August 7 – August 13, 2017

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Reports claim that a nation-state actor has breached EirGrid, Ireland's electricity transmission company, and gained complete access to the company's network. It is not yet clear what the attacker's goal was in this breach, which could have been utilized to cause blackouts across Ireland.

- The Russian hacker group APT28 (Fancy Bear), famous for breaching and leaking the contents of the DNC in the 2016 American elections, is likely behind breaches into several hotels in the Middle East and Europe. The group used their access to hotels' networks to steal credentials and gain control of visitors using the hotels' WiFi. APT28 utilized EternalBlue, an SMB 0-day vulnerability attributed to the NSA.

  Check Point IPS blade provides protection against this threat (Microsoft Windows EternalBlue SMB Remote Code Execution)

- Television network HBO has attempted to gather $250,000 in Bitcoins to pay the hackers who breached the company's network, in what HBO prefers to call a "bug bounty payment". Some claim this was a delay tactic. The hackers, however, demand millions of dollars, and have so far leaked episodes of many HBO shows, the script of the 5th episode of the popular HBO series Game of Thrones, and personal information of the show's stars.

- The Mamba ransomware, which affected San Francisco's Metro last year, has recently resurfaced and targeted corporations in Brazil and Saudi Arabia, according to researchers. The article includes a technical analysis of the ransomware.

  Check Point Anti-Bot blade provides protection against this threat (Trojan-ransom.Win32.Mamba.)*

- An anti-Israeli wiper malware dubbed 'IsraBye' was discovered targeting Israel-based entities in the wild. The malware poses as ransomware, but the files cannot be recovered once encrypted.

  Check Point Anti-Bot blade provides protection against this threat (Trojan.Win32.IsraBye.)*

VULNERABILITIES AND PATCHES

- Researchers have managed to encode malware into DNA molecules. Once the modified DNA is processed by a vulnerable sequencing device, the device will become infected and the attacker will gain remote code access to it.

- A new study shows that self-driving cars are vulnerable to the defacement of physical street signs, which could confuse the cars' machine-learning algorithm and dangerously alter their behavior. The researchers have also demonstrated that the defacement can look like regular graffiti of street signs.

- A new research shows that USB devices are vulnerable to crosstalk leakage, which means that electricity from the activity of the device leaks into adjacent USB ports. This can be exploited by malicious USB devices to spy on the activity of devices plugged to adjacent ports.

- Several major vendors have released security updates for a large number of vulnerabilities. Among them are Adobe, Juniper, Microsoft, Mozilla and Symantec. Some of these vulnerabilities are tagged as critical, meaning that successful exploitation could result in remote code execution on vulnerable machines. Microsoft's patch included a vulnerability in Windows Search service dubbed CVE-2017-8620, that could allow attackers privilege escalation and "wormability" inside a network.

  Check Point IPS blade provides protection against some of these threats

THREAT INTELLIGENCE REPORTS

- Researchers have discovered a new obfuscation technique used by the Magnitude exploit kit to install the Cerber Ransomware. Magnitude uses binary padding to enlarge the file size of Cerber from 200 KBs to over 70 MB, which helps the malware bypass several protection tools which have file size restrictions.

  Check Point IPS and Anti-Bot blades provide protection against this threat (Magnitude Exploit Kit., Operator.Magnitude, Trojan-Ransom.Win32.Cerber, Operator.Cerber.*)*

- Over a thousand Android Spyware apps related to the "SonicSpy" spyware family have been discovered, some of which were available on Google Play store.

  Check Point Mobile Threat Prevention users are protected from this threat

- A new variant of the popular Locky ransomware named Diablo6 is being spread in a spam email campaign.

  Check Point IPS and Anti-Bot blades provide protection against this threat (Suspicious Mail Attachment Containing JavaScript Code; Trojan-ransom.Win32.Locky.; Operator.Locky)*