Check Point
SOFTWARE TECHNOLOGIES LTD.

Oct 26 – Nov 01, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- CISA, FBI and HHS have released a warning against an increase in Ryuk ransomware attacks on US hospitals. Check Point Research have shown that indeed, healthcare is currently the most targeted industry in the US, with a 71% increase in attacks compared to last month. Other regions have experienced an increase of 30%.

  Check Point SandBlast and SandBlast Agent provide protection against this threat (Ransomware.Win32.Ryuk)

- The Republican Party of Wisconsin (WisGOP) has confirmed 2.3 million dollars reserved for president Donald Trump's reelection campaign were stolen in a phishing email scam.

- Wroba, a new Mobile banking Trojan associated with "Mantis group", has been targeting US Android and iPhone users. The campaign is spread via text massages, baring fake notifications about package deliveries as a lure. When clicking the malicious link, Android users are redirected to a notification asking to update the browser, while actually installing the malware on the device. iOS users are redirected to a phishing website trying to steal their Apple ID credentials.

  Check Point SandBlast Mobile provides protection against this threat (Trojan.Android.Wroba)

- An unknown threat actor has offered for sale a database containing 34 million user records stolen from 17 companies, including Singapore online grocery platform RedMart, Mexican Clip and more. All breaches allegedly took place in 2020.

- Researches have uncovered a new watering hole attack targeting the Korean diaspora, dubbed Operation Earth Kitsune. The attackers exploit flaws in web browsers, both Chrome and IE, to deploy two new backdoors, dneSpy and agfSpy.

- REvil ransomware operators are claiming to have stolen 540GB of data in recent attack from Gaming Partners International (CPI), supplier of gaming furniture and equipment for casinos worldwide.

  Check Point SandBlast and SandBlast Agent provide protection against this threat (Ransomware.Win32.Revil)

VULNERABILITIES AND PATCHES

- Google's project Zero has disclosed a new Windows 0day vulnerability currently under active exploitation. The vulnerability (CVE-2020-17087), affecting Windows 7 to 10, allows attackers to escape Chrome sandboxes and run malware on the operating system.

  Check Point IPS provides protection against this threat (Microsoft Windows Kernel Local Elevation of Privilege (CVE-2020-17087))

- A severe vulnerability in Oracle WebLogic Server disclosed last month is actively being scanned for in the wild, and might also be exploited.

  Check Point IPS provides protection against this threat (Oracle WebLogic Remote Code Execution (CVE-2020-14882))

- Research has shown that over 100,000 machines facing the internet are still vulnerable to Microsoft SMBGhost vulnerability (CVE-2020-0796) despite the company's patch, released over 8 months ago.

  Check Point IPS provides protection against this threat (Microsoft Windows SMBv3 Remote Code Execution (CVE-2020-0796))

- WordPress has patched 10 security bugs as part of the release of version 5.5.2 of its web publishing software, including a 3-year-old high severity RCE vulnerability.

THREAT INTELLIGENCE REPORTS

- Check Point Research has done the profiling of an exploit developer known as "PlayBit" or "luxore2008", identifying his fingerprints across different exploits. This developer's exploits are used by high-profile malware and ransomware, including Ramnit, Dyre, Maze, Locky, REvil and others.

  Check Point SandBlast provides protection against this threat

- Maze ransomware operators seem to be in the process of shutting down their business. Affiliates are switching to a new operation called Egregor, partially based on the same code as Maze.

  Check Point SandBlast Agent provides protection against this threat

- US Cyber command CISA and FBI have exposed eight new Russian malware samples. The samples are for ComRAT and Zebrocy malware, attributed to Turla and APT28 groups respectively.

  Check Point SandBlast Agent and Anti-Bot provide protection against this threat (Trojan-Downloader.Win32.Zebrocy)

- A new Android malware called Firestarter, developed by the DoNot APT group, is abusing the legitimate Google Firebase Cloud Messaging server as a command and control communication mechanism.

  Check Point SandBlast Mobile provides protection against this threat (downloader.Android.Firestarter)

- Researchers have found Emotet botnet is abusing parked domains to deliver malware payloads as part of a new large-scale phishing campaign.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Trojan.win32.Emotet)