April 22 - 28, 2019

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point researchers have uncovered a targeted attack against officials within government finance authorities and representatives in several embassies in Europe. The attack, which starts with a malicious attachment disguised as a top-secret US document, weaponizes TeamViewer, the popular remote access and desktop sharing software, to gain full control of the infected computer.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat

- A cryptojacking campaign dubbed "Beapy" is targeting enterprise networks in China, leverages the NSA's leaked DoublePulsar backdoor and EternalBlue exploit to spread a file-based cryptocurrency malware.

  Check Point SandBlast, IPS, Anti-Bot and Anti-Virus blades provide protection against this threat (Microsoft Windows DoublePulsar SMB Remote Code Execution; Microsoft Windows EternalBlue SMB Remote Code Execution; Cryptominer.Win32.Beapy)

- Security researches have uncovered a new campaign conducted by the Russian hacking group called 'Gamaredon'. The campaign targeted Ukrainian military personnel in an espionage operation camouflaged as an internal document of the Defense Ministry dated to April 2nd 2019.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Dropper.Win32.Gamaredon)

- The city of Stuart has fallen victim to a Ryuk Ransomware attack which also included the Trickbot Trojan. The attack infected several servers and systems and forced them offline.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Trojan-Ransom.Win32.Ryuk; Trokan-Banker.win32.Trickbot)

- Docker Hub database has been hacked, exposing sensitive data of more than 190,000 users including usernames, hashed passwords, and keys and tokens for GitHub and Bitbucket repositories.

- Millions of medical documents belonging to addiction and recovery patients were exposed online due to an unsecured ElasticSearch database. The information includes data on all rehab treatments and procedures, linked with patients' names, bills, location in which the treatment was given and more.

VULNERABILITIES AND PATCHES

- A proof of concept (PoC) has been released for a critical flaw in WordPress in the WooCommerce Checkout Manager plugin, exposing more than 60,000 websites. The flaw is an “arbitrary file upload” that may allow remote attackers to execute arbitrary server-side code in the context of the web server process, access or modify data and gain administrative access.

  Check Point IPS blade will provide protection against this vulnerability in the next releases

- Millions of IoT devices have been found exposed to 2 serious vulnerabilities in the iLnkP2P peer-to-peer (P2P) system, which allows users to remotely connect to their IoT devices. The vulnerabilities could allow an attacker to intercept connections of vulnerable devices and conduct man-in-the-middle attacks.

- Two vulnerabilities have been discovered in Android-based smart-TVs from Sony. The vulnerabilities reside in the ‘Photo Sharing Plus feature’ used for smartphone screen mirroring, and could allow an attacker to access WiFi passwords and images stored on the devices.

  Check Point IPS blade will provide protection against this vulnerability in the next releases

- Several critical vulnerabilities have been found affecting Sierra Wireless AirLink G5 gateways and routers, which used in PoS, industrial IoT and distributed enterprise settings. The vulnerabilities could allow remote code-execution (RCE) and arbitrary command-injection.

  Check Point IPS blade will provide protection against this vulnerability in the next releases

THREAT INTELLIGENCE REPORTS

- Karkoff, a new remote administration tool created by the threat actors behind the DNSpionage tool has been recently deployed and directed at carefully selected targets, mostly in Lebanon. Karkoff allows the threat actors to selectively choose which targets to infect by gathering system information, operating system, domain, and list of running processes on the victim’s machine.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Win32.Karkoff)

- A new analysis is reviewing the “Carbanak” malware used in thousands of financially motivated attacks associated with the Russian FIN7 group. The analysis reveals Carbanak's full source code, builders, previously unseen plugins and a complex command-handling function for C2 communication.

  Check Point Anti-Virus blade provides protection against this threat (Backdoor.Win32.Carbana)

- A new variant of the Qbot Trojan has been spotted in a new campaign, using a phishing-based infection technique. The phishing emails contain malicious links delivered as part of a pre-existing email thread.

  Check Point Anti-VIrus and Anti-Bot blades provide protection against this threat (Trojan-Banker.Win32.Qbot; Trojan.Win32.Carbanak)