Check Point
SOFTWARE TECHNOLOGIES LTD.

July 23 - 29, 2018

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Cosco, a Chinese state-owned ocean shipping company, has been hit by a ransomware attack. The attack crippled multiple company networks across the Americas region, and in response the company shut down the network connections with other regions.

- OilRig, an espionage group which operates in the Middle East, has been carrying out a targeted campaign against a technology services provider and a certain government entity in the same nation in the Middle East, using the Quadagent Backdoor. The attack originates from a government agency in the same state, which was most likely compromised by the group for this purpose.

  Check Point Anti-Bot and Anti-Virus blades provide protection against all known variants of this threat (Oilrig; Trojan.Win32.Oilrig; Operator.Oilrig)

- Several local and state government agencies across the US received peculiar letters, which included compact discs (CDs) containing malware. The CDs were in envelopes postmarked in Chinese, and included Mandarin language Word files and malicious Visual Basic scripts.

- LifeLock, an American identity theft protection company, recently patched a bug that enabled attackers to index email addresses associated with millions of its users' accounts via a web browser. The bug could also allow attackers to carry out tailored operations targeting LifeLock customers.

- Blue Springs Family Care, a health care provider based in Missouri, has been the victim of a ransomware attack. Some 45,000 patient records, which include personal identification details, medical diagnoses and disability codes, may have been compromised.

- Several fake banking applications, which collect card payment data and banking credentials, were found in Google Play app store. The applications target customers of three Indian banks, by offering to increase credit card limits. The stolen credentials are then leaked online.

  Check Point SandBlast Mobile customers are protected from this threat

VULNERABILITIES AND PATCHES

- Intel released patches for three vulnerabilities in its Smart Sound Technology, all classified as Important and might allow an attacker to execute arbitrary code on Intel Core and PCs based on the Atom processor. Smart Sound is a processor built to handle audio, video and speech interactions such as voice commands and high fidelity audio.
- Some 20 flaws have been found in Samsung's SmartThings Hub controller, a device used to manage various home digital devices. The flaws might allow attackers to take control over the devices, and thus to configure home alarms, monitor cameras and perform various functions.
- Researchers discovered a vulnerability in some Bluetooth implementations, which impacts the standard's Secure Simple Pairing feature. The flaw, assigned CVE-2018-5383, may allow an attacker to intercept or influence data sent between two vulnerable devices. Software and firmware updates are expected to be released in the coming weeks.

THREAT INTELLIGENCE REPORTS

- An analysis of the Micropsia malware, which was used in a targeted campaign against Palestinian targets, recently reported by Check Point researchers, is presenting the malware's advanced surveillance capabilities, which include microphone recording and document theft from connected USB devices.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Micropsia; Big Bang)*

- Check Point researchers have reviewed the Emotet malware downloader reincarnations and current functions. Emotet began its way as a unique Banking Trojan, and has evolved to operating as a sophisticated third-party malware distributor, with a variety of modules and evasion techniques.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Emotet)*

- A new type of drive-by attack kit was observed in the wild, spreading a custom payload which downloads the Hidden Bee Crypto Miner Botnet to infected machines. The kit leverages malvertising via adult sites to redirect its victims to the exploit kit landing page, and targets primarily Asian users.

  Check Point IPS and Anti-Virus blade provides protection against this threat *(Adobe Flash Player Use After Free (APSB18-03: CVE-2018-4878); Microsoft Windows VBScript Engine Remote Code Execution (CVE-2018-8174); Hidden_Bee; Trojan.Win32.Hidden_Bee)*

- Researchers have revealed a new malware dubbed Calisto, which targets Mac OS users and had remained under the radar since it first emerged in 2016. The malware is well disguised as an up-to-date version of the Intego Internet Security for Mac, and could be related to the Proton malware family.

  Check Point Anti-Virus blade provide protection against this threat *(Trojan.MacOX.Calisto)*