CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- 7-Eleven, the global convenience store chain, confirmed a breach after an unauthorized access to systems used for franchisee documents. ShinyHunters claimed responsibility and said it stole more than 600,000 Salesforce records containing personal and corporate information, with affected individuals offered identity protection services.
- Code hosting platform GitHub has suffered a breach after attackers weaponized a Visual Studio Code extension to compromise an employee device and steal internal source code. The company estimated about 3,800 internal repositories were exfiltrated, with no evidence of impact on customer-facing systems.
- Grafana Labs, an open-source observability software company, disclosed a breach after a compromised GitHub token allowed intruders to access parts of its source code. The company reports that it has refused to pay ransom to the attackers and claims no customer data exposure or service disruption.
- The FBI warns about Kali365, a phishing-as-a-service kit that is actively being used to target Americans and is distributed mainly through Telegram. The platform targets Microsoft 365 users with device-code phishing, captures OAuth access and refresh tokens, and enables persistent access to Outlook, Teams, and OneDrive while bypassing MFA.

AI THREATS

- Check Point Research released the March-April 2026 AI Threat Landscape digest and demonstrated that AI-driven attacks have entered routine criminal use, citing a campaign where a single operator used commercial AI to compromise nine Mexican government agencies and execute over 5,000 automated commands. It also notes malicious configuration files that override safety controls, commercialized toolkits, and stolen API keys enabling abuse.
- Researchers identified phishing campaigns that use indirect prompt injections to evade AI-powered email filters. Attackers embed invisible text inside messages, using zero-size fonts or background-matched colors, so recipients see ordinary content while AI scanning tools process attacker instructions during automated security review.
- Researchers unveiled an AI-driven influence and fraud campaign run by a Russian-speaking actor behind a MAGA-themed Telegram channel with 17,000 subscribers. The operator bypassed Gemini safeguards to automate propaganda and credential theft, used stolen API keys, cracked WordPress accounts, and drained a crypto wallet.

VULNERABILITIES AND PATCHES

- Microsoft published fixes for CVE-2026-41091 and CVE-2026-45498, two actively exploited Windows Defender flaws affecting the Malware Protection Engine and Defender Antimalware Platform. The first allows local privilege escalation, while the second can cause denial of service, with updated components released automatically through normal Defender updates.
- Trend Micro addressed CVE-2026-34926, a directory traversal flaw in Apex One on-premises servers that allows attackers with administrator access push malicious code to endpoints. Exploitation attempts were observed against Windows systems, and the issue affects the enterprise endpoint security platform in corporate deployments
- Drupal released emergency patches for CVE-2026-9082, a critical SQL injection flaw affecting Drupal sites using PostgreSQL. Successful exploitation can allow database command execution, potentially leading to data theft or code execution. Active attacks were reported shortly after disclosure across thousands of sites.

  Check Point IPS provides protection against this threat *(Drupal Core SQL Injection (CVE-2026-9082))*

THREAT INTELLIGENCE REPORTS

- Check Point Research has revealed new campaigns of Nimbus Manticore, an IRGC-linked group that resurfaced during Operation Epic Fury with upgraded techniques. The campaigns use SEO poisoning and career-themed phishing across the United States, Europe, and the Middle East, and then delivered a new MiniFast backdoor.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
- Check Point researchers have highlighted a 124% surge in hacktivism and ransomware across Germany, Austria, and Switzerland in 2025. Germany accounted for most incidents, while hacktivists drove defacements and DDoS attacks, and ransomware activity was led by Akira, Qilin, and Safepay.
- Researchers have uncovered Showboat, a Linux malware family used against international telecommunications providers. The modular post-exploitation framework can hide processes, transfer files, spawn remote shells, and operate as a SOCKS5 proxy. The activity is attributed to China-aligned threat actors.
- Researchers uncovered a supply chain attack on Laravel Lang localization packages via Composer, where attackers rewrote GitHub tags to point to malicious commits. The campaign deployed a cross-platform credential stealer targeting cloud keys, developer tokens, and browser passwords across hundreds of package versions.
- Researchers identified large-scale abuse of Middle Eastern telecom and hosting networks, with more than 1,350 active command-and-control servers across 98 providers. Linked activity included Phorpiex, Eagle Werewolf espionage, exploitation of a React Native CLI flaw, and RondoDox botnet activity at significant scale.