October 14 - 20, 2024

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Boston Children's Health Physicians, part of the Boston Children's Hospital network, suffered a data breach in September, exposing sensitive patient information, including Social Security numbers, medical records, and health insurance details. The breach was discovered after unusual activity was detected on September 6, leading to system shutdowns by September 10. The BianLian ransomware group, responsible for previous high-profile attacks, claimed responsibility for the breach.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Wins.BianLian, Ransomware.Wins.BianLian.ta)*

- Insurance giant Globe Life is facing extortion attempts after hackers stole data on over 5,000 individuals from its subsidiary, American Income Life Insurance Company. The stolen information includes Social Security numbers, names, addresses, and health-related data. The threat actors, who did not use ransomware or disrupt operations, have shared some of the stolen data with short sellers and plaintiffs' attorneys while claiming to possess additional unverified information.

- Japan's ruling Liberal Democratic Party (LDP) experienced a distributed denial-of-service (DDoS) cyberattack on its website, disrupting operations at the start of the country's general election campaign. Pro-Russian hacker groups, including NoName057(16) and the Cyber Army of Russia, claimed responsibility, citing Japan's upcoming joint military exercise with the U.S. as motivation. Other government and local websites were also affected.

- Nidec Corporation, a Japanese tech giant, confirmed a data breach following a ransomware attack earlier this year, with stolen data leaked on the dark web after refusing to meet the attackers' extortion demands. The breach targeted Nidec's Precision division in Vietnam, where attackers accessed servers using stolen VPN credentials, stealing over 50,000 files, including internal documents, contracts, and business partner communications. The 8BASE ransomware gang initially claimed responsibility, followed by the Everest group.

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

- Game Freak, the developer behind the Pokémon series, disclosed a cyberattack that occurred in August 2024, resulting in the leak of source code and game designs for unpublished titles, as well as personal information of employees, contractors, and former business associates. Game Freak has assured that players' data was not affected.

- Decentralized finance platform Radiant Capital has reported the theft of over $50 million in cryptocurrency following a sophisticated attack that compromised the devices of three trusted developers. Hackers gained access to multiple private keys, enabling them to drain user funds by executing malicious transactions without obvious warning signs.

VULNERABILITIES AND PATCHES

- Google has shared a security update for its Chrome browser, addressing 17 security vulnerabilities. Among the vulnerabilities is CVE-2024-9954, a high severity use-after-free vulnerability that allowed remote attackers to exploit heap corruption.
- Oracle has released its October patch update; the update included a total of 334 security updates, with fixes for 35 Critical vulnerabilities. The majority of fixes target Oracle Commerce and Oracle Hyperion.
- A new macOS vulnerability known as "HM Surf" (CVE-2024-44133) allows attackers to bypass the Transparency, Consent, and Control (TCC) technology in macOS. Successful exploitation of the flaw could lead to unauthorized access to a user's data, including browsing history, camera, microphone, and location. Apple released a fix for this vulnerability in the Sequoia update on September 16th.
- WordPress plugin Jetpack has released a critical security update, addressing a vulnerability in the Contact Form feature. The vulnerability allowed any logged user on a site to read contact forms submitted by other users.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports that in Q3 2024, global cyberattacks surged by 75% compared to the same period in 2023, with an average of 1,876 attacks per organization. The Education/Research sector was the most targeted, while Africa faced the highest attack rates regionally. Ransomware incidents remained persistent, with North America experiencing 57% of the attacks. The Manufacturing and Healthcare sectors were particularly impacted by ransomware.
- Check Point Research has analyzed phishing trends for Q3 2024, revealing that Microsoft was the most imitated brand, responsible for 61% of phishing attempts, followed by Apple (12%) and Google (7%). Notably, Alibaba entered the top 10 for the first time, ranking seventh, and Adobe reappeared in the rankings. The most targeted industries were Technology, Social Networks, and Banking.
- Researchers have uncovered that North Korean IT workers, who infiltrate Western companies by using fake identities, are now extorting their former employers by stealing sensitive data and demanding ransom. These workers, often hired as contractors, leverage tools like VPNs and remote desktop applications to mask their locations. After their employment is terminated, they send extortion emails threatening to leak the stolen data unless paid in cryptocurrency.
- Researchers have identified a new wave of attacks by the Russian-speaking group UAT-5647, targeting Ukrainian government entities and some Polish organizations using updated variants of RomCom malware. The threat actor’s goal appears to be both data exfiltration and potential ransomware deployment, indicating a dual focus on espionage and financial gain.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Backdoor.Wins.Romcom, Backdoor.Win.Romcom, Trojan.Win.RomCom.la, Trojan.Wins.RomCom)