Check Point
SOFTWARE TECHNOLOGIES LTD.

July 22 - 28, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- City Power, the electricity provider in the city of Johannesburg, South Africa, has suffered serious disruptions after a Ransomware attack. The attack prevented prepaid customers from buying electricity units and access City Power's official website, eventually leaving them without electricity power.

- New Android Spyware named "Monokle" has been spotted in targeted attacks and attributed to the Russian defense contractor Special Technology Centre (STC). Monokle presents sophisticated surveillance abilities and novel techniques to exfiltrate data including self-signing trusted certificates, recording a phone's lockscreen activity in order to obtain users' passcodes, and more.

  Check Point SandBlast Mobile provides protection against this threat

- Security researchers have discovered a novel steganography technique used by attackers to hack fully patched websites in Latin America. The attackers hide PHP scripts in Exchangeable Image Format (EXIF) headers of JPEG images that are uploaded on the website, then able to deploy malicious webshell.

- Credit company Equifax has to pay up to $700 million in fines after its infamous massive data breach in 2017 which exposed personal and financial data of nearly 150 million Americans.

- Security researches have spotted multistage attacks targeting unprotected or publicly available Elasticsearch Databases. The attacks deliver "Setag" and BillGates backdoors which can turn the infected targets into botnet zombies used in distributed-denial-of-service (DDoS) attacks.

  Check Point Anti-Virus blade provides protection against this threat *(Backdoor.Linux.Setag)*

- Security researchers have discovered a new strain of malware dubbed "Okrum" distributed by the Chinese cyber-espionage group APT15. Okrum is capable of downloading and uploading files, executing files and shell commands, and was spread within a PNG file with steganography technique to evade detection.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat *(Backdoor.Win32.Okrum)*

VULNERABILITIES AND PATCHES

- A critical remote code-execution vulnerability has been uncovered in the GlobalProtect portal and GlobalProtect Gateway interface security products of Palo Alto Networks, which provide virtual private network (VPN) access to an internal network.

  Check Point IPS blade provides protection against this vulnerability *(Palo Alto Networks GlobalProtect SSL VPN Remote Code Execution (CVE-2019-1579))*

- A Serious vulnerability has been discovered in the popular open-source ProFTPD file transfer protocol (FTP) server which is currently being used by over one million servers worldwide. The vulnerability could allow an attacker to copy files to vulnerable servers and potentially execute arbitrary code.

- VLC Media Player, used by more than 3.1 billion users, is exposed to a critical vulnerability that can allow attackers to execute code, create a denial of service state, disclose information, or manipulate files.

- A new severe code execution vulnerability has been discovered on the popular open-source office suite software "LibreOffice". The vulnerability could allow an attacker to craft a malicious document that can silently execute arbitrary python commands.

- A remote code execution vulnerability has been found in Adobe ColdFusion. The vulnerability is due to the JNBridge binary protocol port being exposed without any authentication.

  Check Point IPS blade provides protection against this vulnerability *(Adobe ColdFusion Remote Code Execution (CVE-2019-7839))*

THREAT INTELLIGENCE REPORTS

- Check Point Research has released its mid-year Cyber Attack Trends report for 2019; discussing targeted Ransomware attacks as prominent ongoing trend, the rising of software supply chain attacks and the attention it get worldwide, the growing sophistication of attacks in the mobile arena, and more.

- Security researchers have discovered a new variant of the Linux-based cryptocurrency mining botnet "WatchBog". The new variant added a module to scan the Internet for Windows RDP servers vulnerable to "Bluekeep", the highly-critical, wormable, remote code execution vulnerability.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat *(Botnet.Linux.WatchBog)*

- The government of Kazakhstan is beginning to intercept all HTTPS Internet traffic of its citizens. The local Internet Service Providers (ISPs) will allow access to the Internet only to customers who installed the government-issued root certificates.

- A security report shows that data for over 23 million payment cards has been offered for sale in the cybercrime underground in the first half of 2019, over 60% of them issued in the US.