Check Point
SOFTWARE TECHNOLOGIES LTD.

October 2 - 8, 2017

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Russian hackers have obtained sensitive NSA material, including details on cyber capabilities in the defensive and offensive arenas. These documents were apparently stored in a personal home computer of one of the agency's contractors, which ran Kaspersky AV. According to some reports, the hackers leveraged the Kaspersky program to gain access to the computer.

- Researchers have found that a campaign against Office365 users dubbed "KnockKnock" has been ongoing since May. The campaign targets carefully chosen accounts, focused on administrative accounts commonly used to integrate corporate email systems with marketing and sales automation software and attempting only 3-5 entry attempts to each in order to fly under the radar. The compromised accounts are later used for spreading phishing campaigns.

- Yahoo has revealed all three billion accounts it had in 2013 were leaked in a massive 2013 breach. The company had formerly admitted only one billion accounts were hacked, but now gave an updated figure. Another breach occurred in 2014, where the attackers gained credentials to half billion accounts.

- The research company Forrester announced it experienced a cyber-attack this week. The company determined the breach was limited to its website, Forrester.com, and data exposed included only materials exposed to clients, and not any client information, confidential data or financial information.

- Personal information of 1,133 National Football League players and agents has been leaked due to a misconfigured online database. The information included home addresses and cell phone numbers.

- New details of the Equifax breach increases the number of Americans whose details were exposed by 2.5 million, to a total of 145.5 million. At a hearing in front of U.S regulators, the company's former CEO took full responsibility to the breach and said the company did not identify the Apache Struts vulnerability which led to it even as late as March 2017.

  Check Point IPS blade provides protection against this threat (Apache Struts2 Content-Type Remote Code Execution; Apache Struts 2 Content-Disposition Remote Code Execution)

VULNERABILITIES AND PATCHES

- Security researchers have revealed a new Rowhammer attack method that could bypass all existing countermeasures. Rowhammer attacks use the fact that hardware vendors place too many memory cells on the same board. The new attack bombards RAM memory cells with constant read-write commands, which could eventually enable an attacker to run arbitrary code on the system.

- Security researchers have revealed seven new vulnerabilities in DNSmasq application, affecting an unknown number of desktops, smartphones and IoT devices. The vulnerabilities are mostly in the DNSmasq DNS and DHCP packages, which are usually open to remote connection, and could enable attackers to gain access to internal networks. The issues were fixed in the programs most recent upgrade, 2.7.8.

  Check Point IPS blade provides protection against this threat (Dnsmasq Heap Based Overflow Remote Code Execution (CVE-2017-14491); Dnsmasq Lack of Free Denial of Service (CVE-2017-14495); Dnsmasq Integer Underflow Denial Of Service (CVE-2017-14496))

- Researchers have discovered three new zero day vulnerabilities on WordPress. Described as critical PHP object injection issues, they affect the Appointments, Flickr Gallery, and RegistrationMagic-Custom Registration Forms plugins, and allow attackers to upload a file to target websites.

THREAT INTELLIGENCE REPORTS

- Security researchers have identified an increase in the activity of the Flusihoc DDoS bot, with a rise in the number of new versions of the bot, and an increase in the number of DDoS attacks conducted with it, summed up in 900 since summer. The botnet is most likely operated out of China.

  Check Point Anti-Bot blade provides protection against this threat (Trojan-DDoS.Win3.Flusihoc.A)

- Security researchers have revealed that a flaw in MPEG-DASH, a common video streaming technique used by Amazon, Netflix, YouTube, Vimeo, and other services, could enable an attacker to accurately assess what a user is watching, even if the streaming is done over HTTPS. This is due to a feature of this technique, which creates an identifiable stream of packets visible to anyone who follows the network traffic, thus creating a unique “fingerprint”.

- Security researchers have revealed that many vendors do not activate all of the embedded motherboard protections, rendering them vulnerable to firmware. The flaws were found in the following motherboards: ASUS Vivo Mini, Lenovo ThinkCentre systems - MSI Cubi2, and Gigabyte BRIX series.