Jul 5-11, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Kaseya supply-chain ransomware attack has hit 1,500 organizations and breached the systems of roughly 60 of Kaseya's direct customers. After first demanding a $5 million ransom per MSP and $55K per customer for an individual decryptor, the Sodinokibi (REvil) threat group proposed to release a universal decryptor for $70 million, and afterward lowered their demand to $50 million.

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

- Kaseya has warned its customers about an ongoing phishing campaign that impersonates a Kaseya advisory and contains malicious links or attachments. Some of the phishing emails delivered the Cobalt Strike payloads while claiming to be a security update "to patch Kaseya vulnerability".

  Check Point Anti-Bot provides protection against this threat (Backdoor.Win32.CobaltStrike)

- The North Korean threat group Lazarus has conducted a phishing campaign impersonating Airbus, General Motors, and Rheinmetall, targeting engineers from Europe and the US. Malicious documents containing macros were used to perform arbitrary code injection into running processes on infected systems.

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

- Threat actors have hacked into the Accellion server of Guidehouse, a third-party vendor of Morgan Stanley, and stole information related to Morgan Stanley stock plan participants. The FIN11 cyber-crime group and the Clop ransomware gang were behind a series of recent Accellion hacks that might be related to this one.

- A spear-phishing campaign has been targeting the energy, oil & gas, and electronics industries for close to a year. The threat actors used social engineering techniques to lure employees into downloading malware such as AgentTesla, Loki, Formbook, and Snake Keylogger.

  Check Point Harmony Endpoint and Anti-Bot provide protection against those threats (Trojan.Win32.AgentTesla; Trojan.Win32.Ransomware.Win32.loki; Infostealer.Win32.Formbook; Backdoor.Win32.Snake)

- The district of Anhalt-Bitterfeld in Germany was the victim of a cyberattack that kept the district offline for more than a week, leaving them unable to pay welfare benefits and to finance youth programs.

- CNA Financial Corporation is notifying its customers that it was a victim of a ransomware attack by Phoenix. The personal information of over 75,000 individuals was stolen and over 15,000 devices were encrypted.

  Check Point Harmony Endpoint provides protection against this threat (Backdoor.Win32.Phoenix)

- Threat actors are targeting telecommunications organizations in Taiwan, Nepal, and the Philippines in an espionage campaign. Researchers suspect that the attacks were committed by TAG-22, a Chinese state-sponsored group. For initial access, the group used compromised GlassFish servers and Cobalt Strike, and then dropped the Winnti, ShadowPad, and Spyder backdoors.

  Check Point Threat Emulation and Anti-Bot provide protection against those threats (Backdoor.Win32.CobaltStrike; Backdoor.Win32.Winnti; Backdoor.Win32.Shadowpad)

VULNERABILITIES AND PATCHES

- Microsoft has released an emergency security update to fix the actively exploited PrintNightmare zero-day vulnerability. Shortly after, security researchers found out that the updates could be bypassed in specific scenarios. Microsoft claims that the current patch fixes the bug, although now non-admins can no longer install printer drivers to a print server and are no longer able to connect to receipt or label printers.

  Check Point IPS and Harmony Endpoint provide protection against this threat (Windows Print Spooler Remote Code Execution (CVE-2021-34527))

- Researchers have published a zero-day vulnerability for the Western Digital NAS devices. The flaw allows an unauthenticated threat actor to execute code as admin and install a permanent backdoor on WD's NAS devices that run My Cloud 3 OS. This OS is outdated and newer versions are not affected.

- QNAP has addressed a critical security vulnerability, CVE-2021-28809, which enables attackers to escalate privileges, execute commands remotely, or read sensitive info without authorization on NAS devices.

THREAT INTELLIGENCE REPORTS

- Researchers have observed a new RAT dubbed BIOPASS that targets online gambling companies in China. BIOPASS is used to spy on its victims, run commands, and for remote desktop access. The hackers distribute the RAT and a Cobalt Strike payload via a seemingly legitimate installer.

  Check Point Anti-Virus and Anti-Bot provide protection against this threat (RAT.Win32.Biopass; Backdoor.Win32.CobaltStrike)

- The FBI is warning exchange and crypto owners of an ongoing attack on virtual assets. In their attacks, the actors are using technical support fraud, SIM swapping, identity theft, and account takeover techniques.

- Approximately 93,000 people have bought fake Android cryptocurrency mining apps from two malware families. The malware, dubbed BitScam and CloudScam, were used to steal a total of $350,000. While almost 150 of the fake apps were sold on third-party app stores, 25 were available in the Google Play Store.