November 14 – November 20, 2022

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- US CISA has discovered nation-state threat activity affecting an American federal government entity. The attackers, who CISA estimates to be Iran-sponsored, exploited the 2021 'Log4Shell' vulnerability in an unpatched server to gain initial access. Afterwards, the attackers deployed a cryptocurrency miner, harvested credentials, and employed various techniques to move laterally and establish persistence in the network.

  Check Point IPS provides protection against this threat (Apache Log4j Remote Code Execution (CVE-2021-44228; CVE-2021-45046))

- Check Point warns of increased scam and phishing activity targeting shoppers during the holiday season. Hackers and scammers are exploiting the boom in online sales during the Thanksgiving period to lure in as many potential victims as possible.

- The FBI, alongside CISA and additional agencies, have published a security advisory regarding the Hive ransomware group. According to the FBI, Hive has ransomed over 1,300 organizations for a total of $100M in the past 18 months, focusing on targets in the Healthcare industry.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Hive.A; Ransomware.Wins.Hive.ta.B))

- The Russian government-affiliated hacktivist group Killnet has launched denial of service attacks against the White House website, as well as the satellite internet communication corporation Starlink which has been used by Ukraine. Killnet claims that the attack has successfully taken down the websites.

- Multiple groups have been exploiting a vulnerability in Adobe Commerce and Magento to gain access to online stores. The attacks, which have risen in volume towards the holiday season, allow the threat actors to gain permanent remote access to the online stores.

  Check Point IPS provides protection against this threat (Adobe Commerce Command Injection (CVE-2022-24086))

- Meta has fired dozens of employees, after the employees had received thousands of dollars in bribes by outside hackers in return for granting access to users' Facebook or Instagram profiles. The employees used the company's internal support tool, which allows full access to any user account.

- In Michigan, schools in two counties were forced to suspend operations due to a ransomware attack. The threat actor behind the attack is not yet known.

VULNERABILITIES AND PATCHES

- Researchers have discovered a critical severity vulnerability affecting Spotify's open source Backstage platform, which is being used by a large number of companies worldwide. The vulnerability could allow a threat actor to gain remote code execution, and was patched by the Spotify Backstage team.
- Samba has patched vulnerabilities in several versions of their software. In certain cases, the vulnerabilities could allow an attack to gain control of affected systems.
- Atlassian Confluence has released patches to critical severity vulnerabilities discovered in Atlassian Crowd Server, and in Atlassian Bitbucket. Both vulnerabilities could allow an attack to gain remote access to an unpatched system.
- F5 has published a security advisory regarding a vulnerability affecting its BIG-IP and BIG-IQ products, which could allow an attacker to gain access to an affected system after fulfilling certain requirements.

THREAT INTELLIGENCE REPORTS

- Researchers have detected modifications made to the DTrack malware, which is being utilized by the North Korean APT group Lazarus. The malware includes spying tools such as keylogging and screenshotting, and also allows injection and exfiltration of files. Recently, the group has expanded its range of operations, and has been observed targeting entities in Europe and Latin America.

  Check Point Threat Emulation provides protection against this threat (RAT.Win32.Dtrack; InfoStealer.Wins.Dtrack.A)

- An analysis of Emotet's latest comeback has been published. After being inactive since July, Emotet campaigns have been detected in large volume in November. According to researchers, the threat actors have made multiple modifications to the malware, including to the end-stage payload which can now also drop the IcedID and Bumblebee malware variants.

  Check Point Threat Emulation, Harmony Endpoint and Anti-Bot provide protection against this threat (Trojan-Downloader.Win32.IcedID; Trojan.Win32.Emotet; Dropper.Win.GenDrop.la.E; Trojan-Downloader.Win.Bumblebee.J)

- Researchers have analyzed the activity of the state-sponsored group dubbed Billbug, likely attributed to China. The group has targeted governments, defense agencies and a certificate authority, all based in Asia. According to the researchers, the motivation behind the attacks was data theft.
- A new botnet targeting Linux IoT devices has been discovered. The attackers attempt to gain access to devices via brute-forcing commonly used default passwords. According to the analysis, the goal of the botnet is to DDoS popular game servers.
- Researchers warn against cyberattacks leveraging the FIFA World Cup to lure victims in phishing attacks.