Check Point
SOFTWARE TECHNOLOGIES LTD.

Mar 22 - 28, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The official PHP Git server has been compromised in a potential attempt to plant a backdoor in the PHP source code, used by 80% of the websites on the internet. The threat was mitigated within a few hours, and the project migrated to GitHub to better control and prevent similar attacks in the future.
- Web shells deployed by the Black Kingdom ransomware operation group have been discovered on approximately 1,500 Exchange servers vulnerable to ProxyLogon attacks, mostly in the US. In some cases, the web shells were later used to install the ransomware.

  Check Point Harmony Endpoint provides protection against this threat
- US-based insurance company CAN has been hit by a new variant of Phoenix CryptoLocker ransomware, possibly linked to the Evil Corp threat group. The attack caused a network disruption and impacted certain CAN systems including corporate email.

  Check Point Harmony Endpoint provides protection against this threat
- Several members of the German Parliament have been hit by a targeted spear-phishing attack allegedly launched by the Russia-linked Ghostwriter threat group.
- Solarius Aviation, a US-based private aviation services provider, has announced that private data of some of its customers and employees was accessed by an unknown party. The data was breached when stored on the Microsoft Azure cloud environment of a third party vendor – Avianis.
- Sierra Wireless, a Canadian multinational manufacturer of Internet of Things devices, has suffered a ransomware attack disrupting internal operations and production facilities for several days.
- Guns.com has suffered a data breach following an attack that took place in January. The data posted this week on a popular darkweb forum contains substantial gun buyer information, including user ID, email addresses, hashed passwords, and physical addresses.

VULNERABILITIES AND PATCHES

- SolarWinds has released security updates that address multiple vulnerabilities affecting the Orion platform.
- Apple has released new out-of-band updates for iOS, iPadOs, macOS and watchOS to address a zero-day flaw actively exploited in the wild, tracked as CVE-2021-1879.
- A new vulnerability in the 5G core network allows data extraction and Dos attacks between network slices on a mobile operator leaving enterprise customers exposed to malicious cyberattack.
- Google has fixed a zero-day Android vulnerability affecting devices that use Qualcomm chips, which is actively exploited in the wild (CVE-2020-11261).

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed a new trend of forged negative COVID-19 test results and fake vaccine certificates offered on the Darknet and various hacking forums for people seeking to board flights, cross borders, attend events or start new jobs.
- The Federal Bureau of Investigation (FBI) has issued an alert to warn that the Mamba ransomware is abusing the DiskCryptor open-source tool to encrypt entire drives.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win32.Mamba)*

- Researches have spotted a new advanced Android spyware that implements exfiltration capabilities and surveillance features, including recording audio and phone calls and taking pictures, posing as “System Update”.

  Check Point Harmony Mobile provides protection against this threat

- Clop ransomware operators have been using a new technique to encourage their victims to pay the ransom – the hackers are now sending emails to victims’ customers, telling them they have access to their private information and asking them to demand the victim to pay the ransom, thus putting more pressure on the victim to pay.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win32.Clop)*

- Purple Fox malware, targeting Windows machines through phishing and exploit kits, has been supplemented with worm capabilities, propagating through SMB password brute-forcing.

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