CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Grubhub, the US-based online food ordering and delivery platform, suffered a data breach due to unauthorized access through a compromised third-party service provider's account. The incident exposed personal details of customers, drivers, and merchants, including names, email addresses, phone numbers, payment card types, last four digits of card numbers, and hashed passwords for certain legacy systems. Grubhub has since revoked the service provider's access and launched an investigation into the incident.

- The city of McKinney, Texas, notified about a cyber-attack it experienced on October 31, 2024, which was detected on November 14. The breach exposed sensitive information, including names, addresses, Social Security numbers, driver's license numbers, credit card details, financial account data, and medical insurance information of approximately 17,751 residents. The city has notified affected individuals and is offering one year of identity protection services.

- Bohemia Interactive has reported severe disruptions to its online gaming services, affecting DayZ and Arma Reforger, due to a sustained DDoS attack. A group named 'styled squad reborn' has claimed responsibility for the attack, though its involvement remains unverified. Some reports suggest the attackers initially demanded a Bitcoin ransom to halt the attacks but later dismissed it as a joke.

- Yazoo Valley Electric Power Association, serving multiple counties in Mississippi, experienced a cyberattack in August 2024 that compromised the personal information of more than 20,000 residents. The breach was linked to the Akira ransomware group, which claimed to have stolen documents containing Social Security numbers and company financial records.

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

- The University of The Bahamas suffered a ransomware attack on February 2nd, which disrupted internet and telephone systems, affecting administrators, professors, and students. The incident impacted all online applications, including email platforms and systems used for classwork, leading to the cancellation of online classes. The university is collaborating with law enforcement to contain the incident and has urged students to change their passwords.

- British engineering company IMI has fallen victim to a cyber-attack which resulted in unauthorized access to its systems. Upon detection, the company engaged external cybersecurity experts to investigate and contain the incident. This event follows a similar cyber-attack reported by another UK-based engineering firm, Smiths Group, nine days earlier.

VULNERABILITIES AND PATCHES

- Trimble has disclosed that a deserialization vulnerability in its Cityworks software, identified as CVE-2025-0994 with a CVSS v4.0 score of 8.6, is being actively exploited. This flaw allows authenticated users to execute remote code on Microsoft Internet Information Services (IIS) servers, leading to unauthorized access and deployment of Cobalt Strike beacons. Cityworks is widely used by local governments and utilities for asset and work order management. Trimble advises users to update to version 15.8.9 or later to mitigate this risk.

- Cisco has published an advisory addressing two critical vulnerabilities in Cisco Identity Services Engine (ISE). The vulnerabilities, CVE-2025-20124 (CVSS 9.9) and CVE-2025-20125 (CVSS 9.1), allow remote attackers to gain escalation privilege and execute arbitrary commands on affected devices.

- A high-severity kernel flaw actively exploited in Android devices was patched by Google in its latest security update. This Linux kernel vulnerability, identified as CVE-2024-53104 (USB video-class driver code), potentially allows several types of attacks through a buffer overflow, triggered by parsing undefined video frames. The latest patch aims to mitigate this by skipping parsing of problematic frames.

THREAT INTELLIGENCE REPORTS

- Check Point Research has identified that threat actors are leveraging AI models like DeepSeek and Qwen to generate malicious content. These models have been manipulated to assist in developing infostealer malware, bypassing anti-fraud protections, and optimizing spam distribution techniques. Researchers observed cybercriminals using "jailbreaking" methods to override built-in security restrictions, allowing the creation of harmful tools.

- Check Point has reported a phishing campaign impersonating Facebook, falsely notifying recipients of copyright infringement. The emails, sent from Salesforce's automated mailing service, direct users to a fake Facebook support page to harvest credentials. The campaign began around December 20, 2024, primarily affecting enterprises across the EU (45.5%), US (45.0%), and Australia (9.5%), with versions in Chinese and Arabic, indicating a broad geographic target.

- Researchers have uncovered an ongoing cyber campaign where Russian threat actors are deploying SmokeLoader malware against Ukrainian government and private sector organizations. The attackers use phishing emails impersonating Ukrainian agencies and businesses, embedding malicious attachments that exploit vulnerabilities to deliver SmokeLoader. This malware, traditionally used for financially motivated attacks, is now being leveraged in cyber-espionage operations against Ukrainian critical infrastructure.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Trojan-Downloader.Win.Smokeloader, Trojan-Downloader.Win.Smokeloader.ta)