April 13 - 19, 2020

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Threat actors have employed the previously-unknown PoetRAT Trojan in a coronavirus-themed campaign aimed at the Azerbaijan government and utility companies. Delivered via phishing, the malware infected ICS and SCADA systems used to control the wind turbines within the renewable energy sector.

  Check Point Anti-Virus provides protection against this threat (PoetRAT.TC)

- Portugal electric company, Energias de Portugal (EDP), has been hit by Ragnar Locker ransomware. The attackers demand 1,580 bitcoin amounting to $10.9 million to retrieve 10 TB of stolen data. To prove they poses the company's data, the threat actors leaked data from EDP's KeePass password manager, which contains the login credentials, accounts, URLs and notes of employees.

  Check Point SandBlast Agent provides protection against this threat

- Cognizant, IT managed services company based in the US, had suffered from a ransomware attack, allegedly Maze ransomware.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Ransomware.Win32.Maze)

- Aptoide, a third-party app store for Android application has suffered a data breach. The data, which was published on a well-known hacking forum, is part of a large batch of 39 million personal identifiable information records stolen between July 21, 2016 and January 28, 2018.

- Taxpayers have been targeted by a new variant of the NetWire RAT in a malspam campaign that makes use of an improved keylogger and credential-collecting feature delivered by an Excel 4.0 macro.

  Check Point SandBlast, Anti-Bot and Anti-virus provide protection against this threat (Trojan.Win32.NetWire)

- A new Ursnif/ISFB campaign is targeting Italian organizations. The dropper has adopted new techniques using XML macros, and two different C2, one of which is in charge of tracking each infection with a unique victim ID.

  Check Point SandBlast and Anti-Bot provides protection against this threat (Banking.Win32.Ursnif)

VULNERABILITIES AND PATCHES

- Oracle has released patches that address 405 new security vulnerabilities in multiple products.
- A new security vulnerability has been found in Slack. The vulnerability allows an attacker to send a message to any workspace, regardless of their membership, thus facilitating phishing attacks.
- Intel has addressed 9 security vulnerabilities in the April 2020 Platform Update, all of them being high and medium severity security flaws impacting multiple software products, firmware, and platforms.
- Microsoft has released its April 2020 Patch Tuesday security updates. The release addressed 113 vulnerabilities, 19 of which rated as critical and 94 rated as important. Four of the vulnerabilities are being exploited in the wild.

  Check Point IPS provides protection against these threats (CVE-2020-0888; CVE-2020-0957; CVE-2020-0956; CVE-2020-0958; CVE-2020-0938; CVE-2020-0968; CVE-2020-1020; CVE-2020-1027; CVE-2020-1004; CVE-2020-0784)

THREAT INTELLIGENCE REPORTS

- Check Point Research have shown how ransomware are blurring the line between traditional ransomware attacks and traditional data breaches, both encrypting files and threatening to publish confidential data if ransom is not paid.

  Check Point SandBlast Agent provides protection against this threat

- Check Point Research have shown that threat actors are leveraging the economic stimulus declared in the US in their phishing campaigns, sending out emails with malicious attachments titled “COVID-19 Payment” or links to phishing websites.
- Google has removed 49 Chrome extensions from the Web Store that posed as legitimate cryptocurrency wallet apps like Ledger, MyEtherWaller, Trezor, Electrum, and others. The extensions contained malicious code able to steal crypto-wallet private keys, mnemonic phrases, and other raw secrets.
- Researchers have found clipboard hijacking in 725 Ruby libraries. The malicious packages were uploaded to the official RubyGems repository between February 16 and 25 and replaced cryptocurrency addresses copied to the clipboard with the attacker's address. All libraries were copies of legitimate libraries, worked as intended, but also contained the malicious files.
- A new AgentTesla variant steals WiFi credentials. The popular infostealer is a .Net-based infostealer that obtains the capability to steal data from different applications on victim machines, such as browsers, FTP clients, and file downloaders recently added a new feature that can steal WiFi usernames and passwords.

  Check Point SandBlast and Anti-Bot provides protection against this threat (Trojan.Win32.AgentTesla)