Check Point
SOFTWARE TECHNOLOGIES LTD.

July 17 - 23, 2017

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A vulnerability in Parity's Ethereum wallet software has led to the theft of $30M worth of Ethereum cryptocurrency coins. Parity's wallet software provides Ethereum coins holders the ability to access their wallet comfortably via a web-browser. The vulnerability that was exploited in the attack allowed threat actors to hijack victims' wallets and conduct fraudulent transactions using them. In a different event, a threat actor has managed to steal $7M in Ethereum coins by compromising a website used for Ethereum payments in an Initial Coin Offering (ICO) of the Blockchain startup CoinDash. The attacker behind the operation has changed the address of the payment Ethereum wallet in CoinDash's website, thus manipulating transactions into his own wallet.

- Security researchers have found an adware called Stantinko that was being used by its authors as a browser hijacker. Infection vector is through bundling the adware with freeware intentionally downloaded by users. The main usage of the adware is for click fraud, but it has also been witnessed to conduct brute-force attacks against Joomla and WordPress sites. According to the researchers, Stantinko has been in the wild for the past 5 years and managed to infect over 500,000 users.

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

- Gandi, a web services provider, has revealed that a security incident had led to the modification of the DNS records of 751 domains in a way that redirected victims' traffic into a malicious site containing an exploit kit. Gandi's technical team managed to repair the records within several hours.

  Check Point IPS blade provides protection against this threat (Neutrino Exploit Kit Landing Page Code Execution; RIG Exploit Kit Landing Page)

- Security researchers have found new evidence for a spear-phishing campaign dubbed Inexsmar, originating from the well-known threat actor group DarkHotel. The evidence show that in this campaign the group moved from targeting CEO'S to political figures.

VULNERABILITIES AND PATCHES

- A new exploit, based on one of the NSA's exploits "ETERNALSYNERGY", has been built and published by a security researcher. The exploit is targeting Windows operating systems and contains an upgraded exploitation mechanism of the known vulnerability dubbed CVE-2017-0143 that exists in SMB V1.

  Check Point IPS blade provided protection against this threat (Microsoft Windows EternalSynergy SMB Remote Code Execution)

- Security researchers have found a new buffer overflow vulnerability dubbed Devil's Ivy in the gSOAP development platform for various IoT devices, which can potentially put thousands of devices at risk.

- A remote code execution vulnerability in Cisco's WebEx browser extensions for Chrome and Firefox has been reported and patched.

  Check Point IPS blade provided protection against this threat (Cisco WebEx Chrome Plugin Remote Code Execution)

- Apple has released security updates for multiple of its products. One of the main bugs that were fixed is the Broadpwn bug, which allows attackers to take over iOS devices that utilize Broadcom WiFi chipsets.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have spotted a new spam email campaign. The emails included malicious zipped js files and communicate with numerous C&C domains that quickly change to avoid blacklisting. To evade detection, the js also includes Wikipedia entries describing different cities and countries.

  Check Point SandBlast and IPS blades provide protection against this threat (Suspicious Mail Attachment Containing JavaScript Code)

- Check Point researchers have published the "most wanted malware" for June. According to the report, 28% of organizations globally were affected by the RoughTed malvertising campaign during this month.

  Check Point IPS blade provides protection against this threat (RoughTED Exploit Kits Traffic Distribution System)

- A new ransomware called Reyptson was recently spotted in the wild targeting Spanish victims. The malware distributes itself by abusing victims' email accounts active on Thunderbird in order to send spam emails with malicious attachments to victims' contacts.

  Check Point IPS blade provides protection against this threat (Suspicious Executable Mail Attachment)

- Security researchers have spotted a campaign targeting Linux devices with older versions of the Samba file-sharing server, using SHELLBIND, a malware exploiting a known vulnerability called SambaCry.

  Check Point IPS blade provide protection against this threat (Linux EternalRed Samba Remote Code Execution (CVE 2017 7494))