Check Point
SOFTWARE TECHNOLOGIES LTD.

September 25 - October 1, 2017

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Deloitte, a top-tier accountancy firm, has suffered a major data breach. In an attack on the company's email server which may be dated back to October 2016, threat actors have managed to steal confidential materials from Deloitte's network. So far 6 clients of the firm were updated that their information was impacted by the attack. The leaked data is likely to contain financial and classified information of Deloitte's clients, as well as private details and credentials for customer accounts.

- Sonic drive-in seems to have suffered a data breach. The incident was discovered after a dark-web marketplace named "Joker's Stash" had offered for sale the credentials of many payment cards, all being linked to Sonic drive-in with past transactions. The company didn't reject the claim, and responded that it is investigating "a potential incident". Credit card leaks of high volumes are usually caused by point-of-sale malware (PoS).

- Threat actors have used compromised Windows webservers in order to mine Monero cryptocurrency. In the incident, which happened last May, the attackers modified legitimate open source Monero mining software and exploited a known vulnerability in Microsoft IIS 6.0 to install the miner on unpatched servers. Researchers estimate that the attackers have generated over $63,000 of profits.

  Check Point IPS blade provides protection against this threat *(Multiple Websites Mine Cryptocurrencies CPU Hijacking; Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow (CVE-2017-7269))*

- R6DB, an online service providing statistics for Rainbow Six Siege computer game, has suffered a ransom attack. According to the company, an attacker had managed to compromise its databases via remote connections enabled for the database, to delete all the data, and to leave a ransom note. Most of the deleted data is unrecoverable.

- Amazon's Whole Food has suffered a credit card breach in some of its stores, such as stores with taprooms and full table-service restaurants located within. The attack's source is yet unknown.

VULNERABILITIES AND PATCHES

- A bug in Internet Explorer allows specially crafted web pages to receive data typed by the user in the URL address bar, data that is supposed to be exposed only to the browser itself.

  Check Point IPS blade provides protection against this threat *(Microsoft Internet Explorer Address Bar Information Disclosure)*

- Oracle has released a security update addressing 7 Apache Struts2 vulnerabilities.

  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); Apache Struts2 Struts1_Plugin Remote Code Execution)*

- Apple has released security updates addressing 66 vulnerabilities in the following products: iCloud for Windows 7, macOS High Sierra 10.12 and macOS Server 5.4.

- A researcher has demonstrated how malware signed with Apple developer certificate can bypass Apple's Gatekeeper, an OS X feature used to prevent malicious applications from harming users' machines.

  Check Point Anti-Bot blade provides protection against this threat *(Trojan.MacOS.exfilKeychain.*)*

- Cisco has released security updates for multiple products addressing 20 vulnerabilities, 8 of which are rated as critical. Some of the vulnerabilities may allow an attacker to conduct remote code execution.

  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); Apache Struts2 Struts1_Plugin Remote Code Execution; Network Time Protocol Daemon peer xmit mode Denial of Service)*

- Mozilla has released security updates for Firefox ESR 52.4 and Firefox 56 addressing 18 vulnerabilities.

THREAT INTELLIGENCE REPORTS

- ZNIU rootkit is the first Android malware to exploit Dirty COW, a Linux vulnerability discovered in 2016. The malware infected over 5,000 victims in 40 countries, with high concentration in East Asia. ZNIU is being distributed via over 1,200 malicious applications, mostly disguised as gaming or porn applications.

  Check Point Sandblast Mobile customers are protected from this threat

- According to a new report, popular stocks trading applications contain vulnerabilities putting users at risk. The researcher behind the report has tested 21 popular trading applications in 14 security tests for design and technical security controls. Six of the tests had failure rates of over 50%.

- A new variant of BankBot mobile banking Trojan, disguised as a gaming application named Jewels Star Classic, has been found and removed from Google Play, after being downloaded 5,000 times.

  Check Point Anti-Bot customers are protected against this threat *(Trojan-Banker.AndroidOS.BankBot.*)*