TOP ATTACKS AND BREACHES

- The LockBit ransomware group has recently claimed responsibility for hacking the Taiwan Semiconductor Manufacturing Company (TSMC), the largest contract chip manufacturer globally, serving tech giants such as Apple and Qualcomm. TSMC denied it was breached by Lockbit, but confirmed that the group has breached one of the company's IT hardware suppliers, Kinmax Technology. The demanded ransom was of $70 Million, one of the largest known ransom demands in the history.

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

- The Cl0p ransomware continues updating its Dark Web leak site, adding several new victims which were affected by the MOVEit attack. Among these victims are European manufacturers Schneider Electric and Siemens Energy, as well as the American university UCLA.

  Check Point IPS blade, Harmony Endpoint and Threat Emulation provide protection against this threat *((Progress MOVEit Transfer Multiple Vulnerabilities); Webshell.Win.Moveit, Ransomware.Win.Clop, Ransomware_Linux_Clop; Exploit.Wins.MOVEit)*

- Analysts have recently uncovered a new infection vector for ALPHV (BlackCat) ransomware. They observed advertisements promoting fraudulent pages on both Google and Bing search engines. The attack included a cloned webpage of WinSCP, an open-source Windows application for file transfer.

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

- A surge in credential-stealing attacks has been identified by Microsoft, attributed to the Russian nation state group Midnight Blizzard, previously known as Nobelium. These intrusions, utilizing residential proxy services to mask the origin IP address, specifically target government entities, IT service providers, non-governmental organizations (NGOs), defense organizations, and critical manufacturing sectors.

  Check Point IPS blade and Threat Emulation provide protection against this threat *(Roundcube Webmail Command Injection (CVE-2020-12641), Roundcube Webmail Cross-Site Scripting (CVE-2020-35730); APT.Wins.Nobelium)*

- Researchers have discovered a new campaign by Andariel, a group associated with the North Korean APT Lazarus. This campaign exploits a Log4j vulnerability to gain initial access, enabling the downloading of a suite of RAT and Backdoor tools.

  Check Point IPS blade, Harmony Endpoint and Threat Emulation provide protection against this threat *(Apache Log4j Remote Code Execution (CVE-2021-44228); APT.Win.Lazarus; APT.Wins.Lazarus)*

VULNERABILITIES AND PATCHES

- Hackers are actively exploiting an unpatched vulnerability (CVE-2023-3460; CVSS score: 9.8) present in all versions of the Ultimate Member plugin, which is utilized by over 200,000 WordPress sites. Their goal is to covertly generate admin accounts.
- Researchers have analyzed CVE-2023-20864, a critical remote code execution vulnerability in VMware Aria Operations for Logs (formerly vRealize), which has been recently patched.

  Check Point IPS blade provides protection against these threats *(VMware Aria Operations for Logs Insecure Deserialization (CVE-2023-20864))*
- The U.S. government has issued a warning regarding a critical vulnerability (CVE-2023-31222) in Medtronic's heart monitor data management system, specifically in the Paceart Messaging Service component within Paceart Optima. Exploiting this flaw could lead to remote code execution or denial-of-service (DoS) attacks. Patches are readily available for this vulnerability.

THREAT INTELLIGENCE REPORTS

- Check Point Research examines security and safety aspects of GPT-4 and reveals how its limitations can be bypassed. Researchers present a new mechanism dubbed “double bind bypass”, colliding GPT-4s internal motivations against itself.
- Check Point Research identified a malicious modified version of the popular messaging application Telegram. The malicious application installs Triada Trojan which can sign up the victim for various paid subscriptions, perform in-app purchases and steal login credentials.
- Researchers have conducted a comprehensive analysis of the operations conducted by Rhysida ransomware. The blog post not only provides technical insights into the malware payloads but also delves into the group's disclosure of files stolen from the Chilean Army and sheds light on the activities and techniques employed by the Rhysida ransomware group.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat.
- Security researchers have discovered a new command and control framework operated by the Iranian state-sponsored group called MuddyWater. The framework is named PhonyC2 and was allegedly used in the attack on the Technion Institute. They claim that the command and control framework is custom-made, continuously in development, and has been used by the MuddyWater group since at least 2021.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(APT.Win.MuddyWater; APT.Wins.MuddyWater)*