June 3 - 9, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- American Medical Collection Agency (AMCA) has suffered a major data breach exposing personal and payment information of some ten million patients. The information included names, date of birth, address, phone, date of service, provider, balance information, and credit card or bank account data.
- A campaign using a replica of the 'CryptoHopper' trading platform site to push various malware payloads has been uncovered. Upon victim's visit the site, Vidar information-stealing Trojan is automatically downloaded, then installing two additional malware: clipboard hijacker and Miner.

  Check Point Anti-Bot blade provides protection against this threat *(Infostealer.Win32. Vidar)*
- A new sophisticated botnet dubbed 'GoldBrute' has been revealed, brute-forcing over 1.5 million publicly accessible Windows RDP servers. In order to evade detection, each bot is equipped with a different set of user and password, thus targeted servers are being brute-forced from different IP addresses, each IP trying different credentials.
- Security researches have uncovered a malicious operation being hosted in Microsoft Azure cloud platform. The attackers abuse Microsoft Azure to deploy and host malware, phishing sites, and command and control server, and use an uncompiled file to evade security detection.
- Two hours of European mobile traffic have been rerouted through the infrastructure of China Telecom, China's third-largest telco and internet service provider (ISP). After a Gateway Protocol (BGP) route leak at Swiss data center of 'Safe Host' company, the Chinese ISP announced the leaked routes as its own.
- Security researches have uncovered a new wave of highly targeted attacks dubbed "Frankenstein campaign", dropping an infostealer on victims' machines. The attackers leveraged four different open-source techniques to build the tools used in the attacks, and employ multiple evasion techniques.

  Check Point IPS Anti-Bot and Anti-Virus blades provide protection against this threat *(Microsoft Office Memory Corruption Remote Code Execution (CVE-2017-11882); Trojan.Win32.Frankenstein)*

VULNERABILITIES AND PATCHES

- Check Point researchers have discovered vulnerabilities in Informir, a Ukrainian TV streaming platform, exposing over 1000 service providers' databases of personal and financial customer details. The vulnerabilities may also allow attackers to stream any content they choose on their customers' screens.

  Check Point IPS blade provides protection against this threat *(Infomir Ministra SQL Injection Remote Code Execution)*

- A 0-day vulnerability has been discovered in macOS. The vulnerability may allow a local attacker to bypass security and privacy features by performing 'Synthetic mouse-clicks' emulating users' consent to access sensitive data or components on the system such as camera, microphone and location data.

- A flaw in Windows Remote Desktop Protocol (RDP) has been found in the Network Level Authentication (NLA) feature recommended by Microsoft as a solution to the BlueKeep RDP vulnerability, and could allow client-side attackers to bypass the Windows lock screen on remote desktop sessions.

- A Microsoft Windows zero-day vulnerability has been found and named "ByeBear", abusing Microsoft Edge browser, and may allow attackers to bypass the recently patched elevation of privilege issue.

- Security researches have revealed a remote file injection vulnerability in Supra Smart Cloud TVs. The vulnerability may allow a local attacker with access to victim's WiFi network to broadcast any video.

THREAT INTELLIGENCE REPORTS

- New strain of malware has been spotted in the wild dubbed "BlackSquid", dropping XMRig miner and employing worm-like propagation capabilities. BlackSquid leverages 8 different exploits to target web servers, network drives, and removable drives, and implements evasion techniques to avoid detection.

  Check Point SandBlast, IPS and Anti-Bot blades provide protection against this threat *(Microsoft Windows EternalBlue SMB Remote Code Execution; Microsoft Windows DoublePulsar SMB Remote Code Execution; Apache Tomcat PUT Method Arbitrary File Upload Remote Code Execution (CVE-2017-12615); Trojan.Win32.BlackSquid)*

- A research reviewing "Scattered Canary" cybercrime group has discovered that the group evolved from a one-man operation into a highly-organized Business Email Compromise (BEC) giant, capable of operating multiple types of scams at the same time against enterprises and government institutions.

- A tool called "Jason" for hijacking Microsoft Exchange email accounts associated with the Iranian OilRig APT group has been leaked online through a Telegram channel.

- Security researchers have released a proof-of-concept (PoC) for a new type of attack dubbed "Tap 'n Ghost", targeting Near Field Communication (NFC)-enabled Android smartphones. The attack exploits flaws at both the software and hardware level and is capable of taking control of a victim device by inducing fake finger taps to conduct unwanted actions.