CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

April 14 - 20, 2025

TOP ATTACKS AND BREACHES

- Retail giant Ahold Delhaize has suffered a cyber-attack resulting in data theft of customer information from its US business systems. The attack, claimed by ransomware group INC Ransom, impacted Ahold Delhaize USA brands and services including e-commerce operations and pharmacies.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.INC)

- Car rental giant Hertz has been a victim of a cyber-attack which resulted in a leakage of customer data due to zero-day vulnerability in a Cleo file share tool. The compromised data includes names, contact information, birth dates, credit card and driver's license information, and for a few individuals, Social Security numbers, passport data, and medical claim details.

- Insurance firm Lemonade revealed a data breach exposing thousands of driver's license numbers due to a vulnerability in its online car insurance application process. The incident, which started in April 2024, lasted for approximately 17 months. It remains unclear whether additional personal data beyond driver's license numbers was compromised during the breach.

- American Kidney dialysis company DaVita has confirmed a ransomware attack. The attack has affected the functionality of its systems, potentially compromising care for its 281,100 patients across 3,166 outpatient dialysis centers worldwide.

- Forum platform 4Chan was breached and subsequently taken offline. The attackers claim to have exfiltrated and leaked the platform's entire source code, along with personal information of users and moderators. A rival forum, Soyjak, has claimed responsibility for the attack.

- American business services company Conduent was hit by a cyber-attack in January 2025 that resulted in the theft of client data. The stolen files contain personal information associated with the clients' end-users, impacting customers across the US including local government agencies. No threat actor has been identified or claimed responsibility for the attack.

- Western Sydney University has experienced a cyber-attack which resulted in the unauthorized access of demographic, enrollment, and academic progression data belonging to approximately 10,000 current and former students. The incident occurred via a compromise of the university's single sign-on system between January and February 2025. The WSU's press release also noted a separate leak which was discovered on the dark web in March 2025, originally posted in November 2024.

- Entertainment services company Legends International has confirmed a cyber-attack that occurred in November 2024, resulting in unauthorized access to its IT systems and the exfiltration of personal data files. The types of the exposed data have not been determined and the scope of the breach including the number of affected individuals remains unknown.

VULNERABILITIES AND PATCHES

- Check Point Research reports on campaigns exploiting CVE-2025-24054, a vulnerability which allows NTLM hash disclosure via spoofing. One of the campaigns targeted government and private entities in Poland and Romania, by delivering a malicious archive via a Dropbox link.

  Check Point Threat Emulation provides protection against this threat.

- Apple has released urgent out-of-band updates in iOS 18.4.1 to address two critical security flaws. The first flaw (CVE-2025-31200) is a weakness in CoreAudio that can result in code execution if a maliciously crafted media file is processed. The second flaw (CVE-2025-31201) is a vulnerability that could allow an attacker to bypass Pointer Authentication.

- Oracle has released its April 2025 critical update, addressing 378 flaws, including nearly 180 unique CVEs. Among them, 255 vulnerabilities are remotely exploitable without authentication, with around 40 classified as critical. Oracle Communications was the most affected product with 103 fixes.

THREAT INTELLIGENCE REPORTS

- Check Point Research analyzed a phishing campaign by Russia affiliated APT29 targeting European diplomatic entities. The campaign impersonates a major European Ministry of Foreign Affairs, distributing fake invitations to wine tasting events that lead to the deployment of a new loader, GRAPELOADER. The loader serves as an initial-stage tool for fingerprinting, persistence, and payload delivery, and is followed by a new variant of the modular backdoor WINELOADER.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Trojan.WIN64.WINELOADER.*; APT.Wins.WineLoader.*)*

- Check Point Research reports an increase in global cyber threats in Q1 2025, with a 47% surge in average weekly cyber-attacks per organization from the same period last year. The most targeted sectors were education, followed by government and telecommunication sectors, while North America accounted for 62% of total ransomware attacks globally.

- Check Point Research unveiled a novel process injection method called 'Waiting Thread Hijacking' (WTH), which leverages thread pools to execute malicious code without triggering security alerts. By avoiding APIs like SuspendThread, ResumeThread, and SetThreadContext, WTH manipulates the return address on stack of waiting threads, redirecting execution to attacker-controlled code.

  Check Point Harmony Endpoint provides protection against this threat (WaitingThreadHijackBlock)

- Researchers found that ransomware group CrazyHunter is targeting Taiwan’s critical infrastructure using advanced evasion techniques like Bring Your Own Vulnerable Driver (BYOVD). About 80% of its toolkit now consists of open-source GitHub tools like Prince Ransomware Builder and ZammoCide.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win.Prince; Ransomware.Wins.Prince.ta.*)*