May and August 2026. The attackers gained initial access through vulnerable Atlassian Confluence installations; insecure, internet-exposed 1C:Enterprise clusters; and compromised contractor infrastructure before deploying three newly documented tools: the Rust-based MQTTDoor, MatrixDoor backdoors, and RDPsSocksProxy.

Following the intrusion, Feral Wolf performed container-to-host escape, privilege escalation, credential harvesting and lateral movement, routing command-and-control traffic covertly through MQTT and Matrix channels to blend with legitimate activity. The operators tunnelled traffic over existing RDP sessions and removed forensic artefacts before deploying GenieLocker ransomware. Organisations should restrict external access to Confluence and 1C services and enforce strong administrative authentication.

|             |                                             |             |                                                          |
|-------------|---------------------------------------------|-------------|----------------------------------------------------------|
| ATTACK TYPE | Vulnerability, Ransomware, Misconfiguration | SECTOR      | IT, Manufacturing, Construction, Retail and Distribution |
| REGION      | Russia                                      | APPLICATION | Atlassian Confluence, Docker, PostgreSQL, Windows, Linux |

Source - <https://bi.zone/eng/expertise/blog/idem-po-sledam-feral-wolf-novye-instrumenty-i-tekhniki-atak/>

# Konni deploys stealthy VelvetCake downloader against diplomats via malicious LNK files

Threat research unit has uncovered Operation Conflict Compass, a cyber-espionage campaign attributed with moderate confidence to the North Korea-linked group Konni. Active since early August 2026, it targets individuals and organisations engaged in Ukraine-related diplomatic, foreign-policy and defence research. The attackers deliver malicious LNK shortcut files, disguised as PDF documents inside ZIP archives, through carefully themed spear-phishing emails.

Once opened, the shortcut establishes scheduled-task persistence that executes VelvetCake, a lightweight PowerShell downloader, every minute. Rather than carrying every function itself, VelvetCake retrieves server-side scripts that perform host reconnaissance and screen capture before exfiltrating collected data over attacker-controlled TCP and HTTP channels. Organisations handling sensitive Ukraine-related work should treat unexpected document archives and meeting installers with heightened caution.

|             |                          |             |                                            |
|-------------|--------------------------|-------------|--------------------------------------------|
| ATTACK TYPE | Malware, Cyber-espionage | SECTOR      | Government, Defence                        |
| REGION      | Ukraine                  | APPLICATION | Windows, Zoom Meetings, PowerShell, GitHub |

Source - <https://gbhackers.com/velvetcake-powershell-malware/>

# Attackers hide credential-stealing SectopRAT inside tampered audio production software

FortiGuard's Incident Response team has uncovered a variant of SectopRAT, a .NET-based remote access trojan also known as ArechClient2, concealed within tampered components of legitimate digital audio workstation software from an Italian vendor. Notably, this was not a supply-chain compromise: attackers modified a locally installed copy rather than the vendor's distribution, using a multi-stage loader to evade detection.

Once executed in memory, the heavily obfuscated payload supports 29 commands spanning remote administration, screen capture, process and file management, shell execution and self-removal. It harvests browser credentials, cookies and cryptocurrency-wallet data, communicating over AES-encrypted channels while using API hashing to frustrate analysis. Organisations are urged to monitor application behaviour rather than trusting software implicitly, and provide security-awareness training.

|             |         |             |                                                                                                              |
|-------------|---------|-------------|--------------------------------------------------------------------------------------------------------------|
| ATTACK TYPE | Malware | SECTOR      | IT                                                                                                           |
| REGION      | Global  | APPLICATION | Microsoft Windows 10, Microsoft Edge, Chromium, Mozilla Firefox, Mozilla Thunderbird, Windows, Google Chrome |

Source - <https://feeds.fortinet.com/-/969841961/0/fortinet/blog/threat-research-Uncovering-a-SectopRAT-Variant-Embedded-in-Legitimate-Software>

# New CARBONATO botnet hunts exposed Docker daemons to harvest AI service credentials

Researchers have uncovered CARBONATO, a Docker-focused botnet that scans reachable networks for unauthenticated Docker daemons exposed on port 2375. Once connected, it launches a privileged container to seize host-level access, then installs the open-source Hermes Agent AI framework. Directed through Telegram, the agent prioritises the theft of AI API keys above SSH credentials, access tokens and other secrets.

Believed to have been active since October 2024, CARBONATO exhibits worm-like behaviour, scanning neighbouring networks every five minutes to compromise further hosts autonomously. It establishes multiple persistence mechanisms and reverse SSH access, and bundles cryptocurrency mining components. Researchers noted infrastructure indicators pointing towards Costa Rica but stopped short of definitive attribution. Organisations must never expose the Docker daemon unauthenticated.

|             |         |             |                         |
|-------------|---------|-------------|-------------------------|
| ATTACK TYPE | Malware | SECTOR      | IT, Cryptocurrency      |
| REGION      | Global  | APPLICATION | Docker, Linux, Telegram |

Source - <https://cyberveille.ch/posts/2026-09-25-carbonato-un-botnet-docker-pilote-par-un-agent-ia-via-telegram-ciblant-les-cles-api/>

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.