Check Point
SOFTWARE TECHNOLOGIES LTD.

September 23 – October 01, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point researchers have identified a targeted and extensive attack against East Asian government entities over the span of 7 months. The attackers, which apparently are members of the Chinese Rancor threat group, used spear-phishing to reach their victims, pretending to send emails from other government offices.

  Check Point SandBlast provides protection against this threat

- Poison Carp, a new hacking group attributed to the Chinese government, has been observed targeting high profile members of several Tibetan groups with one-click exploits for iOS and Android devices. Once infected, the attackers were able to gain full access to the victim's device and the content of its apps, including Twitter, Gmail, WhatsApp and others.

- Forums of the cybersecurity company Comodo have been breached using the vBulletin platform zero-day remote code execution vulnerability. The data breach has exposed the information of nearly 245,000 of the forum users including usernames, hashed passwords, email addresses, etc.

  Check Point IPS blade provides protection against this threat *(vBulletin Forum Remote Code Execution (CVE-2019-16759))*

- DoorDash, the San Francisco–based on-demand food delivery service, has suffered a major data breach. The exposed data included personal information of its 4.9 million users (names, email and personal address, order history, hashed passwords, etc.), partial financial information of its users and merchants and the driver's license numbers for 100,000 of the company's drivers.

- A new variant of the cross-platform Remote Access Trojan Adwind has been seen targeting the US petroleum sector, according to researchers. This campaign utilizes obfuscated JAR files attached to phishing emails to infect its victims.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat *(Backdoor.Java.Adwind.TC)*

VULNERABILITIES AND PATCHES

- "Checkm8", a new unpatchable BootROM vulnerability might be used to jailbreak most of the iPhone and iPad models available. Researchers raise concern that an attacker with local access to the device can install malware, spouse-ware or stalker-ware without the victim's knowledge.
- A zero-day remote code execution vulnerability (CVE-2019-16759) in the vBulletin forum platform has been publicly disclosed with a working exploit. The vulnerability allows an attacker to execute any command on the affected website. Several websites have already fallen victim to this vulnerability and an official patch has been released.

  Check Point IPS blade provides protection against this threat *(vBulletin Forum Remote Code Execution (CVE-2019-16759))*

- Microsoft has released a patch for a memory-corruption zero day vulnerability in Microsoft Internet Explorer. This vulnerability allows a remote attacker to gain privileged access to the victim's machine by manipulating the victim into visiting a specially crafted website.

  Check Point IPS blade provides protection against this threat *(Microsoft Internet Explorer Use After free (CVE-2019-1367))*

- An unpatched bug in iOS 13 and iPadOS allows third-party keyboard apps to gain full access to the text typed by the user, even if such permission was previously denied.
- A critical heap-based overflow vulnerability has been patched in the popular open-source Exim email server software. Tracked as CVE-2019-16928, the vulnerability may be used in remote code execution and denial of service attacks.

THREAT INTELLIGENCE REPORTS

- Check Point Research, in cooperation with Intezer, has analyzed 2000 samples attributed to the Russian cyberwarfare apparatus. This report highlights the connections (or lack thereof) between different Russian actors.
- A flaw in several antivirus engines treats OpenDocument Text (ODT) files as simple archives, thus allowing malicious OLE objects to be embedded in them. According to researchers, such files were used to deliver RevengeRAT, njRAT and AZOrult malware samples.
- The threat actors behind Emotet, the popular banking Trojan, have been spotted by researchers using a fake Microsoft Office Activation Wizard template to manipulate new victims into enabling macros in the malicious document.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Botnet.Win32.Emotet.TC)*