CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Fashion giant Dior confirmed a data breach that exposed customer information from its Fashion and Accessories line. The leaked data includes names, gender, phone numbers, email addresses, postal addresses, and purchase history with customers in South Korea and China most affected. Specific details regarding the quantity and additional countries affected remain undisclosed.
- Cryptocurrency exchange Coinbase experienced a data breach that resulted in unauthorized access to customer data and a $20 million ransom demand. The breach led to the exposure of personal information of approximately 1 million customers, including names, contact details, and government issued IDs. Though the threat actors behind the breach have not yet been identified, Coinbase emphasized that no customer passwords, private keys, or funds were compromised.
- The US's largest steel producer, Nucor Corporation, has suffered a cyber-attack that compromised parts of its network systems, resulting in significant disruptions and temporary suspension of production at multiple locations. The severity of the impact on Nucor's business, as well as possible data breaches, remain uncertain at this time. No threat actor has claimed responsibility.
- The Alabama state government was the victim of a cyber-attack on May 9 that disrupted some of its communications and potentially compromised some state employee usernames and passwords. While it's currently believed that no resident's personally identifiable information was compromised, the full impact of the attack, including the exact data affected, is still unknown.
- Global Crossing Airlines Group (GlobalX) has confirmed a cyber attack that gave hackers access to systems supporting parts of its business applications. The breach resulted in theft of flight records and manifests, affecting the data related to its ICE deportation flights. An anonymous hacktivist group is possibly behind the attack, claiming to have defaced GlobalX's subdomains.
- Russian private hospital Lecardo Clinic was hit by a cyber-attack that resulted in a three-day shutdown of its operations. The threat actors targeted the clinic's software used to handle patient records, with the potential compromise of additional similar systems. The pro-Ukraine hacktivist group 4B1D has claimed responsibility for this breach, stating it disrupted more than 100 computers, encrypted, wiped and exported patient data, including personal details, for an estimated 52,000 patients and staff, with around 2,000 records reported to have been sold on the dark web.
- The Australian Human Rights Commission (AHRC) has disclosed a data breach that resulted in the exposure of hundreds of private documents on major search engines. The breach, which occurred between 2021 and 2025, impacted submissions that exposed sensitive information such as names, contact info, health records, religious beliefs, and photos. The organization stated no malicious external attack was responsible, and no threat actor has claimed responsibility yet.

VULNERABILITIES AND PATCHES

- A patch has been released for CVE-2025-31324 and CVE-2025-42999, two SAP NetWeaver Visual Composer flaws that, when chained, enable unauthenticated remote code execution. These vulnerabilities have been exploited in the wild by ransomware groups such as RansomEXX and BianLian, as well as Chinese APTs to deploy web shells, Brute Ratel, and PipeMagic malware, compromising over 580 instances, including critical infrastructure.

  Check Point IPS and Threat Emulation provide protection against this threat *(SAP NetWeaver Remote Code Execution (CVE-2025-31324); Ransomware.Win.Ransomexx.glat; Ransomware.Wins.BianLian.ta.*; Ransomware.Wins.BianLian; Backdoor.Wins.BianLian; HackTool.Wins.BianLian)*

- Fortinet has issued security updates addressing a critical remote code execution vulnerability (CVE-2025-32756), exploited as a zero-day in attacks on FortiVoice enterprise phone systems. The stack-based overflow flaw also affects additional Fortinet devices, including FortiMail, FortiNDR, FortiRecorder, and FortiCamera. Successful exploitation by a remote, unauthenticated attacker could result in arbitrary code or command execution via maliciously crafted HTTP requests.

- Google has released a patch for a high-severity flaw (CVE-2025-4664) in its Chrome web browser, which if exploited, could lead to full account takeover. The vulnerability allows attackers to leak cross-origin data via malicious HTML. Evidence of this exploit existing in the wild has been reported, although it remains uncertain whether it has been utilized in attacks.

THREAT INTELLIGENCE REPORTS

- Check Point Research identified a large-scale phishing campaign using fake email quarantine alerts to steal credentials. The attackers, who managed to send out 32,000 malicious emails to 6,358 customers from compromised accounts of three different domains, employed manipulative subject lines to create an illusion of urgency and legitimacy, compelling the recipients to act. Most targets were in North America (90%), with others in Europe and Australia.

- Check Point Research found a sophisticated phishing campaign targeting healthcare organizations, impersonating medical service providers like Zocdoc. The campaign, which started on March 20, launched cyber attacks on healthcare organizations resulting in over 276 million patient records being compromised. The threat actors' goal is to steal patient data, build identity kits, and use them for psychological warfare or fraud, including medical services.

- Check Point Research uncovered a 94% surge in weekly cyberattacks towards telecommunications infrastructure in Q1 2025, driven by growing reliance on 5G, AI, and automation. These threats risk disrupting national services, emergency response, and financial systems.

- Check Point Research reports a sharp rise in ransomware attacks in 2025, driven by RaaS and AI-generated malware. Ransomware has evolved into multi-stage extortion targeting data, uptime, and public trust - especially in US business, manufacturing, and retail sectors. Tactics now include data extortion, disinformation, and AI-assisted targeting.