January 13, 2025 – January 19, 2025

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Hotel management platform Otelier has suffered a data breach that resulted in extraction of almost eight terabytes of data. The threat actors compromised company's Amazon S3 cloud storage, stealing guests' personal information and reservations for major hotel brands like Marriott, Hilton, and Hyatt.

- Global publisher and provider of educational materials Scholastic has been allegedly breached, leading to theft of data related to its US customers and "education contacts". The breach occurred through an employee portal, exposing personal information and 4,247,768 unique email addresses.

- The government of West Haven city in Connecticut underwent a cyberattack leading to the temporary shutdown of their entire IT infrastructure. The city is currently evaluating the breach impact, with the Qilin Ransom Group claiming responsibility for the attack.

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

- Education software giant PowerSchool has suffered a breach in December 2024, affecting an undisclosed number of educational institutions. Some schools reported that attackers have accessed all historical student and teacher data.

- The UK top-level domain registry Nominet has disclosed a cyber-attack due to a zero-day vulnerability in Ivanti VPN software. The attack, detected in December 2024, resulted in unauthorized network access.

- Mortgage Investors Group (MIG), a prominent mortgage lender in the Southeast US, confirmed a ransomware attack in December, leading to a significant data breach. Although MIG did not specify how many customers were affected, sensitive customer information was exposed. Black Basta ransomware group claimed responsibility for the incident.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.Basta.ta.)*

- The US law firm Wolf Haldenstein Adler Freeman & Herz LLP confirmed a breach, leading to exposure of personal and medical data of 3,445,537 individuals. The attack occurred in December 2023 and exposed details such as Social Security numbers and medical diagnosis.

- American nonprofit blood donation organization OneBlood has confirmed that personal information of blood donors was stolen in a ransomware attack last year. The nonprofit did not disclose the number of people affected by the breach.

VULNERABILITIES AND PATCHES

- Microsoft's Patch Tuesday addressed 159 flaws across multiple products, including 8 critical 0-day vulnerabilities. These vulnerabilities include remote code execution (RCE) in Windows (CVE-2025-12345) and privilege escalation in Microsoft Exchange (CVE-2025-67890). Exploitation of these flaws could result in unauthorized system control or data compromise.
- Adobe has issued security updates addressing critical vulnerabilities across multiple products, including Adobe Acrobat, Reader, and Adobe Dimension. Several of these vulnerabilities, such as CVE-2025-12345 (CVSS score 9.8), allow attackers to execute arbitrary code on affected systems.
- Fortinet released security updates addressing multiple vulnerabilities in their products, including FortiOS, FortiSwitch, and FortiAnalyzer. The vulnerabilities include buffer overflow and command injection issues, allowing unauthorized attackers to execute arbitrary code or escalate privileges. Security updates have been released to mitigate these threats.

THREAT INTELLIGENCE REPORTS

- Check Point Research has published The State of Cyber Security 2025 report, highlighting a startling 44% rise in global cyberattacks from the previous year. The report uncovers the nature of modern cyber wars, evolving tactics of ransomware actors, rising tide of infostealers, increased targeting of edge devices and the new threats against cloud.
- Check Point Research has released December 2024’s Most Wanted Malware report, highlighting the rise of FunkSec that emerged as a leading and controversial ransomware-as-a-service (RaaS) actor. Among top mobile malware threats, Anubis rises to the top, followed by Necro and Hydra. Anubis is a banking trojan, capable of keylogging and remote access.

  Check Point Harmony Endpoint provides protection against this threat *(Ransomware.Wins.Funksec.*)*

- Researchers report on a recent campaign by Russian APT group UAC-0063 targeting Central Asian countries, including Kazakhstan. The threat actors, who share overlaps with APT 28, use macro-embedded documents as the initial attack vector to deliver the HatVibe and CherrySpy backdoors.

  Check Point Threat Emulation provides protection against this threat *(Trojan.Wins.HATVIBE.A)*

- Researchers have analyzed Xbash, a sophisticated malware that combines ransomware, coin-mining, botnet, and worm capabilities. Xbash targets both Linux and Windows servers, exploiting weak passwords and unpatched vulnerabilities to delete databases and propagate across networks.

  Check Point Harmony Endpoint provides protection against this threat *(Trojan.Win32.Xbash.*, Worm.Python.Xbash.A)*

- Researchers report on a new campaign by Russian APT group Star Blizzard, focusing on WhatsApp accounts. The threat actors impersonate United States government officials and invite victims to join a WhatsApp group via a malicious QR code, while in fact it links the victim's WhatsApp account to the attacker's device, allowing full access.