December 22 – 28, 2025

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Romanian Waters, the country's national water management authority, was hit by a ransomware attack that resulted in nearly 1,000 computer systems across national and regional offices being encrypted. The attack affected geographic information systems, databases, email, web servers, and Windows workstations. Operational technology controlling water infrastructure was not impacted, and no data leakage has been reported, but key IT services were disrupted across the organization.

- France's postal service La Poste has suffered a cyber-attack that disrupted key digital systems, impacting online parcel tracking, mail distribution, and banking services for customers of both the postal service and La Banque Postale. Some services were temporarily unavailable, with no evidence of data compromise. The attack was claimed by the pro-Russian hacktivist group NoName057(16).

- Insurance giant Aflac has confirmed a data breach they experienced in June that resulted in the theft of sensitive files containing insurance claims, health data and Social Security numbers. The breach affected personal details of approximately 22.7 million individuals in its US business. The attack has been attributed to Scattered Spider threat group.

  Check Point Harmony Endpoint provides protection against this threat.

- Japan's leading carmaker Nissan Motor Corporation has acknowledged a data breach that resulted in the exposure of personal information for approximately 21,000 customers from Nissan Fukuoka Sales Corporation including names, addresses, phone numbers, email addresses, and sales operation data. The incident occurred after unauthorized access to Red Hat data servers led to the leak, but financial data was not affected. The Crimson Collective threat actor claimed responsibility for the initial breach, with ShinyHunters later hosting samples of the stolen data.

- Trust Wallet, a popular non-custodial cryptocurrency wallet, has disclosed a cyber-attack involving a compromised Chrome extension update. The attack exfiltrated sensitive wallet data, including seed phrases, to a malicious domain, resulting in at least $7 million in losses. The incident primarily affected users of Chrome extension version 2.68.0, allowing attackers to drain wallets.

- Ubisoft's live service game Rainbow Six Siege (R6) has confirmed a cyber-attack in which threat actors abused internal systems to manipulate bans, unlock all cosmetics and developer-only skins, and distribute around $13.33 million worth of in-game currency worldwide.

- Baker University has encountered a data breach that resulted in attackers accessing its network and stealing sensitive information belongs to 53,624 students, alumni, staff, and affiliates of the university, such as names, Social Security numbers, financial account details, and medical records.

VULNERABILITIES AND PATCHES

- A high-severity memory-read vulnerability, CVE-2025-14847, dubbed "MongoBleed" has been identified in multiple MongoDB Server versions, allowing unauthenticated remote attackers to exploit a zlib implementation flaw and potentially access uninitialized heap memory. The issue, caused by improper handling of length parameter inconsistency (CWE-130), may permit arbitrary code execution and system compromise. Affected versions include MongoDB 4.0 through 8.2.3.
- Details on a critical serialization injection vulnerability in LangChain Core were disclosed. CVE-2025-68664 (CVSS 9.3) affects langchain-core, where unescaped user-controlled dictionaries with lc keys are treated as trusted objects during deserialization, enabling secret extraction, prompt injection, and potentially arbitrary code execution.
- A critical buffer overflow vulnerability, CVE-2025-68615, in Net-SNMP's snmptrapd daemon can be triggered remotely via a specially crafted packet. The issue has a CVSS score of 9.8 and may allow unauthenticated attackers to achieve remote code execution or cause service crashes. Patches are available, and the vulnerability is addressed in Net-SNMP versions 5.9.5 and 5.10.pre2.

THREAT INTELLIGENCE REPORTS

- Check Point researchers describe a phishing campaign in which attackers abused Google Cloud Application Integration's "Send Email" workflow to send over 9,000 spoofed Google notification emails from a Google address. The messages targeted manufacturing, technology, and finance sectors and used multi-step redirection through Google domains to lead victims to a Microsoft-themed credential harvesting site. Most victims located in the US, Asia-Pacific, and Europe.
- Researchers uncovered a two-year Evasive Panda campaign using adversary-in-the-middle DNS poisoning to deliver MgBot via fake updaters and stealthy loaders. The chain used multi-stage shellcode, hybrid encryption, and DLL sideloading to run MgBot in memory, with victim-specific payloads tied to machines via DPAPI and RC5. Attackers poisoned legitimate domains, injected into signed system processes for persistence, and updated configs with hardcoded C2s.

  Check Point Harmony Endpoint provides protection against this threat (Infostealer.Win.MgBot)
- A Webrat campaign leveraged fake GitHub repositories masquerading as exploit and proof-of-concept code for high-severity CVEs, targeting gamers, students, and inexperienced security researchers. The attack uses droppers to elevate privileges, disable Windows Defender, and deploy the Webrat backdoor, enabling remote control, credential theft, keylogging, and device surveillance.
- Researchers found lotusbail, a malicious npm package masquerading as a WhatsApp Web API library that intercepts messages and steals session/auth data, contacts, and media via WebSocket tampering and device-pairing hijack. Separately, 14 malicious NuGet packages were found redirecting crypto funds and stealing Google Ads OAuth tokens.