November 19-25, 2018

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Over 6,500 dark web services hosted on Daniel's Hosting, one of the largest Dark Web hosting providers, have been taken down with no recovery option, after hackers targeted the hosting service and deleted all of its data and hosting database.
- A new Emotet Thanksgiving-themed campaign has been observed in the wild, targeting U.S email accounts. The campaign is using improved macro obfuscating and formatting methods embedded in email attachments to run an upgraded variant of the infamous Trojan.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Win32.Emotet)
- 13 fraudulent mobile applications disguised as games were found on Google Play with over 500,000 installations. Once installed, the fake applications would attempt to download another application that will push unwanted ads to the user whenever they unlock the device, and gain full network access.

  Check Point SandBlast Mobile customers are protected from this threat
- A new spam campaign has been targeting users of Exodus cryptocurrency wallet for macOS, and distributing a spyware. The spyware is delivered via malicious mail attachments, urging users to run them in order to update their wallets to the most recent version.
- Software company OSIsoft has suffered a security breach affecting all of its domain accounts. The attackers used stolen credentials to remotely access the company's computers, reportedly extorting personal user credentials of 135 accounts.
- The North Korean APT group Lazarus has been involved in several attacks targeting banks in Latin America. These attacks seem to be part of the group's latest activities involving their ATM malware tracked as FastCash Trojan.

  Check Point Anti-Virus blade provides protection against this threat (Trojan.Win32.FASTcash)

VULNERABILITIES AND PATCHES

- New zero-day vulnerabilities have been found in fully patched iPhone X, Samsung Galaxy S9 and Xiaomi Mi6. The disclosed vulnerabilities may allow attackers to compromise the target device via its browser or Wi-Fi, most of them without any user interaction.
- The US postal service has patched a critical vulnerability in its API for the USPS "Informed Visibility" program, exposing data of more than 60 million users. The vulnerability allows anyone who has an account at usps.com to view and modify account details for other users.
- 7 New variants of Meltdown and Spectre attacks have neem found leveraging a CPU technique known as “transient execution”. These attacks affect Intel, AMD and ARM CPU processors, and may allow attackers to obtain sensitive user information.
- A vulnerability in German eID cards has been discovered, residing in the Radio Frequency Identification (RFID) chip of the card. The vulnerability allows attackers to obtain sensitive information, alter the data of the card holder and distort the validation process.

THREAT INTELLIGENCE REPORTS

- Security researchers have discovered a new malware dubbed “Cannon”, attributed to the Russia-linked APT group, Sofacy. Cannon was used in recent spear phishing campaigns weaponized with malicious documents, targeting government entities in North America, Europe and in a former Soviet state.

  Check Point SandBlast provides protection against this threat
- More than 10 new Mirai botnet variants have been spotted, attempting to exploit the recently disclosed command injection flaw in Hadoop YARN on Intel servers. These Mirai variants are tailored to run on Linux servers and are the first that do not target IoT devices.
- A flaw on Instagram has led to the exposure of user passwords in plain text while using the new “Download Your Data” feature. The passwords appeared in the URL and stored on Facebook’s servers.
- A new Bluetooth attack technique called CarsBlues has been found, potentially affecting millions of vehicles. The technique allowing attackers to access user’s personal information by leveraging security flaws in entertainment systems installed in modern cars that enable syncing smartphones via Bluetooth.
- Security experts have managed to gain full access to Apple`s macOS devices by chaining together three zero-day vulnerabilities that have been patched separately by Apple in the past year. The chained exploits have allowed penetrating the OS by deceiving a user to browse to a malicious website.