CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The International Civil Aviation Organization (ICAO), that is part of the UN, confirmed a compromise of its recruitment database that exposed 42,000 recruitment applications. The data contains records from April 2016 to July 2024 and includes recruitment-related information, such as names, email addresses, dates of birth, and employment history.

- Argentina’s airport security police (PSA) has been compromised with threat actors gaining access to its payroll systems. The attack occurred through a vulnerability in the systems of Banco Nación, which processes PSA’s payroll. The threat actors obtained personal and financial data of the agency’s officers and civilian personnel.

- Slovakia’s Office of Geodesy, Cartography and Land Registry (UGKK) has been compromised, affecting availability of the land ownership database. Media outlets report that UGKK fell victim to an undisclosed ransomware group.

- Spanish telecommunications company Telefónica was targeted by Hellcat Ransomware. The threat actors accessed Telefónica’s ticketing system and extracted 2,3 GB of documents, tickets data and internal files. The database was leaked on a hacking forum.

- Everest ransomware group has breached a popular cannabis vendor named STIIIZY through a 3rd party point-of-sale processing service. The compromise occurred between October 10, 2024, and November 10, 2024, and led to extraction of personal data and IDs of 422,075 customers.

- BayMark Health Services were compromised by RansomHub ransomware group, which also exfiltrated 1.5 TB of its data. The attack occurred between September 24, 2024, and October 14, 2024, providing the attackers access to personal identifiable information, such as Social Security numbers, dates of birth, insurance information and other details.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win.RansomHub; Ransomware.Wins.RansomHub.ta.)*

- Russian internet services provider (ISP) named Nodex was shut down by a Ukrainian hacktivist group Ukrainian Cyber Alliance. The attack has destroyed the company’s network, dropping global traffic from Nodex’s autonomous system AS29329 to zero.

- The Green Bay Packers' official online store suffered a security breach that resulted in the theft of payment card information from over 8,500 customers. Attackers injected malicious code into the checkout page between September and October 2024, capturing personal and payment details. Payments made via gift cards, PayPal, or Amazon Pay were not affected.

VULNERABILITIES AND PATCHES

- Mozilla has released version 134 of its Firefox browser, addressing 11 security vulnerabilities. Three of the patched vulnerabilities, CVE-2025-0242, CVE-2025-0244 and CVE-2025-0247 are considered of high severity as they allowed memory corruption or address bar spoofing.
- SonicWall has published an advisory addressing high severity authentication bypass vulnerability CVE-2024-53704 alongside three other medium security vulnerabilities. The company has been sending out emails urging customers to update the firmware due to high susceptibility of exploitation of the vulnerability.
- Mediatek has issued an advisory addressing 13 security vulnerabilities affecting the company's products. Among the vulnerabilities is the critical vulnerability CVE-2024-20154, which allows exploiting an out-of-bounds write to gain remote code execution.

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered Banshee, a macOS infostealer that mimics Apple's XProtect antivirus engine to evade detection. Operating as a Stealer-as-a-Service, Banshee has been distributed via phishing websites and malicious GitHub repositories, targeting macOS users to steal browser credentials, cryptocurrency wallets, and sensitive file data. Despite the operation's shutdown following a source code leak, threat actors continue to distribute the infostealer.
- Check Point Research has analyzed the FunkSec ransomware group, which emerged in late 2024 and claimed over 85 victims in December, surpassing other ransomware groups during that period. FunkSec appears to utilize AI-assisted malware development, enabling even inexperienced actors to produce and refine advanced tools rapidly. The group's activities blur the line between hacktivism and cybercrime, with some leaked datasets recycled from previous hacktivist campaigns, raising doubts about the authenticity of their disclosures.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Wins.Funksec.A)
- Check Point has identified a phishing campaign that has targeted 7,300 businesses and 40,000 individuals around the world, with the majority of targets in the US. The campaign uses compromised accounts of a travel agency Riya, delivering malware, and harvesting credentials.
- Researchers have identified that China-affiliated espionage groups are exploiting a newly disclosed vulnerability, CVE-2025-0282, in Ivanti's Connect Secure VPN appliances. Mandiant observed initial exploitation in mid-December by malware families such as SPAWN, previously associated with Chinese threat actors like UNC5221. The US Cybersecurity and Infrastructure Security Agency (CISA) has mandated federal agencies to patch this vulnerability by January 15, 2025, due to its active exploitation.