Check Point SOFTWARE TECHNOLOGIES LTD.

Dec 20 – 26, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Researchers have revealed an APT-like campaign targeting the US Federal Government Commission on international rights and religious freedom. Threat actors used a backdoor that possibly gave them full visibility and control over the compromised network for further exploitation.

- New phishing campaign is luring victims into opening files containing malicious payload with fake employment termination notices or COVID-19 Omicron variant exposure warnings. Once the victim clicks on enable content, Dridex malware infects the device for credential theft purposes.

  Check Point Threat Emulation, Anti-Virus and Anti-Bot provide protection against this threat

- Belgium's ministry of defense has been hit by an attack exploiting the Log4j vulnerability, leaving parts of their network including their email system down for a few days to contain the attack.

  Check Point IPS provides protection against this threat *(Apache Log4j Remote Code Execution (CVE-2021-44228))*

- Over half a million Android users have downloaded “Color Message”, infected with Joker malware, from Google Play Store. The malware can extract contact list and subscribe users to unwanted paid services.

  Check Point Harmony mobile provides protection against this threat

- French IT service provider Inetum Group has announced it was victim of a ransomware attack which caused a limited disruption on their operations and customers. Hackers allegedly leveraged the BlackCat Ransomware (aka Noberus) which was unusually coded in Rust.

  Check Point Harmony Endpoint provides protection against this threat

- Log4shell exploits are used to drop Dridex Trojan on Windows machines, which can be used to collect banking credentials and to infect machines with ransomware. On Linux, it is used to drop Meterpreter.

  Check Point IPS, Threat Emulation and Anti-Bot provide protection against these threats *(Metasploit Meterpreter Reverse Payloads Remote Code Execution; Trojan.Win32.Meterpreter; Apache Log4j Remote Code Execution (CVE-2021-44228))*

VULNERABILITIES AND PATCHES

- Researchers have found multiple vulnerabilities in Microsoft Teams that could let hackers access internal Microsoft services, spoofing the link preview and leaking Android IP address or performing denial of service on their channels.
- Apple has released a patch for the bypass vulnerability CVE-2021-30853 in macOS that unauthorized script based applications could leverage. Once exploited, hackers can download and drop malicious payloads.
- Blackmagic Software has released updates to address two critical remote code execution security flaws in the DaVinci Resolve software tracked CVE-2021-40417 and CVE-2021-40418. The flaws, which do not require user interaction for exploitation, are activated when trying to decode a video file by a heap-based buffer overflow.
- Researchers have detected a vulnerability exploited since at least 2017, dubbed "NotLegit", in the Azure App Service exposing users' application source code written in PHP, Python, Ruby or Node.

THREAT INTELLIGENCE REPORTS

- New malware campaign called "Blister" has been found to be using valid code signing certificates to evade security detections in order to deploy Cobalt Strike beacons and BitRAT on vulnerable systems. The malware is disguised into "colorui.dll" and is delivered by "dxpo8umrzrr1w6gm.exe" dropper.
- CoinSpot cryptocurrency exchange users are being targeted by a new phishing campaign attempting to steal two-factor authentication credentials. Victims receive a socially engineered email, a CoinSpot looking template pushing the user into confirming or canceling a withdrawal transaction.
- The recently emerged ransomware operation Rook, usually dropped by Cobalt Strike via phishing email campaigns, was found to have ties with the Babuk ransomware codebase.
- AvosLocker ransomware operation have recently managed to reboot devices into Windows Safe Mode in order to attack endpoints without being detected, and then to easily encrypt victim's data.

  Check Point Anti-Virus provides protection against this threat *(HEUR:Trojan-Ransom.Win32.AvosLocker.gen)*
- Researchers have found a new alternative attack vector for the Log4j vulnerability, exploiting a Javascript WebSocket connection to activate the remote code execution on unpatched applications.

  Check Point IPS provides protection against this threat *(Apache Log4j Remote Code Execution (CVE-2021-44228))*