Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- US unit of China's largest bank, the Industrial and Commercial Bank of China (ICBC), has suffered a ransomware attack that disrupted some of its financial services systems, reportedly affecting liquidity in US Treasuries. LockBit ransomware gang is reportedly behind the attack.

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

- OpenAI has been a victim of an ongoing distributed denial-of-service (DDoS) attack that has resulted in periodic outages that affected its API and ChatGPT services. Hacktivists group Anonymous Sudan, which is affiliated to Russia, claimed responsibility for the attack that they conducted due to alleged biasness towards Israel and against Palestine.

- DP World Australia suspended since Friday its operations at four major Australian ports due to serious and ongoing cyber incident. DP World Australia, which manages almost half of the goods that are imported and exported into the country, said it was looking into the incident.

- Maine state agencies were hit by a cyber-attack leading to data theft by the Cl0p ransomware gang, exploiting a vulnerability in the widely used MOVEit file transfer tool. The attack has impacted approximately 1.3M individuals' private data, including full names, state IDs, Social Security numbers (SSN), dates of birth, and drivers' license numbers, as well as medical information and health insurance information.

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

- The non-profit US organization McLaren Health Care has disclosed a data breach that affected sensitive personal information of 2.2M patients. ALPHV/BlackCat ransomware gang claimed responsibility for the attack, which resulted in the exposure of full names, dates of birth, Social Security numbers (SSN), health insurance information and other medical information.

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

- The US mortgage services giant, Mr. Cooper, has been a victim of a cyber-attack that disrupted loan payments and other transactions for millions of customers. The company is still investigating the nature of the compromised data.

VULNERABILITIES AND PATCHES

- Check Point Research reveals a technique abusing Microsoft Access's feature (Part of the Office suite) that might allow attackers to bypass Firewall rules designed to stop NTLM credential theft. Attacks against NTLM vary between brute force attacks, Man in the Middle and "pass-the-hash" scenarios, all aimed at stealing personal information and impersonating identities. CPR responsibly disclosed the information to Microsoft.

  Check Point IPS provides protection against this threat *(Microsoft Windows NTLM Information Disclosure)*

- Veeam ONE has released patches for two critical and two medium severity vulnerabilities (CVE-2023-38547, CVE-2023-38548, CVE-2023-38549, CVE-2023-41723) in its IT monitoring platform. The vulnerabilities could allow threat actors to gain Remote Code Execution capabilities on SQL database configuration servers, and NLTM hashed credentials from vulnerable servers.

- QNAP has published advisories for two critical severity command injection vulnerabilities (CVE-2023-23368, CVE-2023-23369). The flaws in the compromised QTS operating system and applications can be exploited by a remote attacker to execute commands via a network.

THREAT INTELLIGENCE REPORTS

- Check Point Research has published its monthly malware report for October 2023 indicating that NJRat, which is known to target government agencies and organizations in the Middle East, went up to second place as most prominent malware. Meanwhile, a new mal-spam campaign has been observed involving AgentTesla, and Education remained the most targeted industry. In addition, Zyxel ZyWALL Command Injection flaw (CVE-2023-28771) was the most exploited vulnerability, impacting 42% of organizations globally.

  Check Point IPS, Harmony Endpoint and Threat Emulation provide protection against this threat *(Zyxel ZyWALL Command Injection (CVE-2023-28771); Rat.Win.Njrat; Infostealer.Win.Agenttesla; Trojan-Downloader.Win.Agenttesla; Trojan.Win.Agenttesla)*

- The threat group FIN11 exploited a zero-day vulnerability in SysAid, a comprehensive IT Service Management, to gain access to corporate servers and deploy Clop ransomware. As a result, they were able to upload a webshell to the SysAid Tomcat web service's webroot.

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

- In the past month, hackers have targeted multiple healthcare organizations in the U.S. by abusing the ScreenConnect remote access tool. They also took steps to prepare for additional attacks on multiple healthcare organizations, including installing additional remote access tools for persistent access.