TOP ATTACKS AND BREACHES

- The LockBit Ransomware gang has claimed the attack on Italy's tax agency, the Internal Revenue Service. According to LockBit's message on their dark web site, the group stole 100 GB of sensitive data, including financial reports, contracts and other documents that they threaten to leak online if the victim does not pay the ransom demand until August 1.

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

- An Austria-based threat actor dubbed KNOTWEED has been exploiting vulnerabilities in Windows and Adobe, including CVE-2022-22047, to deploy their malware, Subzero, on highly targeted victims located in Europe and Central America.

  Check Point IPS provides protection against this threat *(Microsoft Windows Client/Server Runtime Subsystem Elevation of Privilege (CVE-2022-22047))*

- A North-Korea affiliated actor named SharpTongue (aka Kimsuky) has been spotted in a new campaign stealing Gmail and AOL users' webmail. The actor is leveraging a malicious browser extension called SHARPTEXT that is supported on Chrome, Edge and Whale.

  Check Point Anti-Virus and Anti-Bot provide protection against this threat *(Trojan.Win32.kimsuky.TC; Backdoor.WIN32.Kimsuky.A)*

- Researchers found "CosmicStrand", a new kind of UEFI firmware rootkit attributed to a Chinese-speaking malicious actor. Victims are located in China, Vietnam, Iran and Russia, all private individuals without ties to a specific industry or organization.

- NetStandard, a US based managed service provider (MSP) has been victim of a cyberattack forcing the company to shut down its main site and cloud services. The company stated that only the MyAppsAnywhere services were impacted. There is speculation that the attack was conducted by a Russian-speaking actor who posted claims on a hacker forum claiming to have breached an MSP.

- Threat actors who go by the name "Adrastea" claim to have breached the multinational manufacturer of missiles MBDA. They allegedly stole 60 GB of data including contract agreements and more employee and customer private information.

VULNERABILITIES AND PATCHES

- Atlassian Confluence critical vulnerability tracked CVE-2022-26138 is currently being exploited in the wild. Unauthenticated actors could leverage the flaw remotely to gain unrestricted access to all pages in confluence. In addition, CISA issued a warning and ordered US federal agencies to address the vulnerability by August 19.

- Two vulnerabilities were patched in FileWave's platform. CVE-2022-34907, an authentication bypass, and CVE-2022-34906, a hard-coded cryptographic key, both remotely exploitable. The flaws concern FileWave's mobile MDM system, potentially affecting thousands of organizations.

- Threat actors have been exploiting a zero-day vulnerability in the PrestaShop e-commerce platform. Tracked CVE-2022-36408, the flaw will let threat actors perform arbitrary code execution into websites that use the platform and steal customers' data.

  Check Point IPS provides protection against this threat *(PrestaShop Command Injection (CVE-2022-36408))*

THREAT INTELLIGENCE REPORTS

- Check Point Research reported a peak of 1.2K weekly cyber-attacks per organization worldwide in Q2 2022 - a 32% increase year-over-year. In addition, CPR saw a 59% increase of organizations impacted by ransomware attacks.

- The info stealing malware Amadey has been found to be distributed by the SmokeLoader backdoor. The Amadey Botnet that has been sold on underground forums for several years is also capable of dropping other malware.

  Check Point Harmony Endpoint, Threat Emulation, Anti-Virus and Anti-Bot provide protection against these threats
  (Trojan.Win.Amadey; Trojan-Downloader.Win.Smokeloader)

- Researchers found that the latest LockBit Ransomware variant, LockBit 3.0, shows similarities with BlackMatter ransomware.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.Lockbit; Trojan-Ransom.Win32.BlackMatter)

- The US Federal Communications Commission (FCC) has issued a warning concerning the increase of SMS phishing (or "smishing") campaigns.

- Luca Stealer's source code has been posted on hacking forums. The info-stealer malware written in Rust currently only targets Windows operated systems.