August 20 - 26, 2018

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Ryuk, a ransomware uncovered by Check Point researchers, has been used in several well-planned targeted attacks against several companies worldwide. The ransomware is connected to the HERMES ransomware attributed to the Lazarus group, and has so far gained some $640,000 in ransom payments.

  Check Point SandBlast provides protection against this threat

- A new malware downloader dubbed AdvisorBot has recently been observed in email campaigns targeting the hospitality and telecommunications sectors. Upon infection, the downloader first loads fingerprinting module used to detect targets of interest, and then delivers a second malware.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat *(Trojan-downloader.Win32.AdvisorBot)*

- The Iranian hacking group Cobalt Dickens, known for attacking hundreds of universities worldwide by delivering phishing pages for a university's online library portal, has been carrying out a new phishing campaign of similar characteristics, targeting universities in Europe, North America, Asia and Australia.

- Lazarus group, an APT group linked to North Korea, has managed to attack several banks and hack several cryptocurrency exchanges and Fintech companies. In order to obtain access the targeted companies, the group used a known malware called Fallchill and a new malware for Mac OS.

  Check Point Anti-Virus blade provides protection against all known variants of this threat *(Trojan.Win32.Fallchill)*

- A new campaign targeting mainly Mexican users called Dark Tequila has recently been exposed. The attackers, most likely based in Latin America, are using a multi-stage payload delivered to customers of several Mexican financial institutions, to collect banking information and login credentials to popular websites.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat *(Trojan-Spy.Win32.DarkTaquila)*

VULNERABILITIES AND PATCHES

- Security researchers have discovered that millions of mobile devices from 11 smartphone vendors are vulnerable to attacks leveraging AT (ATtention) commands. The AT commands are exposed via the device's USB interface, and may allow an attacker to rewrite device firmware, exfiltrate sensitive information, unlock screen, and mimic touchscreen taps, enabling to take full control over the device.
- A vulnerability has been revealed in the popular Fortnite Android app, exposing it to man-in-the-disk (MitD) attacks. A successful exploitation allows low-privileged malicious apps already installed on a user's phone to hijack the Fortnite app's installation process, and install other malicious apps.
- A flaw has been found in Ghostscript, a popular interpreter for Adobe PostScript and PDF page description languages. The flaw might allow an attacker to gain remote control over vulnerable systems. Known affected vendors include Red Hat, Ubuntu and Artifex Software and ImageMagick, and currently there is no available patch.
- Apache has released a software update meant to fix a critical vulnerability in Apache Struts, a Web application platform. An exploit has already been posted online.

  Check Point IPS blade provides protection against this threat *(Apache Struts Remote Code Execution (CVE-2018-11776))*

THREAT INTELLIGENCE REPORTS

- Check Point researchers have published a visualization of all generations of the "Big Bang APT", targeting the Palestinian Authority, demonstrating the similarities in infrastructure and TV/movie themes.

  Check Point SandBlast provides protection against this threat
- Triout is a newly discovered Android espionage malware, which features extensive spyware capabilities such as phone call recording, text message monitoring, photos and videos theft, and user location collection. The malware is spread via a fake, but certified Android app.

  Check Point SandBlast Mobile customers are protected from this threat
- Academic researchers have developed a method to collect information from a personal computer by recording acoustic signals from the machine's LCD screen and determining the content in real-time. The new technique could be used in espionage campaigns.
- Researchers have investigated a sophisticated backdoor deployed by the Turla APT group in multiple operations as of 2009, including a recent one in which it was used to intercept sensitive communications of several authorities and foreign offices across Europe.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat *(Backdoor.Win32.Turla; Turla)*