August 21 – 27, 2017

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A new email phishing campaign has been detected, aiming to lure its victims with leaked episodes of the popular TV show "Games of Thrones". The malicious documents attached to the emails contain fake links to previews from the new episodes, which in fact download a remote access Trojan.

  Check Point IPS blade will provide protection against this threat in its next online package

- A security researcher has discovered a list of thousands of active Telnet credentials for many Internet of Things (IoT) devices. The list is suspected to have helped threat actors with improving their Denial-of-Service platforms. Several credentials included in the list suggest that some of the devices had already been conscripted into botnets.

  Check Point IPS blade provides protection against this threat (Weak Password Login Attempt Over Telnet)

- Security researchers have found a new ransomware dubbed "Defray" being spread in two targeted campaigns in the wild, one targeting healthcare and education verticals and the other - manufacturing and technology. It is being spread via Microsoft Word document email attachments.

  Check Point IPS blade will provide protection against this threat in its next online package

- Additional files have been leaked on WikiLeaks as a part of Vault 7. The files contain disturbing details about a system called ExpressLane, developed by the CIA, which collects biometric data from the agency's intelligence partners without their permission.

VULNERABILITIES AND PATCHES

- A security researcher has published how he managed to find and exploit vulnerabilities that exist in the kernel of iPhone devices that are running with IOS 10.3.1 and previous versions. The vulnerability allowed him to gain full read/write and root privileges on a compromise device.

- Two zero-day vulnerabilities have been exposed in Foxit pdf reader. The vulnerabilities were reported to Foxit in May, but are still not patches, leaving over 400M users exposed to this threat.

  Check Point IPS blade provides protection against this threat *(Foxit Reader PDF Arbitrary File Write Remote Code Execution (CVE-2017-10952); Foxit Reader PDF Command Injection Remote Code Execution (CVE-2017-10951))*

- Security researchers have found a new vulnerability in SAP POS Express Server which offers a point-of-sale solution for retailers. An attacker can modify critical functions in the application without providing any credentials because there are no authentication checks. The researchers demonstrated how they managed to purchase a MacBook for only $1.

THREAT INTELLIGENCE REPORTS

- Several WordPress websites have been encrypted by hackers who demand ransom. Interestingly, the hackers aren't able to decrypt the websites' key files, and so paying the ransom is useless.

  Check Point IPS blade provides protection against this threat *(Multiple PHP Webservers Ransomware Upload)*

- Chinese threat actors are now offering in the underground a service which consists of an Android application that allows anyone to simply create customized Android ransomware.

- Security researchers have found a new variant of the CryptoMix ransomware that encrypts files with ".EMPTY" extension. The encryption method remained the same in this variant. On a similar note, a new variant of Crysis ransomware has been spotted in the wild, adding the ".arena" extension. This ransomware is known to be spread by remote desktop access.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Multiple RDP Initial Connection Requests; Trojan-Ransom.Win32.CryptoMix.*; Trojan.Win32.Crysis.*)*

- According to a new report, 90% of the companies have experienced attempts to exploit old vulnerabilities on their platforms during the 2nd quarter of 2017.

- Security researchers have showed in a new report that there was an increase of distributed denial of service (DDoS) attacks against web applications during the 2nd quarter of 2017. They further claim that the high number mostly came from the large-scale attack of the PBot DDoS malware.

  Check Point Anti-Bot blade provides protection against this threat *(Backdoor.Win32.Pbot.*)*

- A new attack vector dubbed Ropemaker can allow threat actors to modify emails after they have already been sent and delivered, adding malicious links and attachments.

- Security researchers have found a malicious Chinese software development kit in over 500 Android apps, downloaded over 100 million times. The kit, downloaded by legitimate apps after their initial installation, steals users' private data and sends it to the creators' servers.