CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Cellcom, a Wisconsin-based wireless provider, has been impacted by a cyberattack that resulted in widespread outages of voice and SMS services beginning on May 14, 2025. The incident disrupted communication for customers across Wisconsin and Upper Michigan, leaving them unable to make phone calls or send text messages. No threat actor has claimed responsibility yet.

- Kettering Health has been targeted in a cyberattack that resulted in a system-wide technology outage across its 14 hospitals and over 120 outpatient facilities in Ohio. The incident disrupted patient care systems and call centers, leading to the cancellation of elective inpatient and outpatient procedures. The ransom note that was left by the attackers links the incident to the Interlock ransomware group.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
  (Ransomware.Win.Interlock., Ransomware.Wins.InterLock.*)*

- Cetus Protocol has confirmed a cyberattack that resulted in the theft of $223 million in cryptocurrency from its decentralized exchange platform. The attacker exploited a vulnerability in a software package, leading to the unauthorized transfer of funds; however, $162 million of the compromised assets have been successfully paused.

- An unsecured ElasticSearch database containing over 184 million login credentials for services including Google, Microsoft, Facebook, and Apple was discovered in May 2025. The 47 GB dataset exposed plaintext usernames and passwords, with entries linked to at least 29 government domains across countries such as the U.S., U.K., Israel, and China.

- The Hauts-de-Seine department in France has been targeted by a large-scale cyberattack, forcing their IT systems and communication channels to shut down indefinitely. The attack rendered the department's network access, applications, and internal communication systems inoperable. It is yet unknown whether the attack involved a ransomware or a DDoS attack.

- Arla Foods has confirmed a cyberattack that disrupted production operations at its Upahl dairy facility in Germany. The incident disrupted the local IT network, leading to temporary production halts and potential delays or cancellations of product deliveries.

- Peter Green Chilled, a major UK logistics company, has confirmed a ransomware attack that resulted in disruptions to its order processing systems, impacting the supply of refrigerated goods to major UK supermarkets including Aldi, Tesco, and Sainsbury's. While the company's transport operations remained unaffected, the cyberattack hindered its ability to process orders, posing a risk of product spoilage.

VULNERABILITIES AND PATCHES

- Mozilla has released patches for two critical zero-day vulnerabilities in Firefox, CVE-2025-4918 and CVE-2025-4919. CVE-2025-4918 involves an out-of-bounds read/write issue in the JavaScript engine when resolving Promise objects, while CVE-2025-4919 pertains to out-of-bounds access on JavaScript objects due to array index confusion.

- Wordfence has patched a critical vulnerability (CVE-2025-4322) in the WordPress Motors theme. The flaw allows unauthenticated attackers to escalate privileges by exploiting the updatePassword() function, potentially leading to full account takeover. The vulnerability, rated as a CVSS score of 9.8, results from improper permission checks and has been actively exploited in the wild.

  Check Point IPS blade provides protection against this threat *(WordPress Motors Theme Privilege Escalation (CVE-2025-4322))*

- Details on critical vulnerabilities in Versa Concerto have been disclosed, including CVE-2025-34027 (CVSS 10.0), which allows unauthenticated attackers to exploit a URL decoding inconsistency and race condition to upload malicious files and achieve remote code execution via ld.so.preload. Another critical flaw, CVE-2025-34028 (CVSS 9.1), enables authentication bypass through improper handling of URL-encoded paths, granting unauthorized access to protected endpoints.

  Check Point IPS blade provides protection against this threat *(Versa Concerto Authentication Bypass)*

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered a global malware campaign that impersonates the popular AI media generation platform Kling AI. Threat actors created counterfeit Facebook pages and paid advertisements to lure users to a fraudulent website mimicking Kling AI, where users were prompted to generate AI content. Instead of delivering legitimate media files, the site provided downloads which were actually malicious executables, ultimately installing infostealers designed to exfiltrate credentials and session tokens.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat

- Security researchers have identified a cryptojacking campaign exploiting exposed Docker Engine APIs to deploy malicious containers running a Dero cryptocurrency miner. The attackers utilize Docker images that mimic legitimate containers, such as "pause," embedding UPX-packed binaries with hardcoded wallet addresses and mining pool URLs to evade detection.

- Researchers have uncovered a Bing SEO poisoning campaign used to deliver Bumblebee malware via malicious pages masquerading as popular software installers. The attackers leveraged SEO techniques to rank malicious links for software like Zoom, Slack, and Citrix, redirecting users through a traffic distribution system (TDS) to download the trojanized files.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(Trojan-Downloader.Win.Bumblebee.*, Trojan-Downloader.Wins.Bumblebee.*)*