June 24 - 30, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point researches have unveiled a long lasting large-scale campaign using Facebook pages to spread malware across mobile and desktop environments, aiming mainly at Libya. The campaign used political relevant content to lure victims into clicking links and downloading files containing the malware.

  Check Point SandBlast, SandBlast Mobile, SandBlast Agent, IPS, Anti-Bot and Anti-Virus blades provide protection against this threat

- A new malspam campaign has been discovered, spreading variants of LokiBot and NanoCore via ISO disk image file attachments. The ISO files contained the malicious binaries and allowed the attackers to bypass email security solutions which usually whitelist such file types.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Botnet.Win32.LokiBot; RAT.Win32.NanoCore)

- A new Linux-based Cryptomining malware has been spotted in the wild dubbed "LoudMiner", targeting Windows and macOS systems. LoudMiner leverages command-line based virtualization software to launch a Linux VM which already contains the hacker-activated cryptocurrency mining software in it.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Cryptominer.Win32.LoudMiner; Cryptominer.OSX.LoudMiner)

- "Silex" malware has been spotted bricking thousands of insecure IoT devices running on Linux or Unix. Developed by a 14-year-old hacker, Silex is capable of trashing the storage of the infected devices, wiping firewall rules and network configurations, then halting the system.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (DDoS.Linux.Silex; Trojan.Linux.Silex)

- A new ongoing Android espionage campaign, "ViceLeaker", has been discovered, spreading malicious repackaged versions of legitimate apps through third-party app stores or instant messengers. The malware is designed to steal surround audio recording, take over the camera, and more.

  Check Point SandBlast Mobile customers are protected from this threat

- The Russian tech giant Yandex has been hacked in an attack involving a new variant of Regin spyware. The attack, which is allegedly attributed to Five Eyes intelligence agencies, targeted the research and development department at Yandex and aimed to compromise the user authentication system.
- A second Florida city, Lake City, has agreed to pay $500,000 in ransom, after a Ransomware attack crippled the city's computer systems for two weeks. The attack, dubbed "Triple Threat", combined three different methods of attack to target network systems and locked phone and email systems.

VULNERABILITIES AND PATCHES

- Check Point security researchers have discovered a chain of vulnerabilities affecting Electronic Arts (EA) Games' login process. The vulnerabilities expose over 300 Million gamers to a potential hack, allowing an attacker to take over EA gamers' accounts and steal sensitive data including players' credit card data.
- A PoC has been released for the patched critical remote code execution vulnerability in Outlook app for Android which affects over 100 million users. The PoC reveals that the vulnerability could allow attackers to read app-related content including users' cookies, tokens and content of the email inbox.

  Check Point IPS blade provides protection against this threat (Microsoft Outlook for Android Cross-Site Scripting (CVE-2019-1105))

THREAT INTELLIGENCE REPORTS

- Security researches have uncovered that the Spelevo Exploit Kit is now spreading via a compromised business-to-business website. Threat actors infected multiple pages on the website which redirect to the infection chain, followed by Google as camouflage, while installing a banking Trojan in the background.

  Check Point IPS, Anti-Bot and Anti-Virus blades provide protection against this threat (Spelevo Exploit Kit Landing Page; SpelevoEK)

- New Mac malware dubbed "OSX/Linker" has been discovered under development and designed to exploit the unpatched bypass GateKeeper vulnerability, which allows attackers to execute unsigned payloads on an infected macOS systems without user consent.
- A new variant of the Dridex banking Trojan has been spotted delivered in phishing emails and introducing new advanced capabilities including new evasion techniques.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Banking.Win32.Dridex)

- On the last month various security researches have witnessed a halt in Emotet's operation as its C2's are down. The estimations are that Emotet it only down temporarily for maintenance and will be back.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Trojan.Win32.Emotet)