

# WEEKLY INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- The Los Angeles Police Department has [reported](#) a data breach involving a digital storage system used by the L.A. City Attorney’s Office. The exposure included 7.7 terabytes and more than 337,000 files, including personnel records, internal affairs material, and unredacted personal information.
- ChipSoft, a Dutch healthcare software vendor whose HiX platform is used by hospitals across the Netherlands, has [suffered](#) a ransomware attack that forced it to disable patient and provider services. Multiple hospitals disconnected from its systems, disrupting operations, and the company warned that the threat actor may have gained unauthorized access to patient data.
- Ransomware group Qilin has [taken](#) responsibility for a cyber-attack targeting German political party Die Linke, which forced the party to shut down its IT infrastructure in late March. The party said membership databases were unaffected, while Qilin threatens to leak stolen sensitive employee and party information.

*Check Point Endpoint and Threat Emulation provide protection against these threats ( Ransomware.Wins.Qilin\*)*

- Bitcoin Depot, a US cryptocurrency ATM operator with more than 25,000 kiosks and checkout locations, has [disclosed](#) a cyberattack that allowed attackers to steal credentials tied to digital asset settlement accounts. The attackers transferred more than 50 BTC worth more than \$3.6M from company-controlled wallets before access was blocked.

## AI THREATS

- Researchers [identified](#) GrafanaGhost, an attack against Grafana’s AI components that can silently exfiltrate enterprise data by chaining indirect prompt injection with image URL validation bypass. The technique can expose financial, infrastructure, and customer information in the background, and Grafana has already addressed the weakness.
- Researchers [outlined](#) AI Agent Traps, a framework describing six web-based attack classes that can manipulate autonomous AI agents through malicious content. The methods can inject hidden instructions, poison reasoning, corrupt memory, and steer tool use, showing how web pages can turn agent workflows into attack surfaces.
- Researchers [measured](#) a growing AI supply chain risk, finding that third-party API routers for AI models can hijack agent tool calls to alter commands and steal credentials. In testing, several routers injected malicious code, abused intercepted cloud keys, and even triggered wallet theft from a researcher environment.

## VULNERABILITIES AND PATCHES

- CISA [warns](#) of active exploitation of Ivanti CVE-2026-1340, a critical code injection flaw in Endpoint Manager Mobile that allows unauthenticated remote code execution and full compromise of affected servers. The vulnerability carries a CVSS score of 9.8, affects multiple 12.5 through 12.7 releases, and has been exploited in the wild.

*Check Point IPS provides protection against this threat (Ivanti Endpoint Manager Mobile Code Injection (CVE-2026-1340))*

- Adobe Reader is [affected](#) by an actively exploited zero-day that uses malicious PDF files to invoke privileged features on fully updated systems, enabling local data theft. Researchers said the activity has run since at least December 2025, uses Russian-language oil and gas lures, and may also enable further compromise.
- Marimo maintainers [released](#) a fix for CVE-2026-39987, a critical remote code execution flaw in the Marimo Python notebook that allowed attackers to open a terminal without authentication and run commands. Exploitation was observed within hours of disclosure against internet-exposed instances, and fixes are available in version 0.23.0.
- Fortinet has [fixed](#) CVE-2026-35616, a critical improper access control flaw in FortiClient EMS that enables unauthenticated code or command execution through crafted requests. The issue been actively exploited in the wild, prompting Fortinet to release an emergency hotfix.

## THREAT INTELLIGENCE REPORTS

- Check Point Research have [analyzed](#) March 2026's threat landscape, with organizations averaging 1,995 weekly attacks. Education remained the most targeted sector, ransomware rose to 672 incidents led by Qilin, Akira, and DragonForce, and GenAI exposure remained high across enterprise environments.
- Researchers [discovered](#) a coordinated software supply chain campaign that planted 36 malicious npm packages impersonating Strapi plugins. The packages executed on installation to search for secrets, maintain command and control, and in some cases enable Redis remote code execution, credential harvesting, and direct PostgreSQL exploitation.
- Researchers [linked](#) Storm-1175, a financially motivated group associated with Medusa ransomware, to high-velocity exploitation of n-day and zero-day flaws. Microsoft said the actor moves quickly from initial access to data theft and ransomware deployment, sometimes weaponizing vulnerabilities within a day and heavily impacting healthcare, education, finance, and services.
- Researchers [identified](#) a hack-for-hire campaign linked to BITTER APT that targeted journalists, activists, and government figures across the Middle East and North Africa. The operators used phishing to access iCloud backups and Signal accounts, and deployed Android spyware disguised as messaging applications to take over victim devices.