December 19 – 25, 2022

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- LastPass revealed that it has been breached for the second time this year, an event that resulted in attackers stealing customer encrypted password vaults and additional account information. The breach was achieved after attackers used information stolen from the LastPass development environment in the August incident to expand their hold on the company's assets.

- Okta, a leading provider of authentication services and Identity and Access Management solutions, has confirmed that it's dealing with the fourth security incident of this year, after a hacker accessed its source code following a breach of its GitHub repositories. Customer data was not impacted.

- Sports betting company BetMGM said a threat actor stole personal information belonging to an undisclosed number of customers in a data breach earlier this year. The issue affected customer information such as name, contact information, date of birth, hashed Social Security number, account identifiers and information related to transactions with BetMGM.

- Play ransomware has taken responsibility for an attack on H-Hotels, a large hotel chain with 60 hotels in 50 locations across Germany, Austria, and Switzerland. The cyber-attack has led to communication outages for the company.

- Researchers have discovered that Play ransomware threat actors are utilizing a novel exploit method (dubbed OWASSRF) that bypasses ProxyNotShell URL rewrite mitigations, allowing remote code execution on vulnerable servers through Outlook Web Access.

  Check Point IPS provides protection against this threat (Microsoft Exchange Server Server-Side Request Forgery (CVE-2022-41080); Microsoft Exchange Server Remote Code Execution (CVE-2022-41082))

- In an attack that lasted at least two years, hackers have managed to hack the John F. Kennedy International Airport (JFK) taxi dispatch system, tamper with the taxi queue and move specific taxis in it to shorten waiting time, all to make profit. Two US citizens have been arrested and accused of allegedly conspiring with Russian hackers to perform the attack.

- Researchers revealed that on August, the Russia-linked Gamaredon APT unsuccessfully attempted to breach a large petroleum refining company within a NATO member state, as a part of a set of intrusion attempts to multiple sectors.

  Check Point Threat Emulation and Anti-Bot provide protection against this threat (InfoStealer.Win.Gamaredon; Trojan.Win32.Gamaredon.A)

VULNERABILITIES AND PATCHES

- Researchers have recently discovered two vulnerabilities in Ghost CMS, an authentication bypass vulnerability (CVE-2022-41654) that can lead to increased privileges, and an enumeration vulnerability (CVE-2022-41697) in the login functionality of Ghost which can lead to a disclosure of sensitive information.
- Apple has released a fix for CVE-2022-42821 (dubbed Achilles), a vulnerability that could be could leveraged to deploy malware on vulnerable macOS devices through untrusted applications, capable of bypassing Gatekeeper application execution restrictions.
- A critical flaw disclosed earlier this year in YITH WooCommerce Gift Cards Premium (CVE-2022-45359), a WordPress plugin used on over 50,000 websites, is being actively exploited. Successful exploitation allows unauthenticated attackers to upload files to vulnerable sites, including web shells that provide full access to the site.

THREAT INTELLIGENCE REPORTS

- As artificial intelligence (AI) models grow more and more popular, Check Point Research discusses the risks and upsides of the technology. CPR demonstrates how AI technologies, like ChatGPT and Codex, can easily be used to create a full infection flow, from spear-phishing to running a reverse shell, and provides examples of the positive impact of AI on the defenders' side.
- Researchers have discovered a new tactic used by the Raspberry Robin malware, a worm-like malware dropper that sells initial access to compromised networks to ransomware gangs and malware operators. The malware is dropping a new fake payload to confuse researchers and evade detection, specifically in those spotted against telecommunication service providers and government systems.

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

- Researchers have shared their spotlight on the notorious FIN7 group, a Russian-speaking and financially motivated threat actor active since at least 2012 and known for various scandalous acts. The report reveals, among others, the group's internal hierarchy and its use of an automated attack system that exploits Microsoft Exchange and SQL injection vulnerabilities to breach corporate networks, steal data, and select targets for ransomware attacks based on their financials.

  Check Point IPS provides protection against this threat *(Microsoft Exchange Server Security Feature Authentication Bypass (CVE-2021-31207); Microsoft Exchange Server Remote Code Execution (CVE-2021-34473); Microsoft Exchange Server Remote Code Execution (CVE-2021-34473))*