June 4 – June 10, 2018

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A new zero-day vulnerability in Adobe Flash has been used for targeted attacks against Windows users in the Middle East, mostly diplomats, in what the researchers assess in a state-backed operation. The vulnerability allows for a maliciously crafted Flash object to execute code on victim computers, which enables an attacker to execute a range of payloads and actions. Adobe has since published a patch.

  Check Point IPS blade provides protection against this threat (Adobe Flash Player Buffer Overflow (CVE-2018-5002))

- Security researchers have warned against a sophisticated malware dubbed InvisiMole. The malware, which presents a wide array of spying capabilities, including recording audio and video from the victim's microphone and webcam, has been found only on a few dozen computers, all in Russia and the Ukraine, and researchers believe it has been created by a state-backed actor active since at least 2013.

- The Atlanta Police Department has reportedly lost years-worth of police car dash-cam videos following the March ransomware attack.

- Researchers have uncovered an espionage campaign targeting service centers in Russia. Targeted malicious emails, allegedly sent from Samsung, include spreadsheets exploiting CVE-2017-11882, a vulnerability in Office's Equation Editor. When exploited, the machine would download and execute "Imminent Monitor" - a freely available, legitimate, software that functions as a remote access Trojan (RAT), enabling the attackers to record video from the victims' webcams and monitor their activity.

- Chinese state-sponsored hackers have stolen a large amount of highly sensitive data from a U.S Navy contractor, including plans for a future anti-ship missile still under development. The leak occurred due to the fact the contractor kept the data on their unclassified network.

- A new botnet has been revealed, which has already compromised over 40,000 servers, modems and other Internet-connected devices. The campaign, dubbed "Operation Prowli" targets CMS servers, backup servers running HP Data Protector, DSL modems and IoT devices. Victim machines are monetized using a variety of methods, including cryptomining, traffic redirection and scams.

VULNERABILITIES AND PATCHES

- Security researchers have warned that an estimated 150,000 websites are still vulnerable to the "Drupalgeddon2" vulnerabilities.

  Check Point IPS blade provides protection against this threat (Drupal Core Remote Code Execution (CVE-2018-7600); Drupal Core Remote Code Execution (CVE-2018-7602))

- The Chinese firm Foscam has released firmware updates addressing three newly discovered vulnerabilities in its webcams.
- Cisco has released security patches to address severe vulnerabilities in Prime Collaboration Provisioning (PCP) solution, one of which was rated as critical.
- Google has released a Chrome update, patching a high severity vulnerability reported last May, details of which are withheld "until a majority of users are updated with a fix", as per Google. They also addressed 56 other vulnerabilities in its June Update, most prominently remote code execution vulnerabilities in the Android media framework.
- Security researchers have uncovered vulnerabilities affecting the firmware of Supermicro server products. These vulnerabilities could potentially weaken the product's preventive measures against potential tampering with their firmware.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have discovered a new strain of banking Trojan, still under development, dubbed "Karius". The malware injects additional fields into a bank's legitimate login page and sends the credentials inputted in the website to the attacker.

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

- Security researchers have warned that the Russian Cyber-Espionage group APT28 had changed its mode of operations. For several years, the group pinpointed only a handful of victims in targeted attacks that usually had a common denominator. Now, the group broads the scope of its attack to a wide group of victims, without a clear link between them, and attempts to infect them with a wide array of malware, including the Koadic remote access Trojan and the Zebrocy backdoor. The operation seems to be targeting publicly available email addresses with emails containing malicious attachments.

  Check Point Anti-Bot blade provides protection against this threat (Backdoor.JS.KoadicRAT; Trojan-Downloader.Win32.Zebrocy)