Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Decentralized multi-chain crypto wallet BitKeep announced it has been a victim of an attack that resulted in the theft of over $9M worth of digital currencies from its customers. Threat actors were able to distribute tainted versions of the company's Android app that were designed to steal users' digital assets.

- Lake Charles Memorial Health System in the US has been a victim of a ransomware attack, conducted by Hive ransomware group. The threat actors leaked personal data belonging to almost 270K patients and employees, including names, home addresses, medical records, health insurance information, Social Security numbers, payment information and more.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Win.Hive)*

- The city of Mount Vernon, Ohio, has been a victim of a ransomware attack, conducted by LockBit ransomware group. The threat actors breached the city's police department, municipal court and other government offices through a remote access tool utilized by the city's IT provider. The city's statement claims no documents with personal information were accessed from the city systems.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(Ransomware.Win.Lockbit)*

- The website of the Port of Lisbon Administration (APL), the third-largest port in Portugal, has been a victim of a ransomware attack, conducted by LockBit ransomware group. The threat actors claim to have access to financial reports, audits, budgets, contracts, personal data of customers, and more. The company's statement confirms there was no impact on the port's operations.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(Ransomware.Win.Lockbit)*

- The Canadian Copper Mountain Mining Corporation has been a victim of a ransomware attack that disrupted its IT systems. While the source of the attack is being investigated, researchers found employee credentials offered for sale on a hackers' marketplace, which implies a compromised account might have been used to gain a foothold in the company's network.

- Alessandria hospital in Italy has been a victim of a ransomware attack, allegedly conducted by the RagnarLocker group. The threat actors claim to have 37GB of leaked data consisting of hundreds of thousands of patients' personal information, including medical IDs, financial and departmental records.

- Bitcoin mining pool BTC.com announced it has been a victim of a cyberattack that resulted in the theft of approximately $3M worth of crypto assets, owned by its parent firm, BIT Mining Limited.

VULNERABILITIES AND PATCHES

- Nintendo has patched the ENLBufferPwn vulnerability (tracked as CVE-2022-47949) that takes advantage of a buffer overflow in the C++ class NetworkBuffer that is included in the enl or Net network library. Successful exploitation, by simply playing online with the victim, might result in a remote code execution on compromised Switch, 3DS, and Wii consoles.
- Netgear has released security update for a high-severity vulnerability affecting multiple WiFi router models. Successful exploitation might result in a denial of service or a remote code execution on impacted routers.

THREAT INTELLIGENCE REPORTS

- Researchers have discovered a previously unknown Linux malware that exploits 30 vulnerabilities in multiple outdated WordPress plugins and themes to inject malicious JavaScripts into websites based on a WordPress CMS (Content Management System). The malware targets both 32-bit and 64-bit Linux systems, giving its operator remote command capabilities.

  Check Point Harmony Endpoint provides protection against this threat *(Backdoor_Linux_WordPressExploit_B)*

- A new malvertising campaign has been observed, abusing Google Ads to mislead users to click on malicious phishing web pages. Threat actors use typosquatting technique to target organizations and individuals, then use Trojanized variants that deploy malware such as Raccoon Stealer and Vidar.

  Check Point Threat Emulation, Harmony Endpoint and Anti-Bot provide protection against this threat *(InfoStealer.Win.Raccoon; Banker.Win.Vidar)*

- Researchers have revealed "EarSpy", a new type of attack on Android devices which provides access to private data including audio conversations, indoor locations and touchscreen inputs, through smartphones' built-in motion sensors.
- Researchers encountered spam campaigns targeting Italian users with PureLogs Stealer, a malicious .NET program offered for sale with an annual subscription. PureLogs is designed to steal browser data, crypto wallets, and various applications such as FTP Clients, email clients, and VPNs installed on a system.
- BlueNoroff group, a financially motivated threat actor, has been analyzed by researchers. The group uses new methods of malware delivery, such as creating numerous fake domains impersonating venture capital companies and banks.