December 3 - 9, 2018

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Signet Jewelers, the world's largest retailer of diamond jewelry, has fixed a massive bug that allowed public access to customer data, including billing and shipping address, phone number, email address, purchased items and the last four digits of customer credit card numbers.

- Eastern Europe banks are the main targets of a new campaign dubbed DarkVishnya, which is based on direct connection of a removable device to the targeted network. The device is connected by an actor disguised as a visitor, and observed devices include a cheap laptop and Bash Bunny, a tool used to carry out USB attacks.

  Check Point Anti-Virus blade provides protection against this threat *(RemoteAdmin.Win32.DameWare)*

- The threat actor behind vast Dridex banking Talware and Locky ransomware campaigns, has been carrying out an email campaign targeting large retail, dining and grocery chains. The campaign uses personalized attachments, tailored to the targeted organization.

  Check Point SandlBlast and Anti-Bot blades provide protection against this threat *(Trojan.Win32.Dridex; Trojan-Ransom.Win32.Locky)*

- DanaBot, a banking Trojan targeting Australian users, has recently shifted its focus to spam mail distribution. The malware is harvesting email credentials in order to send spam content from the compromised mailboxes as replies to actual messages in the inbox.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Trojan-banker.Win32.Danabot)*

- A new hybrid malware targeting Mac computers has been observed, spread via a decoy version of Adobe Zii, a software used to activate cracked Adobe programs. The malware combines open-source tools – the XMRig cryptocurrency miner and the EmPyre backdoor.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat *(Trojan.WIN32.XMRig; Backdoor.Win32.EmPyre)*

VULNERABILITIES AND PATCHES

- A new zero-day vulnerability in Adobe Flash Player has recently been utilized in a targeted attack against a Russian research facility. The vulnerability, assigned CVE-2018-15982, was exploited via a Word questionnaire with an embedded Flash object, and was delivered inside a WinRAR archive.
- A security researcher has published an exploit for a vulnerability in WebKit, the web browser engine of Safari and other Apple applications. The exploit leverages an optimization error leading to arbitrary code execution on vulnerable devices, impacting the iOS and MacOS versions of the Safari browser.
- Threat actors have recently utilized a vulnerability in Mozilla Firefox browser which was first reported on 2007. The bug leads to the appearance of an authentication modal in a loop, preventing users to leave the website. Actors are using it to push victims into purchasing shady products and services.
- Apple has released a security update for multiple products including iTunes, iCloud and the latest iOS version, 12.1.1. The update features patches for remote code execution (RCE) and privilege flaws, including a fix for a bug that allows access to an iPhone user's contacts while the device is locked.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have discovered a unique new service in the ransomware landscape. A Russian company named 'Dr. Shifro' claims to legitimately provide file decryption to ransomware victims, though in fact it pays the ransomware's author, passing on the cost to the victim with a massive profit margin.
- A report analyzes several of the most prominent threats dominating the current cyber landscape, including Emotet and Trickbot banking malware and PowerShell attacks. The report covers the distribution, key features and expected evolution of these threats.
- Researchers have reviewed the most common threats and attack methods used by cybercriminals during the western holiday season, including gift card related email fraud, Point-of-Sale malware and social media support scams.
- The 2018 APT landscape has been dominated by both steady, long-operating groups and new actors, according to an annual report. The notorious Russian-speaking Sofacy group stood out with campaigns targeting embassies and EU agencies, and new groups, including the Iranian Domestic Kitten, focused mainly on Middle East and South East Asia targets.
- Formjacking is a technique used to steal payment information from checkout web pages of e-commerce portals via a malicious JavaScript code.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Magecart)