August 28 - September 3, 2017

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Instagram has suffered a breach in which personal data of 6 million accounts was leaked and offered for sale on Doxagram. The attack was made possible due to a critical API vulnerability in Instagram, which has since been patched. On a similar note, Selena Gomez's Instagram account was recently compromised, allowing the attacker access to intimate pictures of her ex-boyfriend Justin Bieber.
- Researchers have revealed a new backdoor attributed to Turla APT, used to spy after embassies worldwide. The backdoor, named Gazer, is advanced and stealthy, and is capable of staying persistent on infected machines.

  Check Point Anti-Bot blade provides protection against this threat (Operator.Gazer)
- The US-CERT has warned users from threat activity disguised as related to hurricane Harvey. According to the warning, threat actors may distribute malware via links/emails seemingly related to the hurricane, or conduct web scams via fake donation requests.
- CeX, a major second-hand online marketplace, has suffered a breach exposing private information of approximately 2 million users. According to the announcement, no financial data was accessed.
- The American Internal Revenue Service (IRS) has warned from phishing scams impersonating the IRS and the FBI as part of a ransomware campaign. The scam includes a message, allegedly sent by both federal organizations, calling recipients to download a questionnaire that turns out to be a ransomware.
- Real Madrid's Twitter account has been compromised and used for a prank – the attackers tweeted that Real Madrid has signed Lionel Messi, rival Barcelona's superstar.
- A new social engineering campaign named "Roboto Condensed" is targeting Chrome and Firefox users, redirecting them in various ways to malicious domains showing a popup message claiming that they are missing the "Roboto Condensed" font, and therefore the website cannot be presented properly. Then, the victims are tempted to download the "missing" font, which turns out to be a malware downloader.

VULNERABILITIES AND PATCHES

- Researchers have revealed a flaw in major web-browsers which may allow attackers to expose web-extensions used by victims. This security flaw can be abused in various ways; from advertising to targeted malware distribution.

- A research sheds light on 6 new vulnerabilities in mobile bootloaders of major vendors. The vulnerabilities may allow various attacks on vulnerable devices, such as breaking the Chain-of-Trust (CoT), running arbitrary code, and denial-of-service.

THREAT INTELLIGENCE REPORTS

- WikiLeaks has revealed another cyber-tool under its "Vault7" project. According to the leak, the tool, dubbed Angelfire, is a CIA multi-component implant used to load and execute any program on target machines running Windows 7 or XP OS. Angelfire includes a component that modifies the partition boot sector of the victim machine, and is entirely encrypted and obfuscated in order to avoid detection.

- A new variant of BTCWare ransomware has recently been discovered. In this new variant there’s no way to decrypt some files, especially large ones, even if the ransom payment is made.

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

- Rig exploit kit is now distributing a ransomware called “Princess Locker”.

  Check Point IPS blade provides protection against this threat (RIG Exploit Kit Landing Page URL)

- According to a new research, IoT devices’ internet communication can risk users’ privacy, even if it’s encrypted. The research demonstrates how passive network adversary can infer private in-home user activities and allow an outside observant to track the IoT devices’ users. The research suggests using traffic shaping in order to address this issue.

- A new research describes the increase in mobile ransomware attacks. According to the research, the first half of 2017 demonstrated a 390% growth in mobile ransomware attacks relatively to the equivalent period in 2016. The research also emphasizes the technical development of mobile crypto-ransomware since their appearance in May 2014.

- A 711 million email records spam-bot dump has been revealed online. The data set includes email addresses, passwords, SMTP servers’ credentials and other sensitive information used for spam distribution. It is not clear where the different records originate from, and yet, it demonstrates well how powerful the modern spam-bots are.

  Check Point Anti-Bot blade provides protection against this threat (Trojan.Win32.Spambot.)*