Check Point
SOFTWARE TECHNOLOGIES LTD.

September 02 – September 08, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Attackers have convinced the CEO of an energy company to send $243,000 to a fake supplier using AI to create a deep fake voice impersonation of a chief executive.
- "Joker", an Android spyware first spotted in June 2019, has been found on 24 different applications on Google Play store. Designed to steal SMS messages, contact lists, device information, the malware targets users from designated 37 countries and has been downloaded by nearly half a million users until removed by Google.

  Check Point SandBlast Mobile provides protection against this threat
- The Serverless Computing Service "Cloudflare Workers" has been abused in a new malicious campaign. The "Workers" have been used in a three-stage campaign to deliver a new variant of the Astaroth Infostealer, a malware first discovered in 2018 targeting victims from Brazil.
- The forums of the known online comic XKCD has suffered a data breach which affected more than half a million users. The data exposed consisted of usernames, hashed passwords and email and IP addresses.
- "Nemty", a ransomware previously spotted spreading via compromised Remote Desktop connections, is now using a fake PayPal page and the RIG exploit kit to infect new victims.

  Check Point IPS, Anti-Virus and Anti-Bot blades provide protection against this threat (RIG Exploit Kit Website Redirection; RIG Exploit Kit Landing Page; Ransomware.Win32.Nemty.TC)
- In another recently published ransom attack, the American city of New Bedford Massachusetts has offered to pay $400,000 instead of the requested $5.3 million in exchange for decryption keys. Attackers rejected the proposal and the city resolved to restore its systems from backups.
- 419 million records of phone number and user IDs of Facebook users have been found on a publicly exposed server that wasn't password protected. The leaked IDs can be used to correlate between the phone numbers and user profiles.

VULNERABILITIES AND PATCHES

- Check Point Research has identified a weakness in certain Android-based phones that could permit an advanced phishing attack. Using a GSM modem, an attacker can send a network configuration message which, once approved by the user, routes all their Internet traffic through a proxy controlled by the attacker, thus exposing it to them.

  Check Point SandBlast Mobile provides protection against this threat

- A remote code execution exploit module for the BlueKeep vulnerability in Microsoft Remote Desktop has been published in the Metasploit framework.

  Check Point SandBlast Agent and IPS provide protection against this threat (Microsoft Remote Desktop Services Remote Code Execution (CVE-2019-0708))

- Baseboard Management Controller (BMC) feature, which allows sysadmins to mount virtual media as virtual USB, exposes Supermicro Servers to remote USB attacks. These vulnerabilities, collectively dubbed "USBAnywhere", have been revealed publicly accessible over the internet in more than 47,000 Servers.

- A critical remote code execution vulnerability has been discovered in the popular open-source Exim email server software. Tracked as CVE-2019-15846, the vulnerability affects over half a million email servers but no known exploits have yet been reported.

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed the Bemstour exploitation tool used by APT3, an alleged Chinese threat actor. The analysis suggests that APT3 investigated network recordings of EternalRomance, a tool supposedly used by the American APT Group Equation, and used it to create Bemstour. EternalRomance had been used by APT3 prior to the Shadow Brokers leak.

  Check Point IPS blade provides protection against this threat (Microsoft SMB Client Transaction Memory Corruption (MS10-020))

- A new social engineering toolkit has been discovered and named Domen. The toolkit prompts the users with a fake software message, urging them to update their browser, flash client, etc. The downloaded fake update infects the victims with malware once ran. According to researchers, it is a highly versatile and sophisticated toolkit, which is able to adapt to different browsers, clients and victims.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Domen.)*

- Researchers warn of a vulnerability in the method used by Windows and antiviruses when handling VHD and VHDX disk image files. In contrary to privilege restrictions and warnings issued for regular files downloaded from the internet, disk image files do not trigger the same Windows and AV protections, thus might deliver malware without being checked.