TOP ATTACKS AND BREACHES

- A Chinese APT group dubbed Bronze Starlight (APT10) is attempting to use ransomware attacks mainly against Japanese companies, only as decoy to hide its true objectives – intellectual property theft and cyber espionage.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Win.Pandora.A)

- The Russian ransomware operation Conti has finally shut down their operation, a process that seems to have begun in May 2022. The group now shut down their data leak and ransom negotiation sites, and its members are presumed to have merged into other ransomware gangs.

- Kazakhstan and Italy are targeted by the sophisticated mobile spyware dubbed Hermit publishes. Android users have been notified on infected devices, infection which exposed them to sensitive data harvesting and to the enabling of audio recordings and redirecting phone calls.

  Check Point Harmony Mobile provides protection against this threat

- Unknown threat actors used a zero-day exploit on Linux-based Mitel MiVoice VoIP appliances (CVE-2022-29499) to gain initial access in a planned ransomware attack.

  Check Point IPS provides protection against this threat (Mitel MiVoice Connect Command Injection (CVE-2022-29499))

- The Raccoon Stealer malware used in the Rig Exploit kit has been replaced with Dridex banking Trojan as part of the ongoing campaign.

  Check Point IPS and Threat Emulation provide protection against these threats (RIG Exploit Kit Landing Page; Banker.Win.Dridex.*)

- Scalper bots have been used to secure appointments to government services in Israel with objective of selling them for high costs.

- Russian intelligence services have reportedly increased attacks against governments and NGOs supporting Ukraine in 42 different countries, with the goal to obtain sensitive information from NATO countries' agencies.

VULNERABILITIES AND PATCHES

- PyPi Python repository was used to send out AWS keys and environment variables as part of a supply chain attack, as threat actors managed to add malicious Python packages to it.
- Researchers discovered 56 vulnerabilities collectively dubbed as OT:ICEFALL, affecting devices from 10 operational technology (OT) vendors. Of the vulnerabilities, 38% allow credentials compromise, 21% allow firmware manipulation, and the rest allow RCE and changing of configuration information.
- MEGA disclosed a number of critical security issues in its cloud storage service that could be leveraged to break the confidentiality and integrity of user data. This by allowing a potential attacker to recover a user's RSA private key by tampering with 512 login attempts and decrypt the stored content.
- A critical remote code execution flaw has been reported in QNAP's Network Attached Storage (NAS) devices. These may by vulnerable to attacks that would exploit a three-year-old vulnerability.

  Check Point IPS provides protection against this threat *(PHP FastCGI Process Manager Remote Code Execution (CVE-2019-11043))*

THREAT INTELLIGENCE REPORTS

- Check Point Research shares recent findings on the Tropic Trooper threat cluster, which uses a previously undescribed loader ("Nimbda") written in Nim language in its activity. The cluster was so far observed targeting the Philippines, Hong Kong and Taiwan, and is bundled with a Chinese language greyware "SMS Bomber" tool that is most likely illegally distributed in the Chinese-speaking web.

  Check Point Threat Emulation and Anti-Bot provide protection against this threat *(Generic.Win32.Tropic Trooper*; Trojan.Win32.KeyBoy*)*
- Researches have provided an initial dive into the activity of an unknown APT dubbed ToddyCat, which has been targeting Microsoft Exchange servers of several high profile entities in Europe and Asia since December 2020. Attribution remains unknown.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Loader.Wins.ToddyCat*)*
- Researchers spotted a new malware tool named Quantum for sale on cybercrime forums. The tool could allow threat actors to create malicious .LNK files (Windows shortcuts) to deliver payloads, to use in initial stages of attack. The Quantum tool offers UAC bypass, Windows Smartscreen bypass, the ability to load multiple payloads on a single LNK file, post-execution hiding, startup or delayed execution.

  Check Point Anti-Bot provides protection against this threat *(Quantum.TC.*)*