CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- One of South Korea's largest ticketing platforms Yes24 has been a victim of a ransomware attack that resulted in a four-day service outage, disrupting online bookings for concerts, e-book access, and community forums. The incident has caused significant turmoil in the entertainment industry, forcing event cancellations and delays for high-profile K-pop stars, musicals, and other performances, while raising concerns about potential unauthorized access to customer personal data.
- WestJet, Canada's second-largest airline, was hit by a cyberattack that resulted in partial access to internal systems, including the WestJet app and website. Users were temporarily unable to log into these services, and the attack has impacted access to critical software and operations.
- Grocery wholesaler giant United Natural Foods (UNFI) has confirmed a cyberattack that resulted in the shutdown of certain systems, impacting its ability to fulfill and distribute customer orders. The incident has caused significant disruptions to business operations, with employees' shifts being reportedly canceled and affected systems were taken temporarily offline. No threat actor has claimed responsibility yet, and it remains unclear whether any data was stolen during the breach.
- Global industrial tech company Sensata Technologies has disclosed a data breach resulting from a ransomware attack that occurred between March 28, 2025, and April 6, 2025. The breach led to the exfiltration of sensitive data, including full names, addresses, Social Security Numbers, driver's license numbers, financial information, medical information, and other personal details belonging to current and former employees and their dependents.
- American insurance company Erie Insurance has confirmed a cyberattack that resulted in widespread platform outages and business disruptions, leaving customers unable to log into the portal, file claims, or access paperwork. The attack has impacted the company's systems, but there is currently no information on whether data was stolen or leaked.
- The Texas Department of Transportation (TxDOT) has suffered a data breach that resulted in the unauthorized download of 300K crash records from its Crash Records Information System (CRIS). The leaked data includes sensitive information such as names, addresses, driver's license numbers, license plate numbers, car insurance policy information and more.
- Thomasville, North Carolina, has experienced a cyberattack that resulted in multiple city systems being taken offline, though essential services remain operational, and it is unclear whether any sensitive information was accessed or compromised. Similarly, the Ogeechee Judicial Circuit District Attorney's Office in Georgia was hit by a cyberattack, leading to phone and internet outages, office closures, and significant disruption to its operations across four counties.

VULNERABILITIES AND PATCHES

- Microsoft has published June's Patch Tuesday, addressing 66 vulnerabilities across the company's products. Among the vulnerabilities is CVE-2025-33053, an actively exploited zero-day remote execution vulnerability in WEBDAV, which was disclosed by Check Point Research.

  Check Point IPS provides protection against this threat *(Microsoft Web Distributed Authoring and Versioning Remote Code Execution (CVE-2025-33053))*

- GitLab released security patches addressing critical vulnerabilities, notably CVE-2025-4278, a high severity HTML injection flaw enabling remote account takeovers, and CVE-2025-5121, a high severity missing authorization issue permitting attackers to inject malicious CI/CD jobs into pipelines.

- Trend Micro has released patches addressing critical vulnerabilities in its Endpoint Encryption PolicyServer and Apex Central, including pre-authentication remote code execution flaws (CVE-2025-49212, CVE-2025-49213) enabling unauthenticated SYSTEM-level access.

THREAT INTELLIGENCE REPORTS

- Check Point Research discovered a cyber espionage campaign by Stealth Falcon group. The campaign was exploiting a zero-day vulnerability (CVE-2025-33053) to deliver malware via .url files, executing malware from WebDAV server. The group targets government and defense entities in the Middle East and Africa using spear-phishing, multi-stage infections, and custom implants like Horus Agent. Tools include keyloggers, credential dumpers, and evasion tactics.

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

- Check Point Research uncovered a malware campaign abusing Discord's invite system to redirect users to malicious servers. It delivers AsyncRAT and a custom Skuld Stealer via trusted platforms like GitHub and Discord, using phishing, multi-stage loaders, and evasion techniques. The campaign also bypasses Chrome's security and exfiltrates data through Discord webhooks.

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

- Check Point Research has released its May 2025 Malware Report, in which SafePay emerged as the most prevalent ransomware group, utilizing a double-extortion strategy to encrypt files while exfiltrating sensitive data. The group features an exclusion of machines that use Cyrillic-language keyboard, suggesting potential ties to Russian-affiliated actors, and has surpassed 200 victims, with nearly 20% of its targets in Germany.

- Check Point researchers highlight rising cyber threats in the travel industry due to its reliance on real-time data and global networks. Major incidents include a March 2025 DDoS attack on an air ticket consolidator and a January 2025 cloud breach exposing 112,000 records. Other threats involve phishing campaigns and third-party compromises targeting payment systems.