September 18 – 24, 2023

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Monti ransomware gang has claimed responsibility for a cyber-attack on New Zealand's third-largest university, Auckland University of Technology. The threat actors claim to have stolen 60GB of data, giving the victim a deadline of October 9th to pay a ransom.

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

- The California-based Software firm Retool has disclosed a data breach that affected 27 clients of the company's cloud platform. The threat actors behind the attack have gained unauthorized access to the clients' accounts by performing SMS-based social engineering attack, which caused a damage of $15M in stolen cryptocurrency for at least one client. Recently introduced Google Authenticator sync feature has been blamed by the company for the breach, as it silently switched from multi-factor authentication (MFA) to alleged single-factor authentication.

- The International Criminal Court has been a victim of a cyber-attack affecting its information systems. The ICC has not provided information as to what information may have been taken, and no threat actor has claimed responsibility for the attack yet.

- Greater Manchester Police, one of the largest police departments in the UK, has confirmed a data breach that occurred as a result of a suspected ransomware attack on a third-party identity cards supplier Digital ID. The personal information of approximately 20K police officers has been exfiltrated, however no financial data is believed to be affected.

- The American household cleaning product maker Clorox has suffered a cyber-attack and has shut down its system as a precaution. The attack has resulted in a wide scale disruption to its operations, including product outages and delays.

- Threat actors have obtained limited access to the Canadian airline Air Canada's internal network, which has affected personal information of its employees. According to the company, clients' information was not impacted in the attack.

- The government of Nova Scotia has confirmed a data breach that has affected personal information of more than 165K citizens. Most of the data, which was stolen due to the MOVEit file transfer system vulnerability that was utilized by Cl0p gang, consists of sensitive information such as social insurance numbers and banking information.

VULNERABILITIES AND PATCHES

- Apple has addressed three patches for vulnerabilities (CVE-2023-41991, CVE-2023-41992 and CVE-2023-41993) in Apple's security framework, Apple's kernel framework and Apple's WebKit web browser engine, which impact various versions of Apple products. Among others affected, the first two flaws impact the Apple Watch Series 4 and later, and the third impacts macOS Monterey.
- GitLab has fixed a high severity vulnerability (CVE-2023-5009), affecting various versions of GitLab EE starting from 13.12 to 16.2.7, and 16.3 to 16.3.4. This flaw allows an attacker to execute pipelines as an arbitrary user through the misuse of scheduled security scan policies.
- Atlassian has released its September 2023 Security Bulletin, which includes patches for several vulnerabilities (CVE-2022-25647, CVE-2023-22512, CVE-2023-22513, and CVE-2023-28709). A malicious cyber actor could exploit some of these vulnerabilities to take control of an affected system.

THREAT INTELLIGENCE REPORTS

- Check Point Research has discovered new version of the BBTok banking malware, which targets clients of over 40 Mexican and Brazilian banks. The research highlights newly discovered infection chains that use a unique combination of Living off the Land Binaries (LOLBins), which results in low detection rates. The research also reveals some of the threat actor's server-side resources used in the attacks, targeting hundreds of users in Brazil and Mexico.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Banker.Wins.BBTok; Banker.Win.BBTok; Technique.Wins.SuxXll; Trojan.Win.XllAddings)

- Check Point Research has exposed threat actor going by the moniker "EMINэM", which is responsible for selling and promoting dual use agents Remcos and GuLoader. The research shows the strong links identified between those agents, and proves that the sellers of Remcos and GuLoader are clearly aware that their tools are embraced by cybercriminals.

  Check Point Threat Emulation provides protection against this threat (Dropper.Win.CloudEyE; Dropper.Win.Guloader; RAT.Win.Remcos)

- The China-based threat actor Earth Lusca's (aka CHROMIUM) employs a Linux-based backdoor variant dubbed SprySOCKS, originating from the open-source Windows backdoor Trochilus. In addition, the implementation of SprySOCKS interactive shell is likely inspired from the Linux variant of the Derusbi malware.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Trojan.Wins.Derusbi; Trojan.Win.Winnti; RAT.Wins.Shadowpad)