October 14 – October 21, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has exposed the Phorpiex botnet which uses thousands of infected machines to deliver millions of sextortion emails to its victims. The botnet utilizes pairs of previously leaked emails and passwords to convince the victims that they have been hacked and their personal online activity will be leaked if they won't pay. In a five months period its revenue is estimated to be $110,000.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Trojan.Win32.Phorpiex.TC)

- Attackers have used posts on Pastebin and spam emails to deliver a trojanized version of the Tor Browser to Russian victims in order to steal cryptocurrency. According to researchers the attackers have stolen $40,000 in 860 Bitcoin transactions.

  Check Point Anti-Virus provides protection against this threat (Trojan.Script.Agent)

- Attackers have breached the internal network of the cybersecurity company Avast using a temporary VPN profile that wasn't protected by two-factor authentication. As several user credentials were used in this attack it is suspected that the company was also a victim of credential theft.

- NordVPN, VPN provider, has been breached in 2018. According to the company, one of its servers was accessed by exploiting an insecure remote management system left by the data center provider.

- Researchers are seeing a rise in the use of the infamous "Cutlet Maker" malware that is used by criminals to manipulate an ATM to eject all of the money stored in it, in an attack called "Jackpotting". As physical access to the ATM machine is required to perform the attack, a proper physical security of the machine may prevent such attacks.

- A new malicious campaign delivering WAV audio files with embedded malware in it has been spotted. Once ran, the code contained in the trojanized files utilized one of three different loader components to load a cryptocurrency miner or a reverse shell on the victim's machine.

VULNERABILITIES AND PATCHES

- Researchers have revealed that two older Amazon devices, 1st generation Amazon Echo and 8th generation Amazon Kindle, are still vulnerable to the Krack Wi-Fi exploit although a fix has been issued at the beginning of 2019. This exploit can be used by an attacker to join an unauthorized wireless network without a password.
- Samsung will patch a vulnerability in the Galaxy S10 phone that allowed an attacker to unlock the phone with an unknown fingerprint by putting a silicon case on it.
- A vulnerability (CVE-2019-14287) in the Linux sudo command, which could be exploited to run a command as another user, including the privileged root user, by using a special user ID, was fixed. The vulnerability requires a special configuration, thus most of the Linux machines were unaffected.
- A critical vulnerability (CVE-2019-17666) in one of the Wi-Fi drivers of the Linux kernel could potentially lead to a full compromise of a vulnerable machine by a buffer overflow attack. A fix is being developed by the Linux kernel team.

THREAT INTELLIGENCE REPORTS

- Check Point Research has discovered that the banking Trojan Redaman uses a new technique called "Chaining" in order to hide the C&C servers of the known infostelaer Pony in the Bitcoin blockchain. The C&C is used both as a drop zone for Pony and storage for its stolen information.

  Check Point Anti-Virus provides protection against this threat (Infostealer.Win32.Pony.TC; Trojan-Banker.Win32.RTM)
- The Russian APT group Turla has used stolen malware and hijacked infrastructure belonging to the Iranian APT group OilRig to disguise their attacks on targets from dozens of countries.
- Researchers have released a dercryptor for 148 variants of the Djvu ransomware that utilizes a side-channel attack on the ransomware's keystream to break the encryption. Without the tool the victims would have to pay $980 to decrypt the files.

  Check Point Anti-Virus provides protection against this threat (Trojan.Win32.Djvu.TC)
- Google will issue a fix for a flaw in its newly released device, Pixel 4, that allowed the phone to be unlocked using the face recognition algorithm even when the eyes of the owner were closed. A concern has been raised that the flaw may be exploited by holding it in front of the face of its sleeping owner.

For comments, please contact: TI-bulletin@checkpoint.com