April 2 - 8, 2018

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

# THREAT INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- Several Natural gas pipeline operators in the United States have suffered a cyber-attack on their electronic systems. The attacks targeted the companies' Electronic Data Interchange (EDI) system which controls sensitive document exchange, and led to the shutdown of their communication systems.
- The New Business Center in Helsinki, Finland, has fallen victim to a major data breach. Actors have stolen over 130,000 users' login usernames and passwords, which were stored on the site in plain-text.
- Several cyber-attacks, including one against an online casino in Central America, have been attributed to the North Korean APT Group - Lazarus. The link has been made due to the use of similar hacking tools which belong to Lazarus in all of the incidents, including the KillDisk disk-wiper.
- Threat actors have compromised over 1,000 ecommerce websites running on the open-source Magento platform. The threat actors have used brute-force attacks to access administration panels, to steal credit card numbers, and to install crypto-mining malware.

  *Check Point IPS blade provides protection against this threat* *(Suspicious Multiple Browsers Fake Update; Web Login Form Password Brute Force Attempt)*

- A new variant of the Mirai Botnet has been used to launch a series of DDoS attacks against the financial industry. The attacks utilized at least 13,000 hijacked IoT devices generating traffic volumes up to 30 Gbps. The variant uses IoTroop code that allows the malware to be updated online.

  *Check Point IPS blade provides protection against this threat* *(AVTECH Devices Multiple Vulnerabilities; Wireless IP Camera (P2P) WIFICAM Cameras *; Linksys WRH54G HTTP Management Interface DoS Code Execution - Ver2; Belkin Linksys WRT110 Remote Command Execution; Cisco Linksys PlayerPT ActiveX Control SetSource sURL Argument Buffer Overflow; MikroTik RouterOS *; Synology DiskStation Manager SLICEUPLOAD Code Execution; TP-Link Wireless Lite N Access Point Directory Traversal; TP-LINK WR1043N Multiple Cross-Site Request Forgery)*

- Facebook has announced that public profile information of its 2.2 billion users has been compromised through a flaw in the search function that allows finding users via their email address or phone number.

## VULNERABILITIES AND PATCHES

- A critical flaw has been disclosed in the Smart Install feature of Cisco IOS Software and Cisco IOS XE Software, affecting thousands of Cisco switches, allowing unauthenticated remote attackers to execute arbitrary code, take full control over vulnerable network equipment, and intercept traffic. Iranian and Russian networks have been compromised by exploiting this flaw to reset routers to the default settings.

  *Check Point IPS blade provides protection against this threat* *(Cisco Smart Install Remote Code Execution (CVE-2018-0171))*

- Microsoft has issued an out-of-band patch to fix a vulnerability in the Malware Protection Engine.

  *Check Point IPS blade provides protection against this threat* *(Microsoft Malware Protection Engine Remote Code Execution(CVE-2018-0986))*

- A critical authentication bypass vulnerability has been discovered in the identity platform "Auth0", affecting over 2,000 enterprises, which may allow attackers to access victims' portals and applications.

## THREAT INTELLIGENCE REPORTS

- Check Point security researchers have uncovered new variants of the Fetsi rootkit, distributed by RIG exploit kit. This rootkit had been silent since the arrest of its developer.

  *Check Point IPS, Anti-Bot and Anti-Virus blades provide protection against this threat* *(RIG Exploit Kit *; Suspicious Multiple Browsers Fake Update; Trojan.Win32. Fetsi)*

- A new strain of Android crypto-miner dubbed "AndroiDos HiddenMiner" has been spotted in the wild, delivered through a fake Google Play update app, exhausting the device's resources in mining Monero.

  *Check Point Sandblast Mobile customers are protected from this threat* *(Trojan.Android.HiddenMiner)*

- New variants of the Android remote administration tool (RAT) "KevDroid" are being distributed in the wild, disguised as a fake anti-virus application dubbed "Naver Defender". The variants are capable of stealing sensitive information from compromised devices, recording phone calls and gaining root access.

  *Check Point IPS blade provides protection against this threat* *(Microsoft Office Memory Corruption Remote Code Execution (CVE-2017-11882)*

- Security researchers have discovered that 10 of 15 of Chrome VPN extensions leak DNS queries that are made via Chrome's 'DNS prefetching' system. 'DNS prefetching' helps Chrome reduce latency delays of DNS resolution time by performing DNS request before the user clicks on a link.

- During an in-depth research about the infamous "LockCrypt" Ransomware, security researchers have revealed a flaw in its code that can allow recovery of a victim's data.

  *Check Point IPS and Anti-Bot blades provide protection against this threat* *(Suspicious executable containing ransomware; Trojan-ransom.Win32.Lockcrypt)*