Check Point
SOFTWARE TECHNOLOGIES LTD.

Jan 10 – 16, 2022

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Russia's Federal Security Service (FSB) has arrested several members of the REvil ransomware group, responsible for the JBS attack and the Kaseya supply chain attack, among others, after carrying out raids at 25 addresses across Russia. It is currently unknown whether leaders of the group have been detained.

  Check Point Harmony Endpoint provides protection against this threat

- Ukraine has been hit by a large scale cyber-attack that took down several of its government and ministries websites. Threat actors defaced the Foreign Affairs website with threatening message reading "Ukrainians!... All information about you has become public, be afraid and expect worse." Researchers additionally found evidence of a significant ongoing operation targeting multiple organizations in Ukraine, leveraging a malware disguised as ransomware that could render a system inoperable.

- German defense contractor Hensoldt has confirmed being victim of a ransomware attack which was claimed by the Lorenz ransomware gang. This financially motivated group is known to sell stolen data to other threat actors should victims refuse to pay the ransom.

- Albuquerque US Public Schools have had to cancel classes after they were hit by a cyber-attack that compromised the student information system. This event follows a ransomware attack that impacted multiple government services across Bernalillo County on January 5th.

- North Korean BlueNoroff group has been targeting cryptocurrency businesses, which led to serious financial losses. The threat actors try to manipulate their targets by pretending to be a venture capital firm and send them a fake contract or documents containing a backdoor with surveillance capabilities.

  Check Point Threat Emulation and Threat Extraction provide protection against this threat

- Goodwill nonprofit organization has disclosed a data breach on its e-commerce auction platform. Notifications were sent to individuals which have had their personal information including address, email and phone number exposed. Fortunately, the breach did not include credit card details which aren't stored on ShopGoodwill servers.

VULNERABILITIES AND PATCHES

- Apple has issued updates addressing a bug dubbed doorLock (CVE-2022-22588) in iOS and iPadOS that could be leveraged for denial-of-service (DoS) attacks. The vulnerability is initially exploited via HomeKit and will get triggered every time the device is rebooted.
- Amazon has fixed AWS "BreakingFormation" and "Superglue" security bugs that could let an attacker get credentials and eventually obtain full access to the internal API service and leak sensitive files.
- An unofficial patch for Windows Zero-Day vulnerability "RemotePotato0" has been issued. The privilege escalation flaw could let hackers obtain domain administrator privileges with an NTLM relay attack. The vulnerability was disclosed to Microsoft on April 2021, and is yet to be fixed by the vendor.
- Apple has released a patch for a vulnerability found in macOS dubbed "powerdir" (CVE-2021-30970), which could let threat actors bypass the operating system's Transparency, Consent, and Control (TCC) feature, and gain access to a user's protected data.
- A new unpatched Apple Safari 15 Browser vulnerability called "IndexedDB Leaks" has been disclosed. The flaw could allow for tracking users' online activity and possibly reveal their identity.

THREAT INTELLIGENCE REPORTS

- Check Point Research has revealed how APT35 (aka Charming Kitten), suspected to be an Iranian state-sponsored group, has been scanning and attempting to leverage the Log4j flaw with a new PowerShell backdoor, "CharmPower", in publicly facing systems, only four days after the flaw was disclosed.

  Check Point IPS provides protection against this threat (Apache Log4j Remote Code Execution (CVE-2021-44228))
- Check Point Research reports a 50% increase in overall cyber-attacks per week on corporate networks compared to 2020, with an all-time peak in Q4 2021.
- Check Point Research warns of a global surge in supply of fake vaccination and PCR/Antigen test certificates following the Omicron variant wave, with their price increasing by up to 600%.
- The US Cyber Command has officially linked the MuddyWater APT group to the Iranian Ministry of Intelligence and Security. The group specializes in espionage campaigns, with a focus on the Middle East.

  Check Point Threat Emulation, Anti-Virus and Anti-Bot provide protection against this threat
- The TellYouThePass ransomware has returned with a version written in the multi-platform coding language Golang, to facilitate its exploitations on macOS and Linux operated systems.

  Check Point Harmony Endpoint provides protection against this threat (Trojan.Win32.Tellyouthepass)