Check Point
SOFTWARE TECHNOLOGIES LTD.

July 1 - 7, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Japanese-American international convenience store 7/11 has shut down its new mobile payment app after threat actors stole $500,000 from its users. The attackers were able to perform unwanted charges on customers' accounts due to a flaw in the password reset function, which allows anyone to reset the password for other customers' accounts.

- Security researches have spotted fake Android app on Google Play named "Updates for Samsung", pretending to provide firmware updates, with over 10 million downloads. The application redirects the users to a website presenting multiple ads and tricks them into paying for firmware updates.

- A new campaign targeting Linux servers has been delivering the Golang malware, which then downloads, a Monero Cryptominer. The attack vector is robust, using several exploits and enumerating over default server credentials. The malware will also try to move laterally within the victim network.

  Check Point IPS and Anti-Virus blades provide protection against this threat *(Drupal Core Remote Code Execution (CVE-2018-7600); Atlassian Confluence and Data Center Remote Code Execution (CVE-2019-3396); ThinkPHP Remote Code Execution (CVE-2019-9082); Cryptominer.Linux.GOMiner)*

- Security researches have revealed that the Iranian cyber-espionage group APT33 is actively exploiting the Outlook vulnerability CVE-2017-11774. The vulnerability could allow the attackers to bypass security features and execute arbitrary commands on targeted machines running Windows.

  Check Point IPS blade protects against this threat *(Microsoft Outlook Security Feature Bypass (CVE-2017-11774))*

- New sextortion campaign has been spotted in the wild claiming a RAT was installed on the victim' machine by exploiting the EternalBlue vulnerability. The scammers then push the victim to pay ransom to prevent the distribution of improper videos of the victim that were captured using the alleged RAT.

- Significant jamming activity has disrupted the GPS signals in the Israeli airport "Ben Gurion" and led to severe problems to the airport's operations. The jamming activity could be linked to Russian electronic systems activity in Syria designed to protect Russia planes at their airbase in Syria.

VULNERABILITIES AND PATCHES

- Google has released the July security patch addressing 33 vulnerabilities in Android OS. Three of them are critical remote code execution vulnerabilities in the Android media framework system, which could be exploited by remote attacker to execute arbitrary code within the context of a privileged process.
- A new cross-site scripting (XSS) vulnerability has been found in the WordPress plugin WP Statistics, a site statistic analysis tool. The flaw could allow full website takeover and inject client-side scripts into websites configured with specific configurations that are not default.

  Check Point IPS blade protects against this threat *(WordPress WP Statistics Plugin Blind SQL Injection)*
- Security researches have published a proof-of-concept for a technique abusing the legitimate Microsoft Excel feature 'Power Query' to launch a remote Dynamic Data Exchange (DDE) attack and run malicious code on users' systems running Excel.

  Check Point IPS blade protects against this threat *(Microsoft Excel Power Query Remote Code Execution)*

THREAT INTELLIGENCE REPORTS

- Security researchers have exposed that the Sodinokibi Ransomware exploits a vulnerability in win32k.sys to elevate privileges on Windows machines.

  Check Point IPS Anti-Virus blades provide protection against this threat *(Microsoft Win32k Elevation of Privilege (CVE-2018-8453); Ransomware.Win32.Sodinokibi)*
- Security researches have uncovered new Lua-based backdoor dubbed "Godlua" targeting both Windows and Linux systems, which abuses the DNS over HTTPS (DoH) protocol to secure its communication channels with the command and control servers.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat *(Backdoor.Win32. Godlua)*
- Security researches have revealed that the TA505 APT has been using a new set of malware in spam campaigns embedding malicious attachments. Named "Gelup" and "FlowerPippi", the malware function as backdoors and as loaders for additional payloads including FlawedAmmyy.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat *(Trojan.Win32.FlawedAmmyy; Trojan.Win32.FlowerPippi; Trojan.Win32.Gelup)*
- The Vietnamese APT group OceanLotus has been observed utilizing a new RAT dubbed "Ratsnif" in their cyber-espionage campaigns. Ratsnif was tailored by the group to their requirements and capable of packet sniffing, ARP poisoning, DNS poisoning, HTTP injection, MAC spoofing, and more.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat *(RAT.Win32.Ratsnif)*