April 21 - 27, 2025

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- British retailer Marks & Spencer (M&S) experienced a cyber-attack that caused disruptions to its online order system and in-store contactless payments. The company suspended online orders temporarily, refunded some customers, and reported the incident to the Information Commissioner's Office (ICO).
- Yale New Haven Health (YNHHS), the largest healthcare provider in Connecticut, reported a massive data breach affecting approximately 5 million individuals. The breach stemmed from vulnerabilities in the systems of a third-party vendor, Perry Johnson & Associates (PJ&A), exposing names, addresses, birth dates, Social Security numbers, medical data, and insurance information.
- Blue Shield of California disclosed a data breach affecting 4.7 million members, after a protected health information was shared with Google Ads platforms due to a misconfiguration. Exposed data included insurance details, medical claims, personal data and search queries. The issue occurred between April 2021 and January 2024 and was discovered in February 2025.
- Baltimore City Public Schools (BCPS) suffered a cyber-attack affecting 25,000 current and former staff and students, causing disruptions to systems and access to educational resources. The Cloak Ransomware group has claimed responsibility for the attack, posting some of the allegedly stolen data on the Dark Web.
- South African telecommunications giant MTN confirmed a cybersecurity incident resulting in unauthorized access to personal information of some customers. The company also stated that its critical infrastructure and customer services remain unaffected. Investigations into the extent of the breach are ongoing.
- A cyberattack targeted Aigües Ter Llobregat (ATLL), a water supplier for Barcelona and surrounding areas. Though ATLL said the attack did not impact water service, threat actors accessed internal systems and files, and the company warned these may include financial and personal details of customers.
- Onsite Mammography, a healthcare service provider in Massachusetts, reported a data breach after an unauthorized third party gained access to its systems after gaining access to an employee’s email account. Compromised information of over 357,000 patients includes names, contact details, medical records, and Social Security numbers.
- The City of Abilene, Texas, disclosed a cybersecurity incident which impacted several internal systems. While services were temporarily disrupted, city officials stated that emergency services and public safety operations remained operational. Officials have yet to confirm if data was compromised.

VULNERABILITIES AND PATCHES

- Researchers reported active exploitation of a zero-day vulnerability in SAP NetWeaver. The flaw, CVE-2025-31324, has received a 10.0 CVSS score and allows unrestricted file upload. In an active campaign, threat actors have exploited the vulnerability to deliver webshells, eventually installing the Brute Ratel framework on victims' networks.

  Check Point IPS provides protection against this threat (SAP NetWeaver Remote Code Execution (CVE-2025-31324))

- Two zero-day vulnerabilities seen massively abused in the wild —CVE-2025-32432 in Craft CMS and CVE-2024-58136 in the Yii framework— have been patched. By chaining these flaws, attackers uploaded a PHP file manager, facilitating data theft and the installation of backdoors. Administrators are advised to update their systems and rotate security credentials.

  Check Point IPS provides protection against this threat (Craft CMS Remote Code Execution)

THREAT INTELLIGENCE REPORTS

- Check Point Research reported a 126% year-over-year increase in ransomware attacks during Q1 2025, with 2,289 victims listed by 74 ransomware groups. Cl0p led the activity by exploiting zero-day vulnerabilities in Cleo file transfer products, mainly targeting North American consumer goods companies. Researchers also observed some groups fabricating victim claims to inflate their visibility.
- Check Point uncovered global phishing campaigns exploiting the death of Pope Francis, where attackers impersonated charities to solicit fraudulent donations. These scams tricked victims into providing personal and financial information via fake websites. Researchers warned users to remain cautious of emotionally charged lures tied to major world events.
- Researchers report that since March 2025, Russian-linked threat actors UTA0352 and UTA0355 have been targeting individuals and organizations connected to Ukraine and human rights groups. Attackers initiate contact via Signal or WhatsApp, impersonating European officials, and persuade victims to provide Microsoft-generated authorization codes, granting unauthorized access to their Microsoft 365 accounts by abusing Microsoft OAuth 2.0 authentication workflows.
- Researchers have reported on a new campaign by China-linked APT group Billbug (AKA Lotus Blossom). The campaign targeted multiple entities in an unnamed Southeast Asian country, including a government ministry and a telecom operator. The group has developed and employed new tools for credential theft from the Chrome browsers of compromised victims.
- Researchers have discovered that blockchain platform XRP Ledger's official NPM package (xrpl.js) was compromised and infected with a backdoor that steals cryptocurrency credentials. The threat actors tried to obfuscate the changes in various package updates. The package has more than 140,000 weekly downloads, and the malicious versions were online for a period of 16 hours.