August 14 – 20, 2017

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point has discovered attacks towards more than 4,000 corporates worldwide, resulting in at least 14 successful infections. Many of the targets were energy and shipping companies. Despite the relative localization and success of the attacks, apparently they were not state-sponsored but rather the work of 1 threat actor based in Nigeria, using widely-available and unsophisticated tools and methods.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat

- A backup of Chicago's entire voter database of over 1.5 million people had been left publically available online on an unsecure Amazon Web Services bucket for months, before being discovered by a research group. The database contains addresses, dates of birth, partial Social Security numbers and in some cases- driver's license numbers. It is unknown whether the database was accessed by malicious actors.

- Hundreds of malicious adware Android apps were discovered in Google Play by analysts, one of which with 5 million downloads, mostly from Southeast Asia, Brazil, Japan, Taiwan, Russia, Italy, and the US. The apps, which masquerade as legitimate, include an auto-clicker for ads, and seek to gain administrator permissions to avoid removal.

- The Ukrainian central bank has warned Ukrainian businesses of the possibility of large-scale threat campaign to be held on August 4th, Ukraine's Independence Day. This speculation stems from a wave of malicious emails enclosing an unknown malware, sent to several Ukrainian organizations earlier this month, according to the Ukrainian central bank, CERT and police.

- Multiple service centers of LG Electronics in South Korea were affected by ransomware. According to Korean officials, the attack is possibly the WannaCry ransomware, which struck worldwide on March.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Suspicious Executable Containing Ransomware; Suspicious Executable Containing Ransomware; Trojan-ransom.Win32.WannaCry.*, WannaCry.*)*

VULNERABILITIES AND PATCHES

- Check Point has discovered a vulnerability in the popular professional networking site LinkedIn, which could allow attackers to obfuscate malicious scripts and send them via LinkedIn's messaging platform.
- A design flaw in the CAN standard used by all modern cars has been discovered. This vulnerability allows attacks to cause denial of service to crucial components of modern cars, such as brakes and airbags. According to researchers, this flaw cannot be patched, and is invisible to current defense systems.
- Apple's iOS Secure Enclave Processor's decryption key has been publically leaked. The SEP is separate from the rest of the device, and performs the operations that involve sensitive data, such as decrypted fingerprints. According to analysts, while this may allow anyone to go over SEP's software and analyze it, attackers would still need to find vulnerabilities in this software in order to pose a threat to iOS users.
- Cisco and Drupal have released patches for security vulnerabilities in their products.

THREAT INTELLIGENCE REPORTS

- Check Point has published its mid-year report on malware trends for 2017. Ransomware was the most prevalent type of threat with 2-times the percentage from all attacks than in H1 2016. Malicious adware and mobile threats have also grown during the past year.
- A new exploit kit called Disdain was detected being advertised to attackers, and was also seen in the wild. Disdain, based on code derived from older kits, offers exploits for vulnerabilities in Mozilla Firefox, Microsoft Internet Explorer and Edge, and Flash.

  Check Point IPS blade provides protection against this threat *(Disdain Exploit Kit Landing Page)*
- Researchers have observed a large increase in Chinese online DDoS platforms. The platforms share very similar source code, names and appearance, but apparently are not run by the same actors, and sometimes even launch attacks against each other.
- A new variant of the popular Locky ransomware is being widely spread in a new malicious spam email campaign. This variant uses the .lokitus extension for encrypted files.

  Check Point SandBlast, IPS and Anti-Bot blades provide protection against this threat *(Ransomware Shared Folder Access; Suspicious Executable Mail Attachment; Suspicious Mail Attachment Containing JavaScript Code; Trojan-ransom.Win32.Locky.*)*
- An analysis of the FakeToken Android banking malware has been published. The malware is capable of accessing multiple payment apps for Android, including Google Play Store, Android Play, and several flight and hotel apps, and can even forward verification SMS messages to its C&C servers.

  Check Point Mobile Threat Prevention users are protected from this threat