Check Point
SOFTWARE TECHNOLOGIES LTD.

September 4 - 10, 2017

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The popular financial services provider Equifax has suffered a security breach which led to the theft of personal information of over 143 million of its customers from the United States, United Kingdom and Canada. Approximately 209,000 credit card numbers and additional 182,000 dispute documents with personal details were compromised by the threat actors.

  Checkpoint IPS blade provides protection against this threat *(Cross-Site Scripting Scanning Attempt; SQL Servers *)*

- Security researchers have found a new ransomware campaign attributed to three different threat actors, with about 26,000 MongoDBs infected. The attackers scanned the Internet for MongoDBs left open for external connections, wiped their content, and replaced it with a ransom demand.

- Researchers have found a new malware campaign against targets in Brazil in which the threat actors used Facebook's CDN service to host their malicious files in order to avoid being blacklisted.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Malicious VBScript In HTML; Trojan-downloader.Win32.Banload*)*

- The threat Group "Shadow Brokers" has announced that it would release a new malware from the NSA leak to its customers. The tool, dubbed UNITEDRAKE, is an advanced RAT with the ability to capture webcam and microphone output, log keystrokes and access external drives in order to spy on its targets.

- The "Dragonfly" threat group, which for several years has been running a targeted campaign against companies in the energy sector, has increased its activity. The group's attack vectors include phishing emails and the use of bogus websites based on mapping the target organization's network behavior.

  Check Point IPS blade provides protection against this threat *(PowerShell Script Encoding Evasion)*

- A new phishing campaign has been targeting users of the accounting firm Xero, spoofing messages that appear to be originating from Xero and adding malicious links to ZIP archives containing a JavaScript file.

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

VULNERABILITIES AND PATCHES

- A security researcher has found a vulnerability in Apache Struts' REST plugin (CVE-2017-9805). The vulnerability may allow an attacker to upload a malformed file and take over an application after gaining remote code execution rights on the target's Struts-based application server. All Versions up to 2.5.13 and 2.3.34 of Apache Struts are affected.

  Check Point IPS blade provides protection against this threat *(Apache Struts REST Plugin XStream Deserialization Remote Code Execution (CVE-2017-9805); Apache Struts2 Freemarker Remote Code Execution (CVE-2017-12611))*

- Researchers have published a list of newly discovered vulnerabilities in D-Link DIR 850L routers, applying full-disclosure policy after the company had ignored their previous findings. The reported flaws may grant attackers with the ability to intercept traffic, upload malicious firmware, or get root privileges.

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

- Security researchers have revealed a new vulnerability in the Android overlay system (CVE-2017-0752). According to the researchers, a malicious app can use a toast message in order to gain access to required privileges. All Android versions up to 7.0 are vulnerable. The issue has been patched.

- In its September release of the Android Security Bulletin, Google addressed 81 vulnerabilities, including 13 remote code execution bugs, most of which are in Android's Media Framework and the others in the Wi-Fi driver Broadcom component, kernel components, and Qualcomm components.

THREAT INTELLIGENCE REPORTS

- Security researchers have found evidence that the threat group "Codefork" had recently changed its mode of operation into using "file-less malware". This attack vector loads malicious code directly into the infected computer's RAM in order to bypass traditional antivirus solutions. The researchers believe that the group is selling access to infected machines to other criminal groups.

  Check Point IPS blade provides protection against this threat *(PowerShell Script Encoding Evasion; Malicious VBScript In HTML)*

- Researchers have found new variants of Emotet banking Trojan, and noted an increase in its activity during August. The researchers have stated that the malware may now be targeting new regions and new industries outside the banking sectors. An infection may lead to information leaking.

  Checkpoint IPS, Anti-bot and Anti-Virus blades provide protection against this threat *(Malicious VBScript In HTML; Microsoft Office Malicious Macros; Microsoft Office Files Containing Malicious VBScript Downloader; Microsoft Office Files Containing Malicious Downloader; Block repetitive SMB login attempts; Trojan.Win32.Emotet.A; Operator.Emotet.*, Emotet.*)*