CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Iranian state-affiliated threat group Handala Hack has breached FBI director's Patel's personal Gmail account and leaked many personal photos and documents. This follows the FBI's seizure of domains related to Handala Hack's activity last week, due to the group's sustained targeting of Israeli and American entities, which increased during the ongoing Iran conflict.
- Spain's Port of Vigo in Galicia has suffered a ransomware attack that forced officials to disconnect parts of its network and switch cargo handling to manual processes. The incident locked equipment and disrupted digital logistics, while physical ship movement could continue without digital communication.
- The Netherlands' Ministry of Finance has confirmed a March 19 cyberattack that breached internal systems in its policy department and disrupted work for some employees. Authorities blocked access to affected environments, while tax, customs, and benefits services remained unaffected and no threat actor publicly claimed responsibility for the attack.
- Decentralized finance platform Resolv has suffered a cyberattack after a compromised private key let an attacker mint about $80 million in uncollateralized USR tokens and swap them for 11,408 ETH worth $24.5 million. Resolv confirmed the incident, paused the app, and offered a 10% bounty for returned funds.

AI THREATS

- Researchers demonstrated a supply chain compromise of LiteLLM, a Python library linking apps to major AI services, after attackers hijacked a security tool and pushed malicious releases on March 24. The tainted packages harvested API keys and cloud credentials, creating downstream exposure for widely used AI projects.
- Researchers outlined three high-severity vulnerabilities in LangChain and LangGraph, open-source frameworks for building AI assistants, that could expose files, environment secrets, and prior conversations. The flaws enabled arbitrary file access, secret leakage, and SQL injection in checkpointing, and patches were issued in updated components.
- Researchers identified a zero-click flaw in Anthropic's Claude Chrome extension that let any website silently inject prompts and control the assistant. The attack combined an overly permissive trusted domain list with a scripting bug in Arkose Labs CAPTCHA handling, enabling token theft, chat access, and email actions.

VULNERABILITIES AND PATCHES

- Cisco has addressed CVE-2026-20131, a CVSS 10 vulnerability in Secure Firewall Management Center that lets unauthenticated attackers execute code as root through the web interface. Cisco confirmed attempted exploitation in March 2026 and released fixes, while on-premises customers have no workaround beyond applying the updates.

  Check Point IPS provides protection against this threat *(Cisco Secure Firewall Management Center Insecure Deserialization (CVE-2026-20131))*

- TP-Link has issued firmware updates addressing CVE-2025-15517 and related critical flaws in Archer NX200, NX210, NX500, and NX600 5G Wi-Fi routers. Attackers could access administrative functions without logging in, upload rogue firmware, execute system commands, and more.

- Citrix has released patches for CVE-2026-3055 and CVE-2026-4368 affecting NetScaler ADC and Gateway. The critical memory flaw can expose sensitive data in SAML Identity Provider deployments, while the second bug can mix up user sessions on gateways, creating confidentiality and access risks.

  Check Point IPS provides protection against this threat *(Citrix NetScaler Out Of Bounds Read (CVE-2026-3055))*

- Researchers warn that a leaked 'DarkSword' iOS exploit chain enables no-click attacks via Safari, threatening up to 270 million unpatched iPhones and iPads. The code eases copycat attacks and has seen use, while Apple issued fixes, including March 11 emergency updates for iOS 15 and 16.

THREAT INTELLIGENCE REPORTS

- Researchers revealed that cybercriminals are abusing Keitaro, a commercial adtech tracker, to distribute phishing, scams, and malware at scale. Infoblox linked the platform to major malvertising and spam operations, including campaigns impersonating Canadian banks, logistics brands, government services, and high-trust retail providers.

- Researchers analyzed three China-aligned activity clusters targeting a Southeast Asian government in a coordinated espionage operation. The campaign combined USB propagation, the Hypnosis loader, and the FluffyGh0st RAT, showing how distinct threat clusters can converge on one high-value government target with complementary tooling.

- Researchers have analyzed the activity of Russian threat group APT28 (aka Fancy Bear). The group has recently targeted Ukraine as well as its European defense supply chain partners with a toolset dubbed PRIXMES, which holds both espionage and sabotage capabilities. APT28 exploited multiple vulnerabilities, including zero-days, in its attacks.

- Researchers identified a coordinated adversary-in-the-middle phishing campaign targeting TikTok for Business users who sign in with Google. Attackers deployed proxy login pages that captured passwords and session cookies to bypass multi-factor authentication, with newly registered domains and Cloudflare-hosted infrastructure used to scale impersonation.