April 30 - May 06, 2018

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Twitter issued an alert prompting its 300 million users to reset their passwords, following the discovery that some of its passwords had been recorded in plain text in a log file accessible by Twitter employees. The company has emphasized that no breach or misuse had been identified.

- A cyberespionage campaign dubbed ZooPark has recently been revealed. The campaign, which infects Android devices with several malware variants, has been taking place since at least 2015, focusing on Middle Eastern targets.

  Check Point Sandblast Mobile customers are protected from this threat

- LoJack, a software designed to report on laptop theft incidents, has been leveraged by the Russian threat group Fancy Bear. The application, which provides admins with remote control over the stolen computer, was unexpectedly communicating with servers that are most likely controlled by the threat group. Fancy Bear is associated with the Russian GRU military intelligence agency.

  Check Point IPS blade provides protection against this threat (Trojan.Win32. LoJack)

- A new phishing campaign is targeting Airbnb users, leveraging the upcoming General Data Protection Regulation (GDPR) privacy laws. The phishing emails lure hosts to insert their personal and financial information, through a fake message that informs users of the changes in the privacy law according to the upcoming GDPR.

- Over one million Dasan GPON home routers are now under attack, following the discovery of two vulnerabilities earlier this week. The vulnerability assigned CVE 2018-10561 may allow any attacker to access the router’s settings, thus gain control over the device, by appending a certain string to any URL. Attackers are trying to assemble the vulnerable devices into a botnet.

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

VULNERABILITIES AND PATCHES

- A review of Kernel drivers MMap handler conducted by Check Point researchers has led to the discovery and disclosure of several issues as well as an eight-year-old vulnerability in a driver that may be used for privilege escalation in the latest Kernel version.
- A critical vulnerability in Windows Host Compute Service Shim (hcsshim) library has been discovered. The flaw, assigned CVE 2018-8115, is caused by the library's failure to perform input validation when importing a Docker container image.
- Intel's Central Processor Units (CPUs) are affected by eight new hardware-level vulnerabilities, similar to the infamous Spectre flaw, which allows applications to read the Kernel memory and requires architectural changes in order to patch it. One of the vulnerabilities should be revealed by Google Project Zero this week.

THREAT INTELLIGENCE REPORTS

- Check Point Researchers have carried out an in-depth investigation into North Korea's home-grown anti-virus software, SiliVaccine. The research revealed that a key component of SiliVaccine's code is a 10-year-old copy of Japan-based Trend Micro's anti-virus, and that the program was designed to ignore one particular signature.
- Winnti, a collection of threat groups and actors linked to the Chinese state and to each other, has been highly active as of 2009, sharing the same modus operandi and targeting software and gaming organizations in the United States, Japan, South Korea and China. The consortium's primary objective is to obtain code signing certificates to sign malware for use in tailored campaigns.
- Researchers have developed a new hacking technique which executes a 'Rowhammer' attack on Android smartphones by leveraging Graphic Processor Units (GPUs), and does not rely on any software bug. In a 'Rowhammer' attack, the RAM memory cells' electrical charge is changed, and as a result the data bits are shifted from 0 to 1 and vice versa.
- Version 3 of the GandCrab Ransomware, which is sold on the dark web and distributed via several exploit kits and malspam campaigns, has been observed in the wild. Significant changes to the malware include a desktop background and an autorun key, which enable the ransomware to start automatically on reboot.

  Check Point IPS and Anti-Bot blades provide protection against this threat (suspicious executable containing ransomware; Trojan-Ransom.Win32.GandCrab)