November 27 - December 3, 2017

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- TIO Networks, recently acquired by PayPal Holdings, has announced that its network was accessed by an unauthorized actor, exposing personal information of some of its customers. The announcement follows PayPal's suspension of TIO's operation a few weeks ago, due to its vulnerable network and poor security.

- Clarkson Plc, a British shipping services provider, has announced that its network has fallen victim to an executed via a compromised user account that has since been blocked. According to the company's announcement, it does not intend to pay any kind of ransom to the attackers, and it expects that stolen data may be publically exposed by the attackers.

- Bitcoin Gold developers have issued a critical warning about a potential compromise of its Windows Wallet installer, followed by a recall window for the installer. The reason for the recall is the upload of two suspicious files into the Bitcoin Gold's Github repository by an unknown source. The files are suspected to be linked to malicious activities such as cryptocurrency theft or malware distribution, and are currently examined by Bitcoin Gold's developers.

- A new and sophisticated support-scam was observed in the wild. In the scam, a fake blue-screen appears on victim's display, followed by a troubleshooter which encourages the victim to purchase an alleged "Windows Defender Essentials" for $25 in PayPal transaction.

- Imgur image-hosting website experienced a major breach during 2014. In the incident, which was only discovered lately, user-names and passwords belonging to 1.7 million users were stolen.

- A former NSA employee pleads guilty of taking classified data from work to his home-computer during 2010-2015. While no government speaker referred to the event's relation with the NSA leak of cyber-tools by the Shadow Brokers threat group, some media reports claim that the worker's InfoSec violations allowed the breach, as his home computer was using Kaspersky's Anti-Virus software, and that the software was used for obtaining the cyber-tools.

VULNERABILITIES AND PATCHES

- Apple has released a security update for macOS High Sierra 10.13 and macOS High Sierra 10.13.1. The update addresses a vulnerability that may allow an attacker to bypass administrator authentication without supplying the administrator's password.

- Cisco has released a security advisory addressing 6 vulnerabilities in Cisco WebEx Recording Format and Advanced Recording Format Players. The vulnerabilities are rated as critical and may allow an attacker to crash target players and potentially even arbitrary code execution.

THREAT INTELLIGENCE REPORTS

- A new ransomware dubbed Halloware is offered for sale on Dark Web forums with a lifetime license proposal of $40. The ransomware, which hasn't been spotted in the wild yet, was located by researchers who analyzed it and found that it uses a hardcoded AES decryption key and thus shows very low sophistication.

- A new variant of BTCWare ransomware has been discovered. With no new capabilities, its key modifications are a different contact email and a different encrypted files' extension.

- The British National Cyber Security Centre (NCSC) of the GCHQ has published an in-depth report about new tools used by the Turla threat group to target the UK. The tools, named Neuron and Nautilus, are being deployed using the Snake rootkit, and mostly target mail and web servers.

- Researchers have reported on a Tizi, spyware for Android-based mobile phones, targeting African countries and mainly Kenya. The malicious app is populated via socially-engineered posts on social media.

  Check Point Sandblast Mobile customers are protected from this threat

- Researchers have discovered a new technique used by web-based cryptocurrency miners in order to extend the amount of time victim's CPU is abused for mining. In the technique, the mining Java Script is injected into a transparent pop-under window. The pop-under, oppositely to a popup, appears in a tiny frame under the Windows taskbar, thus assuring that even if the victim will attempt to shut down the mining by closing the browser, it will still be running without the victim's awareness.

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

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