June 18 – 24, 2018

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point security researchers have revealed a phishing operation targeting World Cup fans worldwide. The operation is luring victims to download an infected "FIFA World Cup schedule and results checker" document, containing an additional downloader dubbed "DownloaderGuide".

  Check point SandBlast, Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Win32. DownloadGuide; PUP.Win.DownloadGuide.C)

- State-sponsored Chinese threat actors have breached a US Navy contractor that works for the Naval Undersea Warfare Center, and reportedly stole over 600 GB of undersea and submarine weapon technology. Attacks that originate in China have also been observed lately targeting US telecommunication companies, and others.

- Thrip, a threat group most likely based in China, has been carrying out an espionage campaign in the past few month which uses PsExec, a legitimate Microsoft tool, to move laterally within infected networks and spread custom malware. Its targets include communications and defense companies in the United States and Southeast Asia.

  Check point Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Win32. Rikamanu; Trojan.Win32. Syndicasec; Trojan.Win32. Spedear)

- Over 100 GB of user data from thousands of mobile applications, both for iOS and Android, has been exposed due to misconfiguration of Firebase databases, a popular backend service from Google, used to create mobile and web-based applications. Leaked data includes plain text passwords, location data and even banking credentials.

- Flightradar24, a highly popular flight tracking service, had been massively breached. About 230,000 user data records, which include email addresses and hashed passwords, may have been exposed.

VULNERABILITIES AND PATCHES

- The highly critical remote code execution flaw in Drupal content management framework, Drupalgeddon3, has been exploited to deliver Monero Crypto-Miner. Threat actors have used an ELF downloader that retrieves a Monero Crypto-Miner and installs it on affected machines.

  Check point IPS blade provides protection against this threat (Drupal Core Remote Code Execution (CVE-2018-7600); Drupal Core Remote Code Execution (CVE-2018-7602))

- An authentication flaw has been discovered in two of Google's most popular consumer products, Google Home and Chromecast. The flaw enables attackers to collect precise user location data via a simple script, and Google is expected to fix the privacy leak in the coming weeks. A follow-up research reveals that the flaw may also be found in other media streaming devices, and is not unique to Google products.
- In its monthly update for June, Cisco has released patches for 34 software flaws, including fixes for six critical vulnerabilities which may allow attackers to execute arbitrary code on vulnerable devices. Four critical vulnerabilities affect the Cisco Fabric Services, which enable synchronization of configuration data between different Cisco devices on the same network.

THREAT INTELLIGENCE REPORTS

- A New and sophisticated botnet has emerged dubbed "Mylobot", equipped with complex evasion techniques including anti-VM, anti-sandbox and anti-debugging techniques. The main functionality of the botnet allows an attacker to take complete control of the user's system, downloading any additional payload from its C&C.

  Check point SandBlast provides protection against this threat

- Researchers have reviewed a new method developed by attackers to steal sensitive information from previously hacked websites using Magento, an open-source e-commerce platform. The method is simple and effective, allowing attackers to re-add their malicious code to a hacked website after it has been removed.
- ZeroFont is a technique used to bypass sophisticated phishing detection mechanisms. The technique is based on hidden words with font size of zero which are inserted within the message content. The method was previously used to bypass spam filters and is now used to trick AI-based engines
- An article has reviewed the role artificial intelligence in conducting and preventing Distributed Denial-of-Service (DDoS) attacks. While AI can be used to track and point at new attack techniques, it can also be leveraged by attackers to bypass protection algorithms and even mislead the algorithm to prevent any identification of the chosen attack techniques.