November 2-8, 2020

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has alerted against a wave of ransomware attacks targeting Israeli companies and corporations, using known ransomware families such as REvil and Ryuk, as well as a new family called 'Pay2Key'. The ransomware is capable of rapid lateral movement within the company network.

  Check Point SandBlast Agent provides protection against these threats *(Ransomware.Win32.Pay2Key; Ransomware.Win32.REvil)*

- Luxottica, the world's largest eyewear company, has admitted it has been breached. The giant's appointment scheduling application has been hacked, leading to the exposure of protected health information (PHI) for patients of eye care practices such as LensCrafters, Target Optical and EyeMed.

- Japanese game developer Capcom has suffered a breach leading to the shutdown of some its systems, possibly by the Ragnar Locker ransomware. Attackers claim that 1TB of sensitive data has been stolen.

  Check Point SandBlast Agent provides protection against this threat *(Ransomware.Win32.Ragnar)*

- The Italian liquor company Campari Group has been hit by the Ragnar Locker ransomware, leading to the theft of 2TB of unencrypted files. The attackers are demanding a $15 million ransom to retrieve the files.

- Check Point Research has uncovered an attack operation targeting the Sangoma and Asterisk VoIP phone systems at nearly 1,200 organizations. The attackers, most likely located in Gaza and the West Bank, target SIP servers to execute telecom fraud, sell phone number and gain access to the organizations' VoIP servers.

  Check Point IPS provides protection against this threat *(SIPVicious Security Scanner; Sangoma FreePBX Authentication Bypass (CVE-2019-19006); Command Injection Over HTTP)*

- North Korean surveillance campaign targeting the aerospace and defense sectors in Australia, Israel, Russia and India is spreading a new spyware called Torisma via fake job offers sent through social media.

- New phishing campaign leverages a flaw in Google Drive to distribute emails and notifications allegedly from Google, which could lead to malicious websites if opened. The scam uses a collaboration feature that generates a notification inviting users to access a shared document.

VULNERABILITIES AND PATCHES

- Apple has released a fix for three zero-day vulnerabilities currently exploited in the wild in iPhone 6s and later, iPod touch 7th generation, iPad Air 2 and later, and iPad mini 4 and later. One of the flaws, assigned CVE-2020-27930, is a memory corruption bug that that allows arbitrary code execution using a maliciously crafted font.

- Cisco has published a zero-day vulnerability in the its AnyConnect Secure Mobility Client software, as well as a Proof-of-Concept exploit code. The flaw, assigned CVE-2020-3556, allows arbitrary code execution to an authenticated local user and does not have a fix yet.

- Vulnerability in Oracle WebLogic, assigned CVE-2020-14882, has been actively exploited by threat actors to deploy Cobalt Strike, a legitimate pen-testing tool often leveraged by attackers, enabling them to establish persistent remote access to infected devices.

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

- New version of Google Chrome for Windows, Mac and Linux has been released to address 10 security vulnerabilities. Among these is a remote code execution zero-day bug assigned CVE-2020-16009, that has been exploited in the wild.

THREAT INTELLIGENCE REPORTS

- Check Point Research conclude that Trickbot and Emotet, massive botnets used for malware distribution, have been the two most prevalent malware in October, responsible for the sharp rise in ransomware attacks against hospitals and healthcare providers globally.

  Check Point SandBlast and Anti-Bot provide protection against these threats *(Trojan-Banker.Win32.TrickBot; Trojan.Win32.Emotet)*

- Researchers have reviewed the ransomware landscape of Q3 2020 and found that nearly half of all ransomware cases now include the threat to release exfiltrated data, but paying the ransom does not guarantee that the data will not be published anyway. The average ransom payment is $233,817 – a 30% increase compared to Q2.

- Recently revealed Chinese hacking group has been using DLL side-loading techniques to execute an attack against non-government organizations in Southeast Asia, especially Myanmar.

- Industrial companies, mainly in Russia, have been targeted by a phishing campaign active since 2018. Upon infection, TeamViewer or Remote Manipulator System (RMS) is installed and utilized for remote control and as a communication channel.