Dec 6 – 12, 2021

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research warns of potential ransomware attacks as samples of Emotet are fast-spreading via Trickbot. Since the Emotet takedown 10 months ago, CPR has spotted over 140,000 victims of Trickbot, across 149 countries, which might now be converted into Emotet, providing ransomware gangs a backdoor into compromised machines. Researchers found that the malware now drops Cobalt Strike beacons, giving immediate network access to threat actors and making ransomware attacks imminent.

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

- Nobelium, the Russian APT group behind the SolarWinds hack, is still targeting government targets and organizations networks around the world by using the new customized malware - “Ceeloader”. The French national cyber-security agency ANSSI has warned that the group has been targeting French organizations with spear-phishing campaigns since February this year.

- The Swedish automaker Volvo has suffered a security breach where some of its R&D data was stolen by a third party, which could potentially have an impact on the company’s operations.

- A Conti ransomware attack targeting Frontier Software, an external payroll software provider for the South Australian Government, has resulted in at least 80,000 government employees’ personal information and records being exfiltrated. Victims were advised to stay cautious with incoming emails, SMS or calls and to immediately reset their passwords.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win32.Conti)

- At least 300 branches of SPAR shops in northern England are facing operational problems after being hit by a cyber-attack that caused a “total IT outage”, forcing them to close many stores as credit card payments and emails weren’t available.

- Taiwanese hardware vendor QNAP has issued a warning concerning an ongoing campaign targeting their network-attached storage (NAS) devices with a new variant of cryptomining malware.

VULNERABILITIES AND PATCHES

- A severe zero-day vulnerability (CVE-2021-44228) in the Apache Log4j Java-based logging library has been reported: exploiting this flaw will allow threat actors to control java-based web servers and launch remote code execution attacks. Threat actors are already scanning for vulnerable servers to deploy different malware and crypto coin miners.

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

- SonicWall warns their customers using SMA 100 series appliances to immediately patch them, as multiple vulnerabilities could allow a threat actor to take control of an exploited system.

- Western Digital has patched a flaw (CVE-2021-36750) in SanDisk Secure Access which could let threat actors brute force passwords and eventually access users' protected data.

- Nearly 300,000 MikroTik RouterOS were found vulnerable to critical flaws that could be leveraged for a DDoS attack, including 20,000 devices that could inject cryptomining script into web pages.

  Check Point IPS provides protection against this threat *(MikroTik RouterOS Winbox Authentication Bypass; MikroTik RouterOS SMB Remote Code Execution)*

- The MANGA, aka Dark Mirai, DDoS botnet has been targeting unpatched TP-Link routers, exploiting a new vulnerability tracked CVE-2021-41653 that allows for remote command execution.

  Check Point IPS provides protection against this threat *(TP-Link TL-WR840N Router Command Injection (CVE-2021-41653))*

THREAT INTELLIGENCE REPORTS

- Check Point Research reveals that following Emotet's comeback after its takedown early this year, it is now the seventh most prevalent malware globally. Trickbot is once again in first place, and education and research are still the most targeted sectors.

- At least 1.6 million WordPress websites are currently being targeted by a campaign exploiting vulnerabilities in 4 plugins and 15 Epsilon Framework themes. The attacks involve updating the "users_can_register" & "default_role" settings to administrator, allowing actor to seize control.

- Threat actors are leveraging the Moobot botnet to exploit a remote code execution vulnerability tracked as CVE-2021-36260 to carry out DDoS attacks on the Chinese security camera provider Hikvision.

  Check Point Anti-Virus provides protection against this threat *(Trojan.Win32.Moobot)*

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