August 10 - 16, 2020

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The SANS information security training institute has suffered a data breach comprised of 27,000 records of PII (Personally Identifiable Information) which were forwarded to an external email address. SANS traced the source of the attack to a phishing email.

- The city of Lafayette Colorado has fallen victim to a ransomware attack and paid the criminals' ransom demand of $45,000. The attack was not part of a targeted campaign and the undisclosed ransomware entered the city's systems through phishing or brute force attack.

- Sodinokibi ransomware group has compromised Jack Daniel's whisky manufacturer – the Brown-Forman spirits group. The threat actor claimed they spent a month inside Brown-Forman's systems and exfiltrated 1 TB of corporate data, but according to the company it stopped the attack before data was encrypted.

  Check Point SandBlast Anti-Ransomware provides protection against this threat

- Maze ransomware-gang has published a 2.2GB archive comprising of files allegedly stolen from Canon during a ransomware attack earlier this month.

  Check Point SandBlast Anti-Ransomware and Anti-Bot provide protection against this (Ransomware.Win32.Maze)

- Data of more than 200K users of Utah-based gun exchange sites has been leaked, and is offered free of charge on a cybercrime forum. According to researchers, the three leaked guns-related databases were all hosted on the same Amazon cloud server.

- The Israeli Defense Ministry has accused the North Korean related Lazarus APT group in targeting employees of major Israeli defense companies through fake LinkedIn profiles. Researchers said that unlike the group's regular financially motivated attacks, the current campaign was focused on technology theft.

VULNERABILITIES AND PATCHES

- Check Point Research has disclosed vulnerabilities in Amazon Alexa that could grant attackers access to users' chat history, banking data, usernames, phone numbers and other sensitive information. Possible attack vector requires user interaction by clicking a malicious link and then utilization of Amazon subdomain vulnerabilities, CORS misconfiguration and XSS to receive victim's CSRF token.

- Citrix has issued fixes for various vulnerabilities residing in its XenMobile Servers. Two of the vulnerabilities are rated critical and together they could allow unauthenticated attackers to take full control of the server.

- On this Patch Tuesday Microsoft has released updates for more than 120 vulnerabilities and bugs, including an Internet Explorer vulnerability actively being exploited (CVE-2020-1380) and various others.

  Check Point IPS provides protection against these threats (CVE-2020-1529, CVE-2020-1566, CVE-2020-1578, CVE-2020-1570, CVE-2020-1380, CVE-2020-1567, CVE-2020-1587, CVE-2020-1480, CVE-2020-1584)

- Attacks targeting a vulnerability in the vBulletin internet-forum-software have been detected shortly after a researcher disclosed it and published three PoC exploits. The new vulnerability is a bypass to an older fix of a 2019 vulnerability.

  Check Point IPS provides protection against this threat (vBulletin Forum Remote Code Execution (CVE-2019-16759))

- Adobe has released updates to address multiple vulnerabilities in its various products. Eleven of the 26 bugs are rated critical.

  Check Point IPS blade provides protection against these threats (CVE-2020-9711, CVE-2020-9707, CVE-2020-9710, CVE-2020-9713, CVE-2020-9706, CVE-2020-9705, CVE-2020-9697)

THREAT INTELLIGENCE REPORTS

- Researchers have reported of a previously unknown APT group dubbed RedCurl involved in business espionage. The Russian-speaking group has been active for at least three years. The group has targeted dozens of companies from various countries, initially compromising them through well-written phishing emails based on in-depth intelligence.

- The FBI and NSA have released details about a new Linux malware dubbed Drovorub, attributed to the Russian military affiliated APT28. Drovorub is a multipurpose tool capable of data exfiltration, remote code execution and more.

- A team of researchers has presented a new method of attack on mobile devices, which could let remote attackers break the encryption of voice calls and spy on targeted individuals. The method requires the attacker to be connected to the same base station and initiate a call to the victim.