Check Point
SOFTWARE TECHNOLOGIES LTD.

Oct 18 – 24, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Russia-based REvil ransomware gang, responsible for the Colonial Pipeline and Kaseya attacks among others, has been hacked and taken-down by law enforcement groups and intelligence agencies from different governments. Following the news of REvil's take-down, the Groove ransomware gang is calling on other extortion groups to attack US targets.

  Check Point Harmony Endpoint provides protection against this threat

- New state-sponsored APT actor called Harvester is deploying an undocumented toolset in attacks targeting telecommunication providers and IT firms in South Asia, with a focus on Afghanistan, in an espionage campaign.

- An ongoing malware distribution campaign targeting South Korea is concealing Remote Access Trojans into an adult game and is being uploaded on WebHards and torrents.

- A threat group dubbed LightBasin (aka UNC1945) has been compromising mobile telecommunication systems worldwide since at least 2016. The nature of the data targeted aligns with information likely to be of significant interest to signals intelligence organizations.

- Google warns of widespread malware campaigns using YouTube videos to distribute password-stealing Trojans, specifically the Raccoon Stealer and RedLine malware, to unsuspecting viewers.

  Check Point Anti-Virus and Anti-Bot provide protection against these threats *(Trojan.Win32.Racoon; Infostealer.Win32.RedLine)*

- SCUF Gaming International, a leading manufacturer of custom PC & console controllers, has notified its customers that its website was hacked last February; Hackers planted a malicious script that was used to steal credit card information of 32,000 customers.

- Researchers have discovered a novel APT group using political and government themed malicious domains to target organizations in India and Afghanistan. The campaign delivers multiple Windows and Android Remote Access Trojan through the exploitation of CVE-2017-11882 and is distributed via malicious documents.

  Check Point IPS blade provides protection against this threat *(Microsoft Office Memory Corruption Remote Code Execution (CVE-2017-11882))*

VULNERABILITIES AND PATCHES

- Microsoft is asking system administrators to patch PowerShell 7 against two vulnerabilities (tracked CVE-2020-0951 and CVE-2021-41355) allowing attackers to bypass Windows Defender Application Control (WDAC) enforcements to run arbitrary code and gain access to plain text credentials.

THREAT INTELLIGENCE REPORTS

- Check Point Research has highlighted the leading brands that hackers imitated in attempts to lure people into giving up personal data in phishing campaigns; with Microsoft at the top (29%), followed by Amazon (13%), DHL (9%), Best Buy (8%), Google (6%) and WhatsApp (3%).
- Check Point Research discuss how hackers can potentially spread malware on Discord, the popular communication service used by over 150M people.
- The FBI has issued an advisory notice for the US public that threat actors are actively exploiting spoofed unemployment benefit websites to collect sensitive financial and personal information from victims.
- A free decryptor for the BlackByte ransomware is available, letting victims recover their files & data.
- Evil Corp cybercrime group has launched a new ransomware named Macaw Locker to evade US sanctions that prevent victims from making ransom payments and negotiate with Evil Corp.
- The FIN7 hacking group is masquerading into a fake cybersecurity company “Bastion Secure”, which claims to specialize in public sector cybersecurity services. Threat actors would perform network attacks with ransomware while pretending to perform penetration testing on the organizations’ systems.
- Researchers have found that the Microsoft-signed FiveSys rootkit has been targeting online gamers in China for over a year. The malware's main objective is to redirect and route internet traffic for both HTTP and HTTPS connections to malicious domains under the attacker's control via a custom proxy server, and can potentially steal credentials.
- Hackers are selling a stolen database collected between 2006 and 2019 containing 50 million records of Moscow car owners’ data for $800 only on an underground forum.
- CISA has warned of supply chain attack targeting the open-source UAParser.js NPM library infecting Linux and Windows devices with cryptominers and password-stealing Trojans.

For comments, please contact: TI-bulletin@checkpoint.com