Check Point
SOFTWARE TECHNOLOGIES LTD.

July 30 – August 5, 2018

YOUR CHECK POINT
# THREAT INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- Reddit has suffered a major data breach, as threat actors managed to gain access to its users' data, and a 2007 backup database containing usernames and hashed passwords. The attack was carried out by intercepting the two-factor authentication codes sent via SMS to Reddit's employees.

- KICKICO, a blockchain-based initial coin offering (ICO) platform has fallen victim to a security breach, and $7.7 million worth of KICK tokens were stolen from it. Threat actors gained access to the smart contract of the project's blockchain network by obtaining the private key, which eventually allowed the attackers to steal KickCoins from the users' wallets.

- Dixons Carphone, the giant electronics and telecommunication retailer, has announced that its breach, discovered in June 2017, affected 10 million customers. The stolen data includes names, addresses and email addresses, as well as 6 million payment cards used at Currys PC World and Dixons Travel.

- Security researchers have uncovered a massive cryptojacking campaign compromising tens of thousands of MikroTik routers. The attackers behind the campaign use a known zero-day MikroTik flaw to change the configuration of the devices and inject a Coinhive crypto mining script into the users' web traffic.

  *Check Point IPS and Anti-Bot blades provide protection against this threat* *(Multiple Websites Mine Cryptocurrencies CPU Hijacking; Trojan.WIN32.CoinHive.*)*

- Security researches have revealed a surgical spear-phishing campaign targeting entities in the industrial sector. The campaign uses phishing emails with malicious attachments or links delivering a legitimate remote administration software - TeamViewer or Remote Manipulator System/Remote Utilities (RMS).

  *Check Point SandBlast and Anti-Virus blades provide protection against this threat* *(Trojan.BAT.Starter; Trojan.Win32.Dllhijack; Trojan.Win32.Waldek; Backdoor.Win32.RA-based; Backdoor.Win32.Agent )*

- Three members of the notorious cybercrime group known as 'FIN7' and 'Carbanak' have been arrested. The group targeted American companies and citizens by stealing valuable consumer data, including personal credit card information, and is responsible for the loss of tens of millions of dollars.

## VULNERABILITIES AND PATCHES

- Drupal, the popular open-source content management system, has released a new software version to address a security bypass vulnerability in the 'Symfony HttpFoundation' component used for the 'Symfony' web application framework, which may allow to take full control of affected Drupal websites.
- A Same-Origin Policy (SOP) - related vulnerability has been patched, affecting the Microsoft Edge browser. Exploiting the vulnerability may allow manipulating the SOP security feature, allowing attackers to collect and steal any data from the local files on the victim's machine.
- Security researchers have discovered about 20 flaws in Samsung SmartThings Hub controller, used to manage a broad range of internet-of-things (IoT) devices in a smart home. These vulnerabilities potentially expose any supported third-party smart home device to cyber-attacks.

## THREAT INTELLIGENCE REPORTS

- Check Point researchers have discovered a new massive campaign of Ramnit Banking Trojan dubbed 'Black', reaching over 100,000 infections in the course of two months. According to the report, the main purpose of the campaign is to use the victims' machines as malicious proxy servers.
- Check Point researchers uncover a huge malvertising campaign that starts with thousands of compromised WordPress sites, leverages ad-bidding platforms and ends with distributing malicious content via multiple exploit kits, to online users everywhere.
- Check Point security researches have published an in-depth report, revealing that the 'Osiris' Banking Trojan highly resembles 'Kronos' banking Trojan – the two share the same capabilities of persistence, encryption, anti-VM, anti-sandboxing and more, and probably have the same author.

  *Check Point SandBlast, Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan-Banker.Win32.Osiris; Trojan-Banker.Win32.Kronos)*
- New version of AZORult data stealer and downloader has been spotted in the wild with sophisticated improvements including the ability to steal histories from non-Microsoft browsers, and support for stealing credentials to Exodus, Jaxx, Mist, Ethereum, Electrum and Electrum-LTC cryptocurrency wallets.

  *Check Point SandBlast, Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Win32.AZORult; Trojan-Ransomware.Win32.Hermes)*
- Security researches have published an updated analysis of the Telegram-based Android RAT dubbed 'HeroRAT', describing its unique characteristics in comparison to other RATs leveraging the Telegram BOT API for communication with C&C.

  *Check Point SandBlast Mobile customers are protected from this threat*