April 23 - April 29, 2018

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Researchers at Check Point have discovered a new type of phishing kit sold in the dark web and aimed at Brazilian users, where threat actors can create convincing fake retail product pages and manage their entire phishing campaign, using reliable replicas of sites such as Walmart, Americanas, Ponto Frio, Casas Bahia, Submarino, Shoptime and Extra.

- Attackers have hijacked the DNS servers of MyEtherWallet.com, a web-based Ether wallet service. Users accessing the site were redirected to a fake version of the website. Those who logged in had their wallet's private keys stolen, which the attacker then used to empty accounts, stealing about $160,000.

- "Careem", the United Arab Emirates version for Uber, has been hacked, and private data of 14 million drivers and customers was stolen, including names, phone numbers, email addresses and ride data.

- Security researchers have warned of a new spam campaign intended to infect users with GrandCrab ransomware. The emails contain messages about payments, tickets, invoices and orders and contain a Javascript attachment which when executed, downloads GrandCrab from a malicious URL.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(suspicious executable containing ransomware; Trojan-Ransom.Win32.GandCrab)*

- Security researchers have revealed that several VPN extensions for Chrome leak user data; including Hola VPN, Touch VPN, Betternet, DotVPN, HoxxVPN, Ivacy VPN and Opera VPN.

  Check Point IPS blade will provide protection against this threat in its next online package

- Equifax, which suffered a massive Data-Breach in 2017, have reported expenses of around $242 million as a result of the attack, and plans to invest additional sums by 2019, in order to improve its data security system.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Apache Struts2 Content-Type Remote Code Execution (CVE-2017-5638))*

VULNERABILITIES AND PATCHES

- Check Point researchers have revealed that NTLM hash leaks can be achieved via PDF files with no user interaction or exploitation.

  Check Point IPS blade provides protection against this threat (Multiple PDF readers NTLMv2 Credential Theft)

- MikroTik has released firmware patches for RouterOS, the operating system that ships with some of its routers. The patches fix a zero-day vulnerability exploited in the wild, affecting all RouterOS versions released since v6.29. The exploit is being used in spreading a new IoT botnet.

  Check Point Anti-Bot blade provides protection against this threat (Trojan.Win32.LuaBot)

- Researchers have published a PoC Code triggering an Instant crash on all Windows versions, even when the PC is locked.

  Check Point IPS blade provides protection against this threat (Microsoft Windows NTFS Denial Of Service)

- Security researchers claim that a patch, released by Oracle in its recent patching effort, can be bypassed and in fact does not actually fix the vulnerability.

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

THREAT INTELLIGENCE REPORTS

- Check Point researchers have exposed a threat actor that used to infect victims with potentially unwanted programs, and is now monetizing on crypto mining malware.

- Security researchers have discovered a new ransomware, still under development, where instead of having the distributed executable perform the ransomware functionality, the executable compiles an embedded encrypted C# program at runtime and launches it directly into memory.

  Check Point SandBlast provides protection against this threat

- Security researchers have revealed that a design flaw in the software of electronic keys produced by Assa Abloy, formerly VingCard, has left millions of hotel rooms worldwide vulnerable to hackers. After obtaining a key, hackers can use an RFID reader to try several key combinations to decode the card, eventually identifying the hotel's code and creating a master key for the hotel. The vulnerability is relevant to hotel rooms in 166 countries and 40,000 locations.

- Security researchers have created a method to turn Amazon Echo into an eavesdropping device, using options available in Alexa software development kit (SDK) to create a calculator app that continues to "listen" after providing the user with a reply to a question.