TOP ATTACKS AND BREACHES

- The Italian municipality of Palermo has been victim of a ransomware attack that caused a large-scale service outage affecting over a million people. The attack was claimed by the Vice Society ransomware group, which used the double extortion ransomware tactic.

- Shields Health Care Group, Massachusetts-based medical services provider, has been a victim of a data breach that happened during March. The stolen data included personal information such as social security numbers, home addresses and billing information. The attack affects over two million people and more than 50 health care facilities and considered one of the largest cyber attacks on healthcare providers in the US this year.

- US federal agencies have revealed that Chinese state-sponsored cyber actors have been targeting major telecommunications companies and network service providers since at least 2020. The Chinese hacking groups have exploited publicly known vulnerabilities to steal credentials and harvest data.

- The Chinese-speaking APT group, Aoqin Dragon, has been linked to an espionage campaign targeting Southeast Asia and Australia. Aoqin Dragon seeks initial access primarily through document exploits and the use of fake removable devices. Other techniques include DLL hijacking, Themida-packed files, and DNS tunneling to evade post-compromise detection. The group has been performing these cyber-espionage campaigns since 2013.

  Check Point Threat Emulation provides protection against this threat (Trojan.Win32.Aoqin Dragon)

- Two online gun shops in the US, Rainier Arms and Numrich Gun Parts, have been victim of data breaches caused by credit card skimmer infections on their websites. Data of approximately 90k customers was compromised.

- The Iranian Lyceum APT group (aka Hexane, Spilrin) has utilized a newly developed .NET based DNS backdoor to perform attacks on companies in the energy and telecommunication sectors.

  Check Point Threat Emulation and Anti-Bot provide protection against this threat (Trojan.Win32.Lyceum)

- Researchers have revealed a major phishing scam targeting Facebook users through the company's Messenger app, in which 1M credentials were stolen in 4 months. The campaign peaked in April-May 2022 but has been active since at least September 2021.

VULNERABILITIES AND PATCHES

- A 0day vulnerability, "DogWalk", affects the same Windows Microsoft Support Diagnostic Tool as Follina, has been reported. This is a path traversal flaw allowing copying an executable to the Windows Startup folder when the target opens a maliciously crafted .diagcab file received via email or web download.

  Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat *(Microsoft Support Diagnostic Tool Remote Code Execution (CVE-2022-30190); Exploit.Win.Follina*)*

- Researchers have discovered a new flaw in Apple M1 CPUs, which enables attackers to execute arbitrary code on Mac systems using a new hardware attack named PACMAN.

- Google has released 41 Android updates in devices running OS versions 10, 11, and 12. Five critical flaws (tracked as CVE-2022-20127, CVE-2022-20130, CVE-2022-20140, CVE-2022-20145, and CVE-2022-20210) could lead to remote code execution on vulnerable devices.

THREAT INTELLIGENCE REPORTS

- Check Point Research identified attacks leveraging the newly published remote code execution vulnerability affecting Atlassian Confluence Server and Data Center instances (CVE-2022-26134) to run crypto miners. Ransomware gangs are also exploiting this flaw for initial access to corporate networks.

  Check Point IPS provides protection against this threat *(Atlassian Confluence Remote Code Execution (CVE-2022-26134)*

- Check Point Research has published its list of most prevalent malware seen during May 2022, which puts Snake keylogger back on the list, in eighth place, following email campaigns delivering malware via PDF files. Emotet still leads the chart as a result of multiple widespread campaigns.

- Researchers have found that the Cuba ransomware group uses a new malware variant that optimizes its execution, minimizes unintended system behavior, and provides technical support to the ransomware victims. The new variant might pose risk for targeted organizations located in the US.

  Check Point Threat Emulation, Anti-Virus and Anti-Bot provides protection against this threat *(Trojan-Ransom.Win32.Cuba.a)*

- New Emotet Variant is stealing Google Chrome user profiles' credit card information.

- Researchers have revealed a new Black Basta ransomware variant targeting VMware ESXi servers running on enterprise Linux servers. The new variant uses the ChaCha20 algorithm to encrypt files, and multithreading for encryption to utilize multiple processors and make itself faster and harder to detect.

- SSNDOB, an online marketplace that sold personal information of approximately 24 million US people, has been taken down by several international law enforcement agencies.