May 16 – 22, 2022

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has unveiled a targeted cyber-espionage operation against at least two research institutes in Russia, which are part of the Rostec Corporation, a state-owned defense conglomerate. The sophisticated campaign, which CPR dubbed “Twisted Panda”, has been attributed to Chinese threat actors, with possible connections to Mustang Panda and Stone Panda (aka APT10). Hackers used new tools, including a multi-layered loader and a backdoor called “SPINNER”.

- The Japanese financial news outlet Nikkei Group has suffered a ransomware attack that hit its headquarters in Singapore. The company, which is still in the process of determining the scope of the attack, claims that no data was leaked although the affected server may have contained customer data.

- Sberbank, a Russian banking services organization, has been the target of continuous attacks in the past month by Pro-Ukraine hackers. The bank recently suffered the largest distributed denial-of-service (DDoS) attack ever recorded, measured at 450GB/sec.

- Chicago Public Schools has suffered a breach that exposed 60,000 employees and 500,000 students’ data, including name, date of birth, gender, ID numbers and more, following a ransomware attack that occurred in December 2021 on one of their technology vendors, Battelle for Kids.

- The Parker Hannifin Corporation, a US based company that specializes in advanced motion and control technologies for the aerospace industry, has been victim of a Conti ransomware attack that resulted in the gang publishing the stolen data online last month. The stolen files included sensitive data of current and former employees such as financial account information, credentials, SSN and more.

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

- An unknown threat actor is targeting Ukraine supporters in Germany with a new campaign leveraging a custom PowerShell RAT malware. Hackers lure their victims with websites supposedly containing exclusive news about the conflict in Ukraine, serving the Trojanized documents instead.

  Check Point Anti-Virus and Anti-Bot provide protection against this threat *(Trojan.Win32.PowerShell; Trojan.WIN32.Powershell)*

VULNERABILITIES AND PATCHES

- Apple has released emergency updates to fix a zero-day vulnerability on Macs and Apple Watch devices. Tracked CVE-2022-22675, it is an out-of-bounds flaw in the AppleAVD that could lead to arbitrary code execution with kernel privileges.
- Cisco has issued a patch for IOS XR zero-day vulnerability tracked CVE-2022-20821, which is already exploited in the wild. The flaw could let a remote and unauthenticated hacker connect to a Redis instance that is running in the NOSi container and execute code.
- VMware has released fixes for two vulnerabilities affecting Workspace ONE Access, Identity Manager and vRealize Automation. Tracked CVE-2022-22972 and CVE-2022-22973, these flaws could be leveraged to backdoor enterprise networks.

THREAT INTELLIGENCE REPORTS

- The Conti Ransomware gang has allegedly taken its infrastructure offline after its leaders announced they were reorganizing their operation. The news comes a few days after Conti extorted Costa Rica, resulting in its government declaring a state of emergency. Conti members are believed to be currently migrating and rebranding into smaller ransomware operations.

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

- North Korean APT group Lazarus has been targeting VMware Horizon servers leveraging the critical remote code execution flaw Log4J (CVE-2021-44228) since at least April 2022. Threat actors proceeded by executing a PowerShell command that would lead to the installation of the NukeSped backdoor.

  Check Point Harmony Endpoint, IPS, Anti-Bot and Threat Emulation provide protection against these threats *(Apache Log4j Remote Code Execution (CVE-2021-44228); Trojan.Win32.NukeSped; APT.Win.Lazarus)*

- Threat actors are currently massively exploiting CVE-2021-25094, a remote code execution flaw in the Tatsu Builder plugin in WordPress, attached to 100,000 websites, of which 50,000 are still vulnerable.
- An increase of 254% has been detected in Linux XorDdoS malware activity in the past six months. This surge is apparently due to the Trojan's various evasion and persistence capabilities. XorDdos has been known since 2014 and is targeting Linux system architectures.

  Check Point Anti-Virus and Anti-Bot provide protection against this threat *(Trojan.Win32.Xorddos)*

- Phishing attacks are now leveraging Chatbot-like web applications to collect credentials, credit card information and other personal data.