April 16 - April 22, 2018

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Security researchers have revealed a sophisticated Internet Explorer zero-day vulnerability being exploited by an APT group, through an embedded component in Microsoft Word documents sent to a limited number of targets. This so called “double-kill” vulnerability affects the latest versions of Internet Explorer and any other applications that might utilize IE components. Once the malicious Office document is opened, the exploit code and malicious payloads are loaded from a remote server.

- Security researchers have identified a threat group dubbed “Orangeworm”, active since at least 2015 and targeting the global healthcare industry, including medical device manufacturers, IT firms that provide services to clinics, and logistics companies that deliver healthcare products. Victim are infected with a backdoor Trojan, and if after gathering initial information the victim is deemed to be of interest, the backdoor spreads though the organization’s network. The attackers’ endgame is still unclear.

- Russian authorities have declared a ban on the instant messaging application “Telegram”. As part of this effort, Russia blocked approximately 15 million IP addresses belonging to Google and Amazon, preventing access to Telegram content hosted by these services. Russian users are attempting to avoid the ban by using VPNs and proxies.

- Researchers have reported on a new malware distributed via the painting application ‘StressPaint’, allegedly meant to relief stress. The malware collects Facebook credentials and payment information and is spread via phishing emails manipulating the victims to download the application. Over 40,000 Facebook users have already been infected.

- Researchers have reported that the recovery efforts made by the city of Atlanta following the ransomware attack it suffered during March are estimated in at least $2.7M, whereas the requested ransom was $51,000.

  Check Point SandBlast, IPS and Anti-Bot blades provide protection against this threat (Suspicious Executable Containing Ransomware; Ransomware.Win32.Samsam.)*

VULNERABILITIES AND PATCHES

- Researchers have uncovered a flaw in the process of pairing iPhone devices with Mac workstations or laptops. The flaw, named 'Trustjacking', may allow attackers to take over the paired iPhone device without the phone owner's knowledge. The issue lies in the 'iTunes Wi-Fi sync' feature, which grants the paired computer access permission even after the iPhone device has disconnected from the computer.
- A remote code execution vulnerability in Spring Data Commons has been disclosed.

  Check Point IPS blade provides protection against this threat (Pivotal Spring Commons Remote Code Execution (CVE-2018-1273)
- A researcher has revealed a detailed proof-of-concept code capable of bypassing Windows 10 security features. The flaw that enables the bypass resides in the behavior of a .NET object within the Windows Lockdown Policy (WLDP), and affects Windows 10 machines with User Mode Code Integrity enabled.

  Check Point IPS blade will provide protection against this threat in its next online package
- Oracle has published its critical patch update for April, offering 254 security fixes across 20 product sets, including Oracle Communications Applications, Oracle Database Server and Oracle E-Business Suite.

  Check Point IPS blade provides protection against this threat (Oracle WebLogic WLS Core Component Remote Code Execution (CVE-2018-2628))

THREAT INTELLIGENCE REPORTS

- Security researchers have reported on a shift of a large-scale botnet dubbed "Muhstik" into exploiting the recently discovered Drupal CMS vulnerability Drupalgeddon 2. The botnet, usually used for DDoS or cryptomining, now scans systems for Drupalgeddon 2 and executes commands on those found vulnerable. In addition, the botnet has increased its targeting of Oracle WebLogic systems.

  Check Point IPS blade provides protection against this threat (Drupal Core Remote Code Execution (CVE-2018-7600); Oracle WebLogic WLS Security Component Remote Code Execution (CVE-2017-10271); Malicious Crypto Miner Downloader)
- Security researchers have warned that steganography-based hacking tools, nicknamed "Stegware", are becoming increasingly popular in Dark Web hacker forums. These tools are based on embedding malicious data within fake images command-and-control, data exfiltration and as an encryption alternative to sending secret messages.

  Check Point IPS blade provides protection against this threat (Steganography Over JPEG; PNG Containing Malicious JavaScript Code)
- Security researchers have announced that millions of apps potentially leak personal user information such as name, age, income and possibly phone numbers and email addresses, through ad-targeting data transmitted to third-party advertisers unencrypted, over HTTP.