November 11 – 17, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Mexican state-owned oil company Petróleos Mexicanos (Pemex) has been infected with the DoppelPaymer ransomware in an incident that reportedly affected less than 5% of its network. DoppelPaymer is a forked version of the BitPaymer ransomware.

  Check Point Anti-Virus and Anti-Ransomware provide protection against this threat *(Ransomware.Win32.Doppelpaymer)*

- US Select Health Network and Solara Medical Supplies have disclosed data breaches after hackers compromised employee email accounts and stole personal records and protected health information.

- InfoTrax Systems, a US-based technology company, has suffered a series of breaches over the course of two years, resulting in the theft of sensitive information of 1 million customers. The company detected the breach after receiving alerts that their server reached maximum storage capacity, which was caused by a data archive file the hacker created.

- The details of the Australian Parliament security incident earlier this year have been revealed; confirming that the intrusion happened after several users accessed an external website that was compromised, which caused malware to be injected to the parliamentary computer network. Two senators and other parliament members had some of their non-sensitive data stolen as a result.

- A wave of DDoS attacks abusing the TCP SYN-ACK reflection mechanism against corporations worldwide has been detected. The DDoS condition is caused by a spoofed SYN packet, containing the IP of the victim as source IP, sent to a wide range of reflection IP addresses. This is causing the reflection services to repeatedly re-transmit SYN-ACK packets to the victim, emulating a DDoS attack.

- The UK Labour party has been targeted by a DDoS attack in an attempt to take their systems offline. Lizard Squad, the notorious hacktivist group, took responsibility for the attempt. The group also claimed to compromise the personal accounts of Jeremy Corbyn’s family, in an attempt to take out his and the Labour party’s online presence ahead of UK’s upcoming general elections.

VULNERABILITIES AND PATCHES

- Check Point research has discovered vulnerabilities affecting Qualcomm chipsets used in Samsung, LG and Motorola smartphone devices. The flaws were discovered in the implementation of third-party components that are loaded and executed in the chip's Trusted Execution Environment. Successful exploitation of the flaws may allow hackers to access the device's TrustZone, a secure storage of the most sensitive information such as passwords, fingerprints and more.
- Stack-based buffer overflow vulnerability has been discovered and patched in WhatsApp. The vulnerability resides in the way WhatsApp parses the metadata of an MP4 file, and may allow denial-of-service or remote code execution attacks by sending a crafted, malicious MP4 file over WhatsApp.
- A beta version exploit for the checkm8 BootROM vulnerability has been made public. The checkm8 vulnerability is an un-patchable Bootrom jailbreak for Apple products released between 2011 and 2017, including iPhone models until X. The published exploit requires physical access to an unlocked device.

THREAT INTELLIGENCE REPORTS

- A new threat actor, tracked as TA2101, has been delivering malware-weaponized emails impersonating government agencies in the United States, Germany and Italy. Among the malware types delivered are the Cobalt Strike pen-testing tool, IcedID banking Trojan and the Maze Ransomware.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Banking.Win32.Icedi, Ransomware.Win32.Maze, Backdoor.Win32.CobaltStrike)

- NextCry, a new ransomware strain, is targeting Linux instances of the NextCloud file sync and share service. It is suggested that the attackers exploited a newly released vulnerability that impacts the NextCloud NGINX configuration to install the ransomware.

  Check Point IPS and Anti-Virus blades provide protection against this threat (PHP FastCGI Process Manager Remote Code Execution (CVE-2019-11043); Ransomware. Linux.NextCry)

- AnteFrigus, a new ransomware, is being delivered through RIG exploit kit malvertising campaigns, and is only targeting drives associated with removable devices and mapped network drives..

  Check Point IPS blade provides protection against this threat (RIG Exploit Kit Landing Page; RIG Exploit Kit URL; RIG Exploit Kit Rotator; RIG Exploit Kit Website Redirection)

- PureLocker, a ransomware that has variants against all major operating systems, is actively targeting production servers. The malware uses several methods to evade detection, including posing as the Crypto++ cryptographic library or terminating itself when running in a debugger environment. Analysis shows that PureLocker borrows code associated with the financially-motivated Cobalt group.

  Check Point SandBlast Agent provides protection against this threat (Ransomware.Win32.PureLocker)