Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Australian Federal Police has disclosed that the hacking group responsible for the massive Medibank hack that compromised the personal information of 9.7 million customers is based in Russia. The group's identity was not yet published.

- Black Basta ransomware group has launched a cyberattack against Canadian grocery and pharmacy chain store Sobeys, impacting some of the company's in-store services and operations.

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

- Security Researchers have disclosed two new surveillance campaigns targeting Uyghurs in the People's Republic of China and abroad with BadBazaar and MOONSHINE spyware.

- Threat actors are mass spreading scam emails that are aimed at website owners worldwide, claiming they allegedly hacked and extracted databases, demanding $2,500 not to sell the data on the dark net.

- County offices in Arkansas, US, are told to work offline due to a breach. It has been said that the issue could last two weeks. No hacking group has yet taken responsibility for the hack.

- Researchers have identified Vidar Stealer and Raccoon malware campaigns using YouTube videos to pose as cracks for popular programs. The videos contain a malicious link within the video description, and once the victims click on the link - they are then redirected to a phishing page that mimics legitimate websites.

  Check Point Threat Emulation and Anti-Bot provide protection against this threat *(InfoStealer.Win/Wins.Raccoon.*; Banker.Win.Vidar.*; Trojan.Win32.Vidar; Trojan.Win32.Raccoon)*

- A new Chinese sub-group of the Advanced Persistent Threat hacking group - APT41 - has been identified in the wild and is called 'Earth Longzhi'. The sub-group is targeting organizations in East Asia, Southeast Asia, and Ukraine using custom versions of Cobalt Strike loaders to plant persistent backdoors on victims' systems.

- Security researchers have linked a series of attacks targeting transportation and logistics organizations in Ukraine and Poland using Prestige ransomware with Russian military cyberespionage group IRIDIUM.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Win.TouchTrapFiles.A; Ransomware.Win.GenRansom.glsf.A; Ransomware.Win.FilesMovedOrOverwrites.A)*

VULNERABILITIES AND PATCHES

- Check Point Research identified a new and unique malicious package on PyPI, the leading package index used by developers for the Python programming language. The package was designed to hide code in images and infect through open-source projects on Github.
- Google has addressed a high-severity security bug, tracked as CVE-2022-20465, affecting all Pixel smartphones, which could be exploited to unlock the devices.
- Researchers have disclosed the details of a vulnerability affecting ABB Totalflow system used in oil and gas organizations. The vulnerability, tracked CVE-2022-0902, is a path-traversal weakness that can be exploited by an attacker to inject and execute arbitrary code.
- Apple has released out-of-band patches for iOS and macOS to address two code execution flaws, tracked as CVE-2022-40303 and CVE-2022-40304, in the libxml2 library for parsing XML documents.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports a significant increase in Lokibot attacks in October, taking it to third place in the top global malware families for the first time in five months. AgentTesla took the top spot.
- The Azov ransomware is being distributed worldwide to encrypt victim files, while in fact an analysis by Check Point Research proves that Azov ransomware is a data wiper aimed at destroying data with no way to recover the files.

  Check Point Harmony Endpoint provides protection against this threat
- The security team of the United States Department of Health and Human Services has published a report on the new Venus ransomware, which they say has hit at least one U.S. healthcare organization since it was first spotted in the wild this August.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Win.TouchTrapFiles.A; APT.Win.MustangPanda.A; Trojan.Win.Staser.glte.F; Ransomware.Win.Netwalker.A)*
- Security Researchers have found evidence that the cyberespionage group – 'Worok' – has started employing steganography – a technique whereby malware is concealed within PNG images to infect systems and steal information.
- The United States Department of Justice has announced the arrest of a 33-year-old Russian and Canadian national who is an alleged member of the notorious LockBit ransomware group.
- Researchers have released a paper that outlines decryption steps for the RanHassan ransomware - a ransomware family that has been primarily targeting victims in India and Arab-speaking countries.