July 24th – July 30st , 2017

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Swedish government is in turmoil, with 2 ministers already having resigned, following the discovery that a government contract has led to a massive leak of nearly all of the country's citizens' personal information. In 2015, the Swedish Transport Agency had outsourced database management to Intel Sweden, which in turn outsourced it to companies in Eastern European countries, whose employees had access to the information despite having no security clearance. The leaked database contains information of all vehicles, including some military vehicles; license information (including photos) of all citizens, including protected individuals (undercover law enforcement officers, persons in witness protection programs); and information about national infrastructure in the country.

- Chinese authorities have arrested 14 employees of Rafotech, a Chinese digital advertising company. Rafotech is the company behind the Fireball malware, a browser hijacker with remote control capabilities which has infected millions of machines worldwide to generate advertisement revenue. According to the Chinese police, their profits in 2016 were almost $12M. The arrests were made following Check Point's publication exposing the malware, its immense infection rate, and its creators.

- According to reports, Chinese authorities are forcing members of the Uyghur Muslim minority to install a spyware app on their phones, or face imprisonment. The app copies credentials and scans for terrorist content on affected devices.

- Italian banking company UniCredit has announced that information of 400,000 of its customers had been disclosed following a breach of one of the company's partners. According to UniCredit, passwords were not leaked in the breach.

- A backdoor has been found in the firmware of several low-cost Android smartphones.

  Check Point Anti-Bot blade provides protection against this threat *(Trojan.AndroidOS.Triada)*

VULNERABILITIES AND PATCHES

- Researchers have found vulnerabilities in the popular PDQ's smart car wash systems. The vulnerabilities can be exploited to alter the system's behavior to physically damage vehicles and passengers.
- Researchers have demonstrated remote control vulnerabilities in Tesla's Model X car in a YouTube video. The researchers managed to access the car's lights, trunk and doors remotely, and even managed to remotely activate the brakes while the car was in motion. Tesla has patched the vulnerabilities.
- Google has released Chrome 60, which among several new features also includes patches for 40 security vulnerabilities.
- Another vulnerability in Microsoft's SMB has been revealed, yet to be patched by the vendor. A successful attack could lead to a denial of service.

  Check Point IPS blade provides protection against this threat *(Microsoft Windows SMB SMBLoris Denial of Service)*
- Researchers have discovered 6 vulnerabilities in the open source FreeRDP platform. Two of the vulnerabilities allow remote code execution, and the rest cause denial of service when exploited.

THREAT INTELLIGENCE REPORTS

- An analysis of a new Ransomware-as-a-Service variant named Philadelphia has been published. The service is widely available on the dark net for around $400, and includes multiple customizable features.

  Check Point Anti-Bot blade provides protection against this threat *(Trojan-Ransom.Win32.Philadelphia.*)*
- A new Backdoor malware variant, CowerSnail, has been discovered, targeting Windows systems. One of the C&C servers used for the malware is also used by the Linux malware SambaCry, leading to the conclusion that the two were created by the same group.

  Check Point IPS, Anti-Bot and Anti-Virus blades provide protection against this threat *(Linux EternalRed Samba Remote Code Execution; Backdoor.Win32.CowerSnail)*
- A decryption tool for the Petya ransomware versions prior to NotPetya has been released, after the creator shared the malware's source code.

  Check Point Anti-Bot blade provides protection against this threat *(Trojan-Ransom.Win32.Petya.*)*
- Researchers have found that 2 banking malware families, Emotet and TrickBot, have added lateral infection capabilities following the success of the WannaCry and NotPetya malware families.

  Check Point IPS, Anti-Bot and Anti-Virus blades provide protection against this threat *(Microsoft Office Files Containing Malicious VBScript Downloader; Suspicious Executable Mail Attachment; Suspicious Mail Attachment Containing JavaScript Code; Operator.Emotet; Operator.Trickbot)*