February 17 - 23, 2025

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research covers the recent ByBit hack, one of the largest thefts in digital asset history, its implications for crypto security, and security recommendations. In this event, hackers gained access to an offline Ethereum wallet and stole $1.5 billion worth of digital assets. The attack occurred during a routine transfer from an offline cold wallet to a warm wallet, where attackers manipulated the transaction to divert funds to an unknown address. Blockchain analytics firms have attributed the heist to North Korea's Lazarus Group.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
  (APT.Wins.Lazarus., APT.Win.Lazarus.*, APT.Wins.Lazarus.ta.*)*

- Ecuador's National Assembly has gone through two cyberattacks targeted at disrupting its systems and accessing sensitive data. The attack took place a week after the country's general election. No details were shared about the impact of the incident or the threat actor behind it.

- Genea, a leading Australian fertility services provider, has experienced a cyber-attack resulting in unauthorized access to its data. The company is currently investigating the nature and extent of the accessed information, including potential exposure of personal data. While some systems were taken offline as a precaution, Genea assures minimal disruption to patient treatments.

- Germany's security services identified a Russian disinformation campaign aimed at influencing the country's federal elections. The campaign, attributed to the group Storm-1516, involves fake videos circulating on social media, falsely depicting ballot manipulation targeting the Alternative for Deutschland (AfD) party. Reports indicate broader efforts to amplify support for the AfD using inauthentic social media accounts.

- New York-based venture capital and private equity firm, Insight Partners, has been a victim of a cyber-attack that resulted in unauthorized access to some of its information systems in January 2025, through a social engineering attack.

- Vorwerk's Thermomix recipe forum, Rezeptwelt.de, suffered a data breach exposing 3.3 million user records. An external service provider's compromised server leaked names, addresses, birth dates, phone numbers, emails, and cooking preferences. Affected users span the Czech Republic, Spain, France, Italy, Poland, Portugal, and Australia.

- CarMoney, a Russian microfinance company, has confirmed a cyberattack that forced it to shut down all systems after attackers sent spam messages to customers, falsely claiming the company was closing and writing off all debts. The Ukrainian Cyber Alliance, a group of pro-Ukraine hacktivists, has claimed responsibility.

VULNERABILITIES AND PATCHES

- A high-severity elevation of privilege vulnerability (CVE-2025-24989) in Microsoft Power Pages was actively exploited as a zero-day before being patched. The flaw allowed attackers to bypass access restrictions on public-facing websites using Power Pages, potentially leading to unauthorized access. Microsoft addressed the vulnerability at the service level and notified affected customers.
- Researchers share technical information on four critical vulnerabilities in Ivanti Endpoint Manager (EPM), allowing unauthenticated attackers to coerce the EPM machine account credential for relay attacks, potentially leading to server compromise. The flaws, Credential Coercion Vulnerabilities (CVE-2024-10811 in GetHashForFile, CVE-2024-13161 in GetHashForSingleFile, CVE-2024-13160 in GetHashForWildcard, and CVE-2024-13159 in GetHashForWildcardRecursive), have been patched.

  Check Point IPS provides protection against these threats (Ivanti Endpoint Manager Path Traversal)
- A newly identified code injection vulnerability (CVE-2025-23209) affects Craft CMS versions 4 and 5, allowing remote code execution when user security keys are compromised. The flaw, now patched, enables attackers to manipulate input fields and inject malicious code into the system. CISA has added the vulnerability to its Known Exploited Vulnerabilities catalog due to observed exploitation.

THREAT INTELLIGENCE REPORTS

- Check Point Research elaborates about threat activity cluster that has been exploiting CVE-2024-24919, a Check Point vulnerability patched in May 2024, to deploy ShadowPad malware. In some cases, NailaoLocker ransomware was also deployed following the initial infection. The campaign, active between June 2024 and January 2025, targeted organizations across Europe, Africa, and the Americas, with the manufacturing sector being the most affected.

  Check Point Harmony End Point, Threat Emulation and IPS provide protection against this threat (behavioral.win.dllsideloading.s , ransomware.win.honey; RAT.Wins.ShadowPad.ta.G; Check Point VPN Information Disclosure (CVE-2024-24919)).
- Check Point Research has found a method to evade detection by exploiting statistical anomalies in the human interaction modules of several sandbox solutions. They provide an alternative algorithm for simulated mouse human interaction, including its specifications, parameters, source code, and visual demonstrations. This approach aims to enhance the effectiveness of sandbox emulation against sophisticated evasion techniques.
- Check Point has identified that cyber criminals are deploying sophisticated URL manipulation techniques within standard phishing emails, such as fake invoices and account activation notices. Their primary deception method exploits the 'userinfo' portion of web addresses—the segment between 'http://' and the '@' symbol—to make malicious URLs appear legitimate.