October 9 - 15, 2017

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Australian officials have revealed that a 2016 breach in a small Navy contractor had led to the leak of sensitive military information about advanced aircrafts and several Navy ships. The breached company appears to have used default and easy to guess credentials, which enabled the initial breach.

  Check Point IPS blade provides protection against this threat *(China Chopper Web Shell Remote Code Execution)*

- Security researchers have provided an in-depth analysis of the hackers group "Bronze Butler". The group is most likely active out of China, and has been specifically targeting Japanese heavy industry firms since at least 2012. Researchers stated that the group's proficiency had grown since its inception, and it is found to use targeted phishing, strategic web compromises and zero-day vulnerabilities in systems especially popular in Japan.

- New information about the Equifax breach has brought the number of UK citizens whose information was exposed to 15.2 Million. The file acquired in the attack contained client information from the years 2011 to 2016, including passwords and answers to security questions.

- Pizza Hut in the U.S has announced that its website, Pizzahut.com, had been hacked, and that the attackers had access to client information between the 1st and 2nd of October 2017. Customers who may have been affected were notified by email.

- Researchers have reported that new variants of Locky ransomware were on the rise during September. They were spread by a large scale spamming campaign - fake invoice was sent as a 7zipped file which contained a VBScript, which in turn downloaded Locky. It is estimated the spam messages were sent to 3 million addresses.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Suspicious Executable Mail Attachment; Trojan-Ransom.Win32.Locky.*)*

- Researchers have reported that hundreds of websites use their users' CPU to mine cryptocurrencies, without their consent. In some cases it is due to being compromised, but in other cases it is done knowingly in an attempt to monetize traffic.

  Check Point IPS blade provides protection against this threat *(Multiple Websites Mine Cryptocurrencies CPU Hijacking)*

- DDoS attacks have caused train delays across Sweden. The first attack hit the Sweden Transport Administration and brought down the IT system used for train orders, its email and website as well as its electronic map service. This impacted train traffic for a day. The next day, two other Swedish transportation agencies were attacked in the same manner.

VULNERABILITIES AND PATCHES

- Security researchers have reported a new zero-day MS Office vulnerability, already being exploited for attacks. The attack utilizes an old MS Office feature called Microsoft Dynamic Data Exchange (DDE), to execute malicious code without the use of Macros. Microsoft patched this issue in its recent bulletin.

  Check Point IPS blade provides protection against this threat *(Microsoft Office Memory Corruption (CVE-2017-11826); Microsoft Office Files Containing Malicious Downloader)*

- Microsoft's security bulletin for October further patched 61 other vulnerabilities, including a DNS server vulnerability which could enable attackers to run arbitrary code on target systems.

- Security analysts have revealed a bug in the Advanced Linux Sound Architecture (ALSA). The bug would allow a local user to gain elevated privileges. Since the attackers must have local access to the system, the likelihood of such an attack is relatively low; however, a patch is already available.

THREAT INTELLIGENCE REPORTS

- Security researchers have reported that the ransomware economy, that is, the darknet based market for ransomware, grew in 2,502% in 2017 compared to 2016. The researchers identified 6,300 places across the darknet where malware was being sold, and over 45,000 ads, ranging from $0.50 to $3,000 per program.

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