Check Point Research

WEEKLY INTELLIGENCE REPORT

Apr 4 – 10, 2022

TOP ATTACKS AND BREACHES

- Check Point Research discovered six applications spreading banking malware on Google Play Store by masquerading as anti-virus solutions, with over 15,000 downloads. The malware, known as ‘Sharkbot’, steals credentials and banking information of Android users.

  Check Point Harmony Mobile and Threat Emulation provide protection against this threat *(Sharkbot.TC)*

- Threat actor APT-C-23, affiliated with the cyber division of the Palestinian group Hamas, has been targeting Israeli individuals and officials in an espionage campaign, using fake Facebook profiles to lure the victims into downloading malicious applications that will grant hackers access to their devices.

- Chinese state-sponsored APT10 group (aka Cicada) is targeting organizations globally with what appears to be a cyber-espionage campaign leveraging the VLC media player. Victims include government, legal, religious and NGO sectors with a concentration in US, Hong Kong, Israel, Turkey, India, and more.

- Snap-on, a US based automobile tools manufacturer, has revealed it has been victim of a Conti ransomware attack after the group started leaking their data online. Conti removed the data which led to speculation that Snap-on paid the ransom.

  Check Point Harmony Endpoint provides protection against this threat *(Ransomware.Win32.Conti)*

- Ukraine has warned of a new campaign, attributed to UAC-0094 threat actor, that aims at gaining access to Telegram accounts. Victims receive messages alerting that a login has been identified from a device in Russia and demanding to confirm their account by clicking on a malicious link.

- The new Spring4shell vulnerability (CVE-2022-22965) has been actively exploited by threat actors since the beginning of April, leveraging the Mirai botnet. The Singapore region has been one of the most impacted geographic area.

  Check Point IPS, Harmony Endpoint for Linux, Anti-Bot and CloudGuard Containers Security provide protection against this threat *(Spring Core Remote Code Execution (CVE-2022-22965); Exploit_Linux_Spring4Shell_B; Exploit_Linux_Spring4Shell_A; Trojan.Win32.Mirai)*

VULNERABILITIES AND PATCHES

- Palo Alto Networks has issued a warning that some of its products including firewall, VPN, and the XDR agent are vulnerable to a high severity vulnerability tracked CVE-2022-0778. The flaw, which wasn't yet exploited, could enable denial-of-service (DoS) attacks or a remote crash of the compromised endpoints.

  Check Point IPS provides protection against this threat (OpenSSL Denial of Service (CVE-2022-0778))

- Check Point Research shows that 16% of the organizations worldwide were impacted with Spring4Shell during the first 4 days after the vulnerability outbreak. VMware has released security updates to address this critical remote code execution flaw within its products.

  Check Point IPS, Harmony Endpoint for Linux and CloudGuard Containers Security provide protection against this threat (Spring Core Remote Code Execution (CVE-2022-22965); Exploit_Linux_Spring4Shell_B; Exploit_Linux_Spring4Shell_A)

THREAT INTELLIGENCE REPORTS

- Microsoft has disrupted Russian state-sponsored APT28 (aka Fancy Bear, Strontium) domains that were used in cyber-attacks against Ukrainian institutions and media organizations, as well as US and EU governmental targets.

- Following the Conti ransomware leaks in March, a hacktivist group known as NB65 started using Conti leaked source code to create its own ransomware strain and target Russian organizations.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win32.Conti)

- Researchers have found the first case of malware that was tailored to be executed in Amazon Web Services (AWS) Lambda environments with cryptominers. Dubbed "Denonia", it is designed to drop the XMRig cryptominer.

  Check Point CloudGuard Log.ic, Threat Emulation and Anti-Bot provide protection against this threat (Miner.Wins.XMRig; TS_Miner.Win32.XMRig.TC; Trojan.WIN32.XMRig)

- Germany has shut down Hydra, the most prominent Russian Darknet market used for drug sales and money laundering.

- A new Remote Access Trojan (RAT) called "Borat" has emerged on Darknet platforms and is available to buy as a tool for DDoS attacks, ransomware deployment and more.