September 18 - 24, 2017

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The FBI and Montana's security forces are investigating a threat operation in which an attacker has breached Columbia Falls Schools District servers. The attacker has gained phone numbers and contact information of students, parents and staff members, and sent them threatening messages. Following the attack, classes were canceled for a couple of days in all 30 schools of the district. The school district officials have received a related ransom note demanding between 75-150K dollars in a few payments proposals. The ransom note is signed after TheDarkOverlord threat group, which is considered to be responsible for the HBO and Netflix breaches earlier this year.

- CCleaner, an anti-potentially-unwanted-programs (PUP) freeware, was lately breached and abused. The program, developed by Avast-owned Piriform, was modified by the attacker so it will insert a backdoor into infected machines, allowing the attacker to run any code. In response to the attack, Piriform has pushed an automatic update for CCleaner in order to disarm the threat and remove the backdoor.

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

- LiteBit, a Dutch cryptocurrency broker, has been breached. The breach is LiteBite's seconds within a couple of months. According to the LiteBite's announcement, the attackers had gained access to private information of its customers, not affecting the servers containing the crypto-wallets.

- The Pirate Bay website, the most popular torrent-downloads websites worldwide, has been found to be using visitors CPU in order to run a Monero cryptocurrency miner. After the issue was exposed, The Pirate Bay released a public announcement claiming that the crypto-mining was a test aimed to check whether it can replace advertising as a way to fund the website's activity.

  Check Point IPS blade provides protection against this threat (Multiple Websites Mine Cryptocurrencies CPU Hijacking)

- Login credentials for approximately 540K records belonging to the vehicle tracking device company SVR Tracking have been leaked online. The data may allow threat actors to access to private information of the company's users, as well to data related to cars tracked by SVR's tracking device.

VULNERABILITIES AND PATCHES

- A vulnerability in Apache has been revealed and dubbed Optionbleed, enabling attackers to get memory dumps out of Apache web servers. This vulnerability is similar to Heartbleed, only less robust.

  Check Point IPS blade provides protection against this threat (Apache HTTP Optionsbleed Memory Leak(CVE 20179798))

- Apple has released security updates for the following products: iOS 11, Safari 11, tvOS 11, watchOS 4, Xcode 9. The updates address 22 different vulnerabilities that may be exploited for various types of attacks, and some of which may allow an attacker to conduct remote code execution.

- Joomla! has released Joomla! 3.8, which includes 2 fixes for medium severity vulnerabilities that may allow attackers to conduct information disclosure attacks.

  Check Point IPS blade provides protection against this threat (Joomla LDAP Information Disclosure (CVE-2017-14596))

- Samba has released security patches for several Samba versions. The patches address 3 vulnerabilities which may allow an attacker to conduct man-in-the-middle attacks.

- WordPress has released WordPress 4.8.2 security update. The release addresses 9 vulnerabilities, 5 of which are cross-site-scripting (XSS) vulnerabilities.

  *Check Point IPS blade provides protection against this threat (SQL Servers *; Cross-Site Scripting Scanning Attempt)*

- Cisco has released security updates for various products addressing critical remote code execution and authentication bypass vulnerabilities, among others.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have recently discovered a free mobile anti-virus app developed by the DU group, which collects user data without the device owner's consent. The application, called DU Antivirus Security, has been downloaded between 10 and 50 million times, according to Google Play data.

  Check Point Sandblast Mobile customers are protected from this threat

- Researchers have revealed a new banking Trojan named Red Alert 2.0, targeting Android mobile devices. Along with usual mobile banker capabilities, e.g. overlay attacks and SMS control, it demonstrates new functions as blocking or manipulating incoming calls from banks, thus disrupting anti-fraud processes.

- A new report sheds light on the activity of APT33, a threat group attributed to Iran, according to which APT33 was found targeting multiple sectors in the US, Saudi Arabia and South Korea. The report suggests that the threat group's recent activity is made for intelligence purposes, as well as industrial espionage.

  Check Point IPS and Anti-Bot blades provide protection against this threat (PowerShell Script Encoding Evasion; Malicious VBScript In HTML; Trojan.Win32.NanoCore., Backdoor.Win32.NetWiredRC.*)*