November 13 - 19, 2017

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A targeted ransomware has hit the students of J. Sterling Morton High School in Cicero, Illinois. The malware, dubbed "J. Sterling Ransomware" is disguised as a students' survey, seems to be unfinished or faulty, as it doesn't encrypt any file on infected machines once executed. The ransom note claims that the malware has encrypted the computer's files, and demand $10 in Bitcoins for decryption.

  Check Point IPS blade provides protection against this threat (Suspicious Executable Containing Ransomware).

- FOREVER-21 fashion retailer has warned its clients that it may have suffered a breach in which threat actors gained access to data of payment cards used to buy at specific FOREVER-21 stores. According to its investigation, only certain point of sale devices in some FOREVER-21 stores were affected as the encryption on those devices was not in operation.

- Kaspersky cyber-security firm has published its investigation report for the NSA cyber-tools leak by "Shadow Brokers" threat group. The report, under the title "Investigation Report for the September 2014 Equation malware detection incident in the US", rejects accusations by the Wall Street Journal alleging that Kaspersky Lab software was used to reach classified data on a home computer of an NSA-related Equation Group's employee. The report details Kaspersky's findings regarding the computer from which the cyber-tools were allegedly leaked, and mentions that it seems to have been compromised by an unknown attacker with "Smoke Loader", a Trojan sold on Russian underground forums.

  Check Point Anti-Bot blade provides protection against this threat (Operator.SmokeLoader; Trojan.Win32.Smokeloader.)*

- A new Android mobile Trojan named AsiaHitGroup was found in Google Play disguised as multiple legitimate apps, such as an alarm clock, a QR scanner, a compass app, a photo editor, an Internet speed test and a file explorer. The malware seems to be targeting victims from Asia.

  Check Point Sandblast Mobile customers are protected from this threat

VULNERABILITIES AND PATCHES

- Microsoft has released its Patch Tuesday for November. The patch addresses 53 vulnerabilities in the following Microsoft products: Internet Explorer, Microsoft Edge, Microsoft Windows, Microsoft Office and Microsoft Office Services and Web Apps, ASP.NET Core, .NET Core and Chakra Core.

  Check Point IPS blade provides protection against this threat *(Microsoft Browser Scripting Engine Memory Corruption; Microsoft Edge Scripting Engine Memory Corruption; Microsoft Edge Memory Corruption; Microsoft Internet Explorer Memory Corruption)*

- Adobe has released security bulletins for the following products: Flash Player, Photoshop CC, Connect, Acrobat and Reader, DNG Converter, InDesign CC, Digital Editions, Shockwave Player and Adobe Experience Manager. The bulletins address 86 vulnerabilities, including 70 of critical severity. The vulnerabilities may allow attackers to conduct various attacks, including arbitrary code execution.

  Check Point IPS blade provides protection against this threat *(Adobe Acrobat and Reader Use After Free; Adobe Acrobat and Reader Buffer Access with Incorrect Length Value; Adobe Acrobat and Reader Buffer Over-read; Adobe Acrobat and Reader Buffer Overflow / Underflow; Adobe Acrobat and Reader Heap Overflow; Adobe Acrobat and Reader Improper Validation of Array Index; Adobe Acrobat and Reader Untrusted Pointer Dereference; Adobe Acrobat and Reader StackExhaustion; Adobe Acrobat and Reader Type Confusion; Adobe Acrobat and Reader Out-of-bounds Read; Adobe Acrobat and Reader Security Bypass)*

- Mozilla has released security advisories for Firefox 5.7 and Firefox ESR 52.5. The advisories address 15 vulnerabilities, including 3 of critical severity which if exploited may allow arbitrary code execution.

THREAT INTELLIGENCE REPORTS

- Google has contacted app developers demanding them to show how accessibility code used in their apps is helping disabled users within 30 days, or else their apps will be removed from its Play Store entirely. This step is the latest in Google's battle against malicious apps abusing the Android accessibility services in order to infect victims.

- A new research describes the thriving collaboration between physical criminals and cyber threat actors in the stolen Apple devices market. According to the research, threat tools used to jailbreak Apple devices and run stolen devices, as well as phishing attacks used to hijack iCloud and Apple ID accounts, are developed and run by threat actors and being used by fraudsters trading with stolen devices. Such collaboration allows criminals to bypass Apple's dense defenses.

- Researchers have spotted a new version of Emotet banking Trojan. The malware features improved anti-sandbox and anti-analysis capabilities, and new Windows API hijacking capabilities. The malware is being distributed via phishing emails containing malicious URLs from which the malware is downloaded.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Microsoft Office Files Containing Malicious VBScript Downloader; Trojan.Win32.Emotet.*)*