CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Three major UK retailers - Co-op, Harrods and Marks & Spencer (M&S) - were hit by cyberattacks that disrupted operations and compromised sensitive data. The attacks are believed linked to the Scattered Spider gang, while DragonForce ransomware gang claimed responsibility for the attacks.

- The American non-profit healthcare system, Ascension, experienced a data breach following a third-party hacking incident in December 2024. The attack led to the theft of patients' personal and health information, including names, addresses, Social Security numbers, and inpatient records. Although no threat actor has claimed responsibility, the timeline suggests a possible link to a series of Cl0p ransomware attacks that exploited a zero-day vulnerability in the Cleo secure file transfer software.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.Clop; Ransomware.Wins.Clop; Ransomware.Wins.Clop.ta.)*

- Hitachi Vantara, a subsidiary of Japanese Hitachi, has suffered a cyberattack that disrupted parts of its systems. The attack was claimed by Akira ransomware gang which allegedly stole files from the company's network and left ransom notes on compromised machines.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Wins.Akira.ta.; Ransomware.Wins.Akira; Ransomware.Win.Akira; Trojan.Win.Akira)*

- Media firm Urban One was hit by a cyberattack that occurred in February, resulting in data leakage of 2.5TB of employees' personal data such as names, addresses, Social Security numbers, direct deposit information and W-2 information. The attack was claimed by Cactus ransomware gang.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.Cactus; Ransomware.Wins.Cactus.ta.)*

- Several public and private organizations in the Netherlands have confirmed a series of DDoS attacks linked to the pro-Russian hacktivist group NoName057(16). These attacks caused access issues and service disruptions across key entities. While no data breaches or system compromises have been reported, the group appears to be responding to the Netherlands' military support for Ukraine.

- Texas-based employee benefits administration company, VeriSource Services, has been a victim of a data breach that occurred in February 2024, impacting over four million people. The breach exposed sensitive data, including full names, addresses, dates of birth, gender, and Social Security numbers.

- Nova Scotia Power, along with its parent company Emera, suffered a cyberattack affecting their Canadian network and business servers. The incident disrupted customer service and online access for over 500,000 clients. Operations remained unaffected, however delays have increased.

VULNERABILITIES AND PATCHES

- SonicWall reported active exploitation of two older vulnerabilities (CVE-2023-44221 and CVE-2024-38475) affecting its Secure Mobile Access (SMA) appliances. CVE-2023-44221 is a high-severity command injection flaw in the SMA100 SSL-VPN interface exploitable by admins, while CVE-2024-38475 affects Apache HTTP Server and allows unauthenticated remote code execution.

  Check Point IPS provides protection against this threat *(SonicWall SMA Command Injection (CVE-2023-44221), Apache HTTP Server Remote Code Execution)*

- Google's 2024 0-days report highlighted 75 zero-day vulnerabilities exploited in the wild, with 33 targeting enterprise technologies. Enterprise-focused products - especially security and networking software - accounted for 44% of the total. Many of the exploits involved platforms such as WebKit, Firefox, revealing attackers' focus on both widely used and specialized technologies.

- A set of 17 vulnerabilities, dubbed "Airborne", was discovered in Apple's AirPlay protocol and SDK. Two flaws (CVE-2025-24252 and CVE-2025-24132) enable wormable zero-click RCE attacks, allowing local network compromise of Apple and third-party devices. Apple issued patches for affected products, including iPhones, iPads, Macs, and Apple Vision Pro.

- Two misconfiguration-related vulnerabilities, CVE-2025-23242 and CVE-2025-23243, have been disclosed in NVIDIA Riva deployments. These flaws could allow unauthorized access and potential abuse of AI services like speech recognition and text-to-speech.

THREAT INTELLIGENCE REPORTS

- Check Point Research released 2025 AI Security Report with an analysis detailing main AI-driven threats, including LLM poisoning, retrieval manipulation, and AI-powered malware. The report highlights AI powered social engineering and the complete loss of digital identities in the age of AI. It also covers Dark LLMs like WormGPT and how AI is used by cybercriminals to process stolen data.

- Researchers have identified Gremlin Stealer, a C#-based infostealer sold on cybercrime forums and Telegram. The malware can exfiltrate data from browsers, clipboards, and local disks, targeting cookies, crypto wallets, FTP and VPN credentials, as well as session data from Telegram and Discord. It also bypasses Chrome cookie V20 protections and uploads stolen data to a remote server.

- Researchers have uncovered Outlaw, a Perl-based cryptomining botnet targeting Linux systems by exploiting weak or default SSH credentials. The attackers deploy custom XMRig miners, terminate competing miners to conserve resources, and use an IRC-based client for DDoS attacks, file uploads, and backdoor access. The botnet primarily targets devices in the United States.

- Researchers have discovered a coordinated supply chain attack involving 21 backdoored Magento extensions from vendors Tigren, Meetanshi, and MGS, affecting 500–1,000 e-commerce stores. The PHP backdoor, injected as early as six years ago and activated on April 20, allows remote code execution leading to data theft, skimmer injection, and admin account creation.