CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- AkzoNobel, a Netherlands-based global paint manufacturer, has confirmed a cyberattack affecting one of its United States sites. The company said the intrusion was contained, while the Anubis ransomware group claimed it stole 170 GB of data, including employee and financial records.
- LexisNexis, a global legal data and analytics provider, has suffered a breach. Attackers claimed they stole 3.9 million records, including about 400,000 user profiles and some government accounts, while the company said the exposed systems mainly held legacy pre-2020 data.
- The Wikimedia Foundation, the nonprofit behind Wikipedia, has faced a self-propagating JavaScript worm that vandalized pages and replaced editor scripts across multiple wikis. Engineers briefly restricted editing while cleaning up the incident, with about 3,996 pages modified and roughly 85 users' personal scripts affected.
- TriZetto Provider Solutions, an American healthcare technology company owned by Cognizant, has disclosed a breach affecting more than 3.4 million people. The exposed data includes insurance and medical information, with notifications issued this week after investigators determined the unauthorized access began in 2024.

AI THREATS

- Researchers outlined how Pakistan-linked APT36 has used AI coding tools to produce large volumes of low-quality malware aimed at Indian government entities and embassies. The group generated variants in less common programming languages and used legitimate cloud services for command channels, complicating detection and response.
- Researchers uncovered AI-themed Chrome and Edge extensions that harvest LLM chat histories and browsing activity. Distributed via the Chrome Web Store, they impersonate legitimate tools and have impacted 900,000 users across 20,000 enterprise environments.
- Researchers tracked a campaign abusing interest in OpenClaw, an AI agent, by planting fake installers on GitHub that appeared in Bing search results. The installers delivered Vidar to steal credentials and cryptocurrency wallets and sometimes deployed GhostSocks, turning infected systems into residential proxies.
- Researchers demonstrated indirect prompt injection campaigns against AI agents that read web content, cataloging 22 techniques across live sites. Hidden instructions can redirect agents to expose data, perform unauthorized transactions, and run server commands, and the researchers also observed a real-world bypass of an AI ad review system.

VULNERABILITIES AND PATCHES

- Google has published patches for CVE-2026-0628, a high-severity vulnerability in Chrome's Gemini AI panel that allowed malicious extensions to inject code and access cameras and microphones. Researchers showed attackers could also take screenshots, access local files, and launch phishing content inside the panel.
- A patch was released for CVE-2026-1492, a critical (9.8 CVSS) privilege escalation flaw in the User Registration & Membership WordPress plugin. The vulnerability lets unauthenticated attackers create administrator accounts and take over sites.
- VMware has patched CVE-2026-22719, a high-severity command injection flaw in Aria Operations, its cloud management platform. The vulnerability allows unauthenticated remote code execution during support-assisted migrations and affects versions 8 through 8.18.5 and 9 through 9.0.1, with patches and a workaround script available.
- Qualcomm has addressed CVE-2026-21385, a memory corruption vulnerability affecting chipsets used in Android phones, tablets, and IoT devices. The flaw can trigger crashes and potentially allow code execution, and CISA said evidence of active exploitation prompted its addition to the Known Exploited Vulnerabilities catalog.

THREAT INTELLIGENCE REPORTS

- Check Point Research have mapped Iran-linked cyber clusters conducting espionage, disruption, and influence operations, including Cotton Sandstorm, Educated Manticore, MuddyWater, Handala, and Agrius. Recent campaigns used impersonation and phishing to steal credentials, remote access tools to persist, and wipers or fake ransomware for impact.
- Check Point Research revealed that, amid the ongoing conflict with Iran, IP cameras in Israel, Qatar, Bahrain, Kuwait, the UAE, and Cyprus have been intensively targeted. Notably, these countries have also experienced significant missile activity from Iran. The findings align with the assessment that Iran incorporates compromised cameras into its operational doctrine, using them both to support missile operations and to conduct ongoing battle damage assessment (BDA).
- Check Point Research has profiled Silver Dragon, a Chinese-aligned group linked to APT41 that targeted government and enterprise networks across Southeast Asia and Europe. Recent operations used the GearDoor backdoor with SSHcmd and SilverScreen, enabling remote access, covert screen capture, and stealthy control after phishing and server exploitation.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats
- Researchers have uncovered Coruna, an iPhone exploit kit used by Chinese scammers and Russia-linked operators to compromise devices through malicious websites. The toolkit used 23 exploits against iOS and deployed malware that stole cryptocurrency, emails, and photos.