March 17 – 23, 2025

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Municipalities in four US states experienced cyberattacks that disrupted services for county offices, courts, and schools. Cleveland Municipal Court was hit by Qilin ransomware attack, forcing employees offline and delaying trials, while Strafford County, Pelham School District, and Derby Police Department also reported service disruptions which were not claimed by any specific threat actor.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Wins.Qilin)

- Blockchain gaming platform WEMIX has confirmed a cyberattack that resulted in the theft of 8,654,860 tokens, valued at nearly $6.1M. The breach, occurred on February 28, 2025, impacted the blockchain gaming platform's token holders, potentially exposing them to financial losses.
- Threat actor "rose87168" on a dark web forum has claimed responsibility for an attack against Oracle which allegedly compromised 6M records from its Cloud SSO platform. The breach exposed encrypted SSO passwords, Java KeyStore (JKS) files, and other sensitive credentials, potentially impacting over 140K businesses. Oracle denies it was breached in any way, claiming that published credentials are not for the Oracle Cloud and no Oracle Cloud customers experienced a breach or lost any data.
- Giant US sperm bank California Cryobank has been a victim of a data breach that resulted in the exposure of personal information such as names, bank account details, Social Security numbers, driver's license numbers, payment card data, and health insurance details. The incident potentially impacted an unknown number of customers. No threat actor has claimed responsibility yet.
- Arizona-based Western Alliance Bank has suffered a data breach that resulted in the exposure of sensitive personal and financial information belonging to almost 22K individuals. The breach was caused by an October 2024 cyberattack on a third-party file transfer software, compromising names, Social Security numbers, driver's license details, and financial account numbers.
- Swiss telecommunications solutions provider Ascom has experienced a cyberattack that affected the company's technical ticketing system and resulted in the exfiltration of 44GB of corporate data. The exposed sensitive internal information includes source code, invoices, and confidential documents. The Hellcat ransomware group has claimed responsibility for the attack.
- The Pennsylvania State Education Association (PSEA) has disclosed a data breach from July 2024 that resulted in the theft of sensitive information belonging to over 517,000 members. The stolen data includes government-issued IDs, Social Security numbers, passport details, and financial information.

VULNERABILITIES AND PATCHES

- US cybersecurity agency CISA warned of an absolute path traversal vulnerability (CVE-2024-48248, CVSS 8.6) in Nakivo Backup and Replication that enables attackers to read arbitrary files and access sensitive data including configuration files and credentials. Exploitation may allow remote code execution and further compromise enterprise environments, with attempts observed in the wild.

  Check Point IPS provides protection against this threat (NAKIVO Arbitrary File Read (CVE-2024-48248))

- New critical vulnerability (CVE-2024-54085) was found in AMI's MegaRAC BMC software that enables an authentication bypass via remote management interfaces like Redfish. Exploitation of this flaw allows remote server control, malware deployment, firmware tampering, and potential hardware bricking. Affected devices include HPE Cray XD670, Asus RS720A-E11-RS24U, and ASRockRack.

- A patch has been released to address a critical vulnerability (CVE-2025-23120) in Veeam Backup & Replication software that allows remote code execution by authenticated domain users. The flaw stems from inconsistent deserialization handling that permits exploitation via unblocked classes such as Veeam.Backup.EsxManager.xmlFrameworkDs and Veeam.Backup.Core.BackupSummary.

THREAT INTELLIGENCE REPORTS

- Check Point Research uncovered a new and rapidly growing ransomware-as-a-service (RaaS) affiliate program that is dubbed VanHelsingRaaS. Check Point Research discovered two VanHelsing ransomware variants targeting Windows, but as the RaaS mentions in its advertisement, it provides more offerings “targeting Linux, BSD, ARM, and ESXi systems”. In less than two weeks since its introduction to the cybercrime community, this ransomware operation has already infected three known victims, demanding large ransom payments for decryption and the deletion of stolen data.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat

- Check Point researchers have reported about a sophisticated credential harvesting attack that leverages Firebase, a popular web application hosting service. This attack involves the creation of highly convincing and professionally designed phishing web pages that impersonate well-known services.

- Researchers found that affiliates of the RansomHub ransomware-as-a-service (RaaS) operation are utilizing a custom-developed backdoor named 'Betruger' in their attacks. This multi-functional malware facilitates various malicious activities, including credential dumping, privilege escalation, network scanning, keylogging, and screenshot capturing. The adoption of such a bespoke tool signifies a strategic shift towards minimizing the use of multiple tools during ransomware preparations, thereby reducing the likelihood of detection.

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