June 10 - 16, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Belgium-based airplane parts and aviation structuring business ASCO Industries has shuttered its plants in Belgium, Germany, Canada and the US after falling victim to a ransomware attack. Nearly 1,000 employees were sent home for the entire week.
- Telegram's founder Pavel Durov links China with the powerful DDoS attack, which disrupted Telegram services. Attack has been connected to the Hong Kong marches in which protestors used Telegram to coordinate demonstrations over a plan to allow extradition to China.
- After a two-year absence, the FIN8 hacking group has returned with a new campaign mainly targeting point-of-sale machines in the hotel industry in an effort to steal credit card and other payment data.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Backdoor.Win32.Shelltea)
- U.S. Customs and Border Protection subcontractor has been hacked, leaking photos of over 100,000 individuals and license plates of travelers crossing U.S. borders. Reports relate this to last month's hack to Perceptics, a license plate reader technology provider whose data had been found on the dark web.
- An active spam campaign targeting European languages is distributing RTF documents exploiting the Microsoft Office and Wordpad CVE-2017-11882 vulnerability. Once opened, these weaponized documents require no user interaction to infect platforms with backdoor malware.

  Check Point IPS blade provides protection against this threat (Microsoft Office Memory Corruption Remote Code Execution (CVE-2017-11882))
- 8.4 TB of email metadata owned by Shanghai Jiao Tong University have been left exposed on an ElasticSearch database revealed through a Shodan search.
- Activity targeting electric utilities in the U.S. and the Asia-Pacific (APAC) region has been detected. The operation is attributed to the Xenotime threat actor which was behind the 2017 Trisis attack on Saudi oil and gas organizations with possible Iranian and Russian links.

- Exim email servers are under attack due to a remote code execution vulnerability, affecting almost half of the internet's email servers.

  Check Point IPS blade provides protection against this threat (Exim Mail Server Remote Code Execution (CVE-2019-10149))

VULNERABILITIES AND PATCHES

- Adobe has released its June 2019 patch Tuesday software update addressing 11 security vulnerabilities in Flash Player, ColdFusion and Campaign.

  Check Point IPS blade provides protection against this threat (Adobe Flash Player Use After Free (APSB19-30: CVE-2019-7845)

- Microsoft has released patches to 88 vulnerabilities in its June patch Tuesday release. 21 of the vulnerabilities are rated critical and 66 important.

  Check Point IPS blade provides protection against these threats (Microsoft Internet Explorer Scripting Engine Memory Corruption (CVE-2019-0920); Microsoft Speech API Remote Code Execution (CVE-2019-0985); Microsoft Edge Chakra Scripting Engine Memory Corruption (CVE-2019-1051); Microsoft Edge Scripting Engine Information Disclosure (CVE-2019-1023); Microsoft Internet Explorer Scripting Engine Memory Corruption (CVE-2019-0988) and more)

- Cybersecurity researchers have discovered a critical flaw in the popular Evernote Chrome extension (4.6 million users) that could allow hackers to hijack user browser and steal sensitive information from any accessed website.

  Check Point IPS blade will provide protection against this threat in its next online package

- Two security vulnerabilities, one with a critical rating of 10, have been found in Becton Dickinson Medical Infusion Pumps, widely used in hospitals. Flaws can be remotely exploited to gain full control of the infusion pump to change infusion rate or completely turn off the pump.

THREAT INTELLIGENCE REPORTS

- The MuddyWater cyber espionage group continues to evolve and has recently used an updated multi-stage PowerShell backdoor in spear-phishing attacks aimed at a university in Jordan and the Turkish government.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Backdoor.Win32.MuddyWater)

- Months long malspam attack on Italian users deliver variants of Ursnif. A new report details the evolution of the malware.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Banking.Win32.Ursnif)