TOP ATTACKS AND BREACHES

- Twitter has suffered a data breach after threat actors used a vulnerability to build a database of phone numbers and email addresses belonging to 5.4 million accounts, with the data now up for sale on a hacker forum for $30,000. It has been reported on a stolen data market that the database contains info about various accounts, including celebrities, companies, and random users.

- Digital security giant Entrust suffered a cyberattack where threat actors breached their network and stole data from internal systems. This could potentially impact some of Entrust's customers, including US government agencies such as the Departments of Energy, Homeland Security, Treasury and others.

- LockBit added several new companies to their victims list, including Madco Energi, Clestra, COIC Fiber, Columbia Grain, FarmaOffice, Christiana Spine Center, Rogagnati, and Redox Brands. The Canadian town of St. Marys, Ontario, has also been hit by Lockbit, which encrypted data and locked staff out of internal systems.

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

- LV ransomware gang has launched an attack against Finland-based company Wartsila, one of the largest manufacturers of machinery and electrical equipment for the marine and energy markets worldwide. More than 2000 GB of data were leaked.

- A new attack campaign has been observed, possibly linked to APT37, a North Korean group of hackers, targeting high-value organizations in the Czech Republic, Poland, and other European countries using malware known as Konni, a remote access Trojan (RAT).

  Check Point Threat Emulation and Anti-Bot provide protection against this threat *(Trojan.WIN32.KONNI)*

- The pro-Russian group Killnet declared that they are moving away from DDoS to a new type of more impactful cyberattacks, claiming their next target would be Lockheed Martin.

- Security researchers have disclosed recent campaigns carried out by Russian APT29 where the group provided a lure of an agenda for an upcoming meeting with an ambassador. These campaigns are believed to have targeted several Western diplomatic missions between May and June 2022.

VULNERABILITIES AND PATCHES

- Australian software firm Atlassian warned customers to immediately patch a critical vulnerability that provides remote attackers with hardcoded credentials to log into unpatched Confluence Server and Data Center servers.
- SonicWall has published a security advisory to warn of a critical SQL injection flaw impacting the GMS (Global Management System) and Analytics on-prem products, tracked as CVE-2022-22280. SonicWall recommends to upgrade to GMS 9.3.1-SP2-Hotfix-2 or later and Analytics 2.5.0.3-Hotfix-1 or later in order to stay protected.

THREAT INTELLIGENCE REPORTS

- Check Point Research published its Q2 Brand Phishing Report, highlighting the brands that cyber criminals most often imitate to trick people into giving up their personal data. In the last quarter, the social media platform LinkedIn continued its reign as the most imitated brand after entering the rankings for the first time in Q1.
- Details have emerged on how the Conti ransomware gang breached the Costa Rican government, showing the attack's precision and the speed of moving from initial access (through compromised VPN credentials) to the final stage of encrypting devices. This is the last attack from the Conti ransomware operation before the group's members spread out between different cybercrime groups.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
- Windows 11 is getting a new security setting to block connections and lock machines attacked by RDP password brute-force, a method often used by ransomware operators.
- A new undocumented spyware named CloudMensis was discovered targeting Apple macOS. The malware uses public cloud storage services to receive commands and exfiltrate files.
- Security researchers have found the new STOP247 ransomware that appends the .stop extension and drops a ransom note named RECOVERY_INFORMATION.TXT.
- Security researchers revealed a new ransomware family dubbed Luna that can be used to encrypt devices running several operating systems, including Windows, Linux, and ESXi systems. The group has managed to attack more than forty different victims within a very short time.