March 3 - 9, 2025

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The City of Mission, Texas, has declared a local state of emergency following a severe cybersecurity incident that threatens to expose protected personal information, health records, and other critical data managed by city departments. The emergency declaration was issued by Mayor Norie Gonzalez Garza on March 4, 2025, after the cyber-attack was identified on February 28, 2025. City officials are concerned that sensitive government data could be compromised, potentially leading to identity theft, disruption of city services, and legal complications if the breach is not contained.

- National Presto Industries has experienced a cyberattack that began on March 1, causing system outages impacting shipping, receiving, manufacturing processes, and back-office functions. The American company has implemented temporary measures to maintain critical operations while systems are being restored. Law enforcement has been notified, and an incident response team is conducting a forensic analysis to determine the scope of the incident.

- The Toronto Zoo has been hit by a ransomware attack in January 2024, exposing visitor transaction data from 2000 to 2023. Stolen data includes names, addresses, phone numbers, emails, and partial credit card details from recent transactions. The Akira ransomware group claimed responsibility, stating they exfiltrated 133GB of data, including confidential agreements and personal files.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Ransomware_Linux_Akira_C/D, Ransomware.Wins.Akira.G/H)

- The Russian-linked Qilin ransomware group has allegedly breached Ukraine's Ministry of Foreign Affairs, stealing data such as private correspondence and personal information. Qilin claims some of this data has already been sold. The Ministry has not confirmed the breach.

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

- NTT Communications Corporation has experienced a cyber-attack that resulted in unauthorized access to its distribution system, compromising data of above 17,000 customers. The breach, discovered on February 5, exposed customer names, contract numbers, phone numbers, email and physical addresses, and service usage information. No threat actor has claimed responsibility yet.

- Penn-Harris-Madison school district in Indiana has suffered a ransomware attack. According to the school district, the attack caused disruptions in school operations, but student Social Security numbers where not leaked in the attack.

- Poland's space agency, POLSA, has recently announced they have been the victim of a cyber-attack. Unauthorized access to the agency's IT infrastructure was detected and affected systems have been secured. The incident is currently under investigation to identify the attackers behind the breach.

VULNERABILITIES AND PATCHES

- A critical out-of-bounds write vulnerability (CVE-2025-22224), which is actively exploited, is affecting over 37,000 internet-exposed VMware ESXi servers. This flaw allows local attackers with administrative privileges on a VM guest to escape the sandbox and execute code on the host as the VMX process. Despite available patches and the flaw inclusion in CISA's Known Exploited Vulnerabilities (KEV) Catalog, a significant number of servers remain unpatched.
- Google has released its March 2025 Android Security Bulletin, addressing 44 flaws, two of them are high-severity ones actively exploited: a privilege escalation in the Framework component (CVE-2024-43093), and a privilege escalation in the HID USB component of the Linux kernel (CVE-2024-50302).
- CISA has added five security flaws affecting Cisco, Hitachi Vantara, Microsoft, and Progress WhatsUp Gold to its KEV catalog. These include a command injection vulnerability in Cisco Small Business RV Series routers (CVE-2023-20118); two flaws (CVE-2022-43939, CVE-2022-43769) in Hitachi Vantara Pentaho BA Server; an improper resource shutdown issue in Microsoft Windows Win32k (CVE-2018-8639); and a path traversal vulnerability in Progress WhatsUp Gold (CVE-2024-4885).

  Check Point IPS provides protection against this threat (Hitachi Vantara Pentaho Business Analytics Server Authentication Bypass (CVE-2022-43939), Hitachi Vantara Pentaho Business Analytics Server Remote Code Execution (CVE-2022-43769), Microsoft Win32k Elevation of Privilege (CVE-2018-8639), WhatsUp Gold Remote Code Execution (CVE-2024-4885))

THREAT INTELLIGENCE REPORTS

- The FBI and CISA warn of a mail scam campaign threating data exposure from a group masquerading as the notorious BianLian ransomware. The campaign uses physical letters, demanding between $250,000 to $500,000 in Bitcoin from corporate executives, claiming unauthorized data access and threaten exposure on ransomware leak sites. Although the linkages to the actual BianLian remain uncertain, the threat actors are primarily targeting executives across the US healthcare industry.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Wins.BianLian.ta.; Ransomware.Wins.BianLian; Backdoor.Wins.BianLian; HackTool.Wins.BianLian)*
- Researchers have identified a large-scale malvertising campaign impacting over one million devices globally. The attack originates from illegal streaming websites embedded with malvertising redirectors, leading users to intermediary sites and subsequently to platforms like GitHub, Discord, and Dropbox, which host the malicious payloads. The campaign employs a sophisticated redirection chain and utilizes various malware, including Lumma Stealer and Doenerium.
- Researchers have noted a 42% increase in Medusa ransomware attacks from 2023 to 2024, with incidents doubling in early 2025. Medusa, operated as a ransomware-as-a-service (RaaS) by the group tracked as Spearwing, employs double extortion tactics, steals and encrypts data.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Ransomware.Wins.MedusaLocker.ta.; Ransomware.Wins.MedusaLocker.*; Trojan.WIN32.Medusalocker.*)*