March 26 - April 1, 2018

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Aerospace company Boeing has fallen victim to a WannaCry ransomware attack. The company announced that the infection was limited to a few machines; however, earlier reports spoke about the infection spreading quickly throughout their network. Researchers suspect it may mean their operating system has been outdated, lacking important patches.

  Check Point SandBlast, IPS and Anti-Bot blades provide protection against this threat *(Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-014*); Microsoft Windows Eternal* SMB Remote Code Execution; Microsoft Windows DoublePulsar SMB Remote Code Execution; Malicious network activity; WannaCry; Trojan-Ransom.Win32.WannaCry.*)*

- Security researchers have reported that the Hajime IoT Botnet had resurfaced, performing extensive scans in an attempt to infect unpatched MikroTik devices. In the last three days of March, 860,000 scans were detected. The bot attempts to exploit a newly discovered vulnerability that affects MikroTik RouterOS firmware 6.38.4 and earlier, and allows attackers to execute code and take over the device.

  Check Point IPS blade provides protection against this threat *(MikroTik RouterOS SMB Remote Code Execution (CVE-2018-7445))*

- The dispatch system of the emergency and the municipal services of the city of Baltimore have suffered a cyber-attack and were taken down for 17 hours, forcing the dispatch system to resort to manual reporting and delaying dispatches. The attack method appears to be similar to that suffered by the city of Atlanta last week - a SamSam ransomware attack.

  Check Point IPS blade provides protection against this threat *(Suspicious executable containing ransomware)*

- A new malware dubbed Fauxpersky is being spread via infected USB drives and masquerading as Kaspersky Anti-Virus. Logged keystrokes are sent to the malware operator via a Google form, which has since been taken down by Google.

- Fitness company Under Armour has announced that a breach had exposed the data of 150 million users of its MyFitnessPal app, including user names, email addresses and hashed passwords.

VULNERABILITIES AND PATCHES

- Security patches for OpenSSL have been released for the first time in 2018, patching three low to moderate severity issues.
- Content-management company Drupal has released a patch for a "highly critical" flaw in versions 6, 7 and 8 of its CMS platform that could allow an attacker to take control of an affected site simply by visiting it. The flaw is estimated to affect over a million websites.

  Check Point IPS blade provides protection against this threat *(Drupal Core Remote Code Execution (CVE 2018 7600))*
- Microsoft has released a fix to a problematic patch for the Meltdown vulnerability, released last January. While securing the system against Meltdown, the patch inadvertently created a Windows kernel privilege elevation vulnerability.

  Check Point IPS blade provides protection against this threat *(Meltdown/Spectre Multiple Browsers Speculative Execution)*
- Cisco has released three patches for critical flaws in their IOS and IOS XE. The company recommends patching immediately.

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

THREAT INTELLIGENCE REPORTS

- Academic researchers have discovered a new side channel attack that takes advantage of the speculative execution feature in modern processors to recover data from users' CPUs. While mostly similar to the Meltdown and Spectre flaws, the attack targets a new section of the speculative execution process. The researchers claim they have successfully tested their method on Intel's Sandy Bridge, Haswell, and Skylake processors.
- The delivery method of the SANNY malware has recently been updated into a multi-stage delivery, each stage downloaded from the attackers' server. The first stage includes a fake-document pretending to be of interest to the victim, usually a government entity. SANNY is suspected to be attributed to a group targeting Korea and diplomatic entities worldwide.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Microsoft Office Files Containing Malicious VBScript Downloader; Trojan.Win32.Sanny)*
- Security researchers have announced that AutoHotKey-based malware is on the rise. The programming language, used mostly for Windows keyboard shortcuts and online-games cheating bots, has recently become a popular language for malware developers, with researchers discovering clipbankers, droppers and keyloggers in the wild.