Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Nevada-based medical transcription company, Perry Johnson & Associates (PJ&A), has disclosed a data breach that affected more than 9M patients at multiple healthcare providers in the US. The exposed data includes patients' names, addresses, dates of birth, Social Security Numbers, and medical records. The attack is considered as one of the most severe medical data breaches in recent years.

- The British Library, one of the largest libraries in the world, suffered a ransomware attack that resulted in the exposure of internal human resources data. Rhysida ransomware gang has claimed responsibility, setting a starting price of 20 bitcoins (approximately $750K) as a ransom with seven days deadline.

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

- A cyberattack on Vanderbilt University Medical Center (VUMC), which operates seven hospitals and numerous healthcare facilities across Nashville, Tennessee, has resulted in a data breach. Meow ransomware gang has claimed responsibility for the attack.

- A sophisticated cyberattack on CTS, a UK-based managed service provider (MSP), has disrupted services for hundreds of law firms. The attack blocked access of hundreds of British law firms from their case management systems, causing delays in legal proceedings and disrupting communication between clients and lawyers. CTS is working to restore services, but no timeline has been given.

- Ransomware group AlphV/BlackCat has assumed responsibility for the cyber-attack on the American real estate insurance giant Fidelity National Financial (FNF), a Fortune 500 company, resulting in the shutdown of its network.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.BlackCat, Ransomware_Linux_BlackCat, Ransomware_Linux_BlackCat)

- The Idaho National Laboratory (INL), a US-based nuclear research center, has confirmed a data breach that resulted in the exposure of internal human resources data. Hacktivists group SiegedSec took responsibility for the attack, claiming to have stolen the personal information of hundreds of thousands of employees, users, and citizens. The allegedly leaked data includes full names, dates of birth, email addresses, phone numbers, Social Security Numbers, addresses and employment info.

VULNERABILITIES AND PATCHES

- Sucuri has released its WordPress Vulnerability & Patch Roundup November 2023. Among the vulnerabilities is the high-severity Elementor Website Builder Stored Cross-Site Scripting flaw (CVE-2023-47505), nine additional medium-severity flaws including WooCommerce Checkout Manager Missing Authorization flaw (CVE-2023-47681), and other low-severity flaws.
- The open-source file-sharing software ownCloud has warned of three critical security vulnerabilities, including a flaw in containerized deployments for certain graphapi versions, a WebDAV Api Authentication Bypass using Pre-Signed URLs affecting core versions, and a Subdomain Validation Bypass in oauth2. These flaws could be exploited to expose confidential data and manipulate files.
- Mozilla has released security patches for Firefox and Thunderbird, which address multiple high severity vulnerabilities. Some of the vulnerabilities potentially allowed remote code execution if exploited.

THREAT INTELLIGENCE REPORTS

- Check Point Research provides a case study of some of the most recent ransomware attacks targeting Linux systems and ESXi systems, which have been increasing over the last few years. The study, encompassing 12 prominent ransomware families, investigates the motivations behind developing ransomware for Linux and reveals that many Linux-targeting families heavily utilize the OpenSSL library along with ChaCha20/RSA and AES/RSA algorithms.
- Check Point Research shares insights from their active tracking of the evolution of SysJoker, a previously publicly unattributed multi-platform backdoor, which we asses was utilized by a Hamas-affiliated APT to target Israel. Notably, the tool went through prominent changes including the shift to Rust language and a move to using OneDrive instead of Google Drive to store dynamic C2 URLs.

  Check Point Harmony Endpoint, Threat Emulation and Anti-Bot provide protection against this threat
  (Backdoor.Wins.Sysjoker.ta, Backdoor_Linux_SysJoker, Backdoor.Win.SysJoker, Backdoor.WIN32.SysJoker)
- Check Point Research, using Threat Intel Blockchain system, uncovered an ongoing sophisticated Rug Pull scheme that managed to pilfer nearly $1M. The actor behind this scheme was traced, unveiling the perpetrator lured unsuspecting victims into investing using the crowd's hype around ill-gotten gains.
- CISA has published a #StopRansomware report on LockBit 3.0 ransomware operation. The report is based, among others, on information shared by Boeing, which had been affected by the group recently.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.Lockbit; Gen.Win.Crypter.Lockbit; Ransomware.Wins.LockBit.ta; Ransomware_Linux_Lockbit)