Check Point
SOFTWARE TECHNOLOGIES LTD.

July 8 - 14, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has exposed a new Android malware dubbed “Agent Smith”, which had infected 25M mobile devices, generating income through malicious advertisement. After installing a seemingly innocent app from Google Play Store and the third party app store “9Apps”, the malware modifies preinstalled applications to display fraudulent ads.

  Check Point SandBlast Mobile provides protection against this threat

- More than 17,000 cloud-based domains have been compromised by an attack on misconfigured AWS S3 buckets. A Magecart associated group has been modifying JavaScript files, appending skimming code designed to collect payment card data in an attack starting April 2019.

  Check Point CloudGuard provides protection against this threat

- FinSpy espionage tool, capable of stealing SMS messages, phone call recordings, emails, contacts, pictures, files and geolocations from iOS and Android mobile platforms, has been used in a campaign targeting Myanmar users. Created by German company Gamma International, the FinSpy tool has been previously associated with human-rights abuses.

- $10.6M worth of electronic equipment, $3.2M of which were of top secret military communication interception equipment, have been stolen from a US defense contractor based in Maryland in an international email scam operation. Scammers issued a purchase order using a Yahoo email address ending in “navy-mil.us” instead of the authentic “.mil” postfix. Investigation into the shipping address used resulted in the indictment of 8 people on a range of federal charges.

- La Porte County and the South Band Clinic in Indiana US have both been hit by a reportedly Ryuk ransomware attack shutting down their operations. La Porte County has agreed to pay $130,000 in Bitcoin as ransom.

VULNERABILITIES AND PATCHES

- A vulnerability in the Mac Zoom Client allows any malicious website to enable users' cameras without permission and could allow attackers to take complete control over Apple Mac computers remotely. The flaw potentially exposes 750,000 companies around the world who use Zoom to conduct day-to-day business. Both Apple and Zoom released updates addressing the issue.

  Check Point IPS blade provides protection against this threat *(Zoom Client Webcam Hijacking (CVE-2019-13450))*

- Microsoft has released its monthly software security update for July, addressing 77 vulnerabilities of which 14 are rated critical and two were found exploited in the wild. The first vulnerability, tracked as CVE-2019-1132, has been exploited by the Buhtrap threat actor in targeted attacks aimed at government organizations in Eastern Europe and was the first zero-day flaw used by Buhtrap in its operations. The Adobe monthly patch resolves vulnerabilities in Adobe Dreamweaver, Experience manager and Bridge CC, none of which are considered critical.

  Check Point IPS blade provides protection against these threats *(Microsoft Win32k Elevation of Privilege (CVE-2019-1132), Microsoft Browser Chakra Scripting Engine Memory Corruption (CVE-2019-1001), Microsoft Internet Explorer Scripting Engine Memory Corruption (CVE-2019-1004), Microsoft Edge Chakra Scripting Engine Memory Corruption (CVE-2019-1062), Microsoft Internet Explorer Memory Corruption (CVE-2019-1063), Microsoft Browser Memory Corruption (CVE-2019-1104))*

- Vulnerabilities found in General Electric's (GE) anesthesia machines (GE Aestiva and GE Aespire -- models 7100 and 7900) could allow attackers on the same network to send remote commands, change settings and modify gas composition thus placing patients in life threatening situations. GE responded saying these vulnerabilities can be avoided if the anesthesia machines aren't connected to a hospital's network.

THREAT INTELLIGENCE REPORTS

- Check Point Research has published a review of a new version of the Smokeloader botnet, which had entered the top 10 most wanted list last December. The new version includes anti-hooking, anti-Debug and anti-VM self-protection mechanisms and new persistence methods.

  Check Point SandBlast and Anti-Bot blades protect against this threat *(Trojan-Downloader.Win32.Smokeloader)*

- Britain's Information Commissioner's office has released a "notice of intent" to issue record setting fines under the EU GDRP against British Airways and Marriott hotels. BA is facing a $230M fine for compromising personal data of 500,000 customers in a 2018 data breach. Marriott is to be fined $125M for exposing 339 million customer records. Also this week, the U.S. Federal Trade Commission has reached a $5B settlement to be paid by Facebook following the 2018 Cambridge Analytica privacy scandal.