TOP ATTACKS AND BREACHES

- Uber has suffered a data breach, allegedly by an 18-year-old hacker who managed to gain access using social engineering tactics on an employee. The hacker claims to have access to Uber's internal IT systems and to the company's HackerOne bug bounty account, which contains vulnerabilities in Uber's systems and apps, disclosed privately by security researchers. Uber claims that the users' private information was not compromised.

- The New York based emergency response and ambulance service Empress EMS confirmed they have suffered a ransomware attack in July, which led to a data breach that exposed customer information. Hive ransomware is suspected to be behind the attack.

- Starbucks's Singapore division suffered a data breach that potentially affected over 219,000 of its customers who have used the chain's mobile app. The data has been offered for sale in a popular underground hacking forum.

- The FBI warns of cybercriminals targeting healthcare payment processors with the goal of stealing millions of dollars, redirected into their financial accounts. The hackers used known methods like social engineering and have already stolen about $5 Million from healthcare companies in only 3 incidents.

- The legislature of Argentina's capital city reported it was hit by a ransomware attack this week, saying that its internal operating systems were compromised and WiFi connectivity was down. No ransomware group has taken credit yet.

- The Russian affiliated Gamaredon group continues targeting Ukrainian entities using a new info-stealing malware that can exfiltrate specific files.

  Check Point Threat Emulation provides protection against this threat (InfoStealer.Win.Gamaredon)

- A new record-breaking DDoS attack in has been recorded this week, peaking at 704.8 Mpps, about 7% higher than the attack recorded on the same European organization last July.

- Researchers suggest that Lorenz ransomware gang exploits a critical remote code execution vulnerability in Mitel MiVoice VOIP appliances (tracked CVE-2022-29499) in their activity against enterprises and corporate networks.

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

VULNERABILITIES AND PATCHES

- Apple released security updates to a zero-day local privilege escalation kernel issue (CVE-2022-32917) exploited by attackers in the wild, affecting devices with macOS, iOS 16, and iOS and iPadOS 15.7.
- Microsoft issued fixes for 63 flaws in its patch Tuesday, five are critical; one is an actively exploited Windows vulnerability in Windows Common Log File System Driver (tracked as CVE-2022-37969).
- A critical zero-day privilege escalation flaw (CVE-2022-3180) in WordPress plugin is actively exploited.

  Check Point IPS provides protection against this threat *(WordPress WPGateway Plugin Privilege Escalation (CVE-2022-3180))*

THREAT INTELLIGENCE REPORTS

- Check Point Research found that in August 2022, FormBook replaced Emotet as the most prevalent malware. Also, the Android spyware Joker is back, taking 3rd place in the top mobile malware list; and Apache Log4j Remote Code Execution returns to 1st place as the most exploited vulnerability.

  Check Point Threat Emulation, Harmony Endpoint and IPS provide protection against this threat
  (InfoStealer.Win.Formbook; Backdoor.Win.SysJoker, Backdoor.Wins.SysJoker; Apache Log4j Remote Code Execution (CVE-2021-44228))

- Following Check Point Research mid-year Trends Report, CPR covers again the discoveries 2022 has brought to the mobile malware landscape: The spyware marketplace thrives, with Pegasus as one of the most powerful tools on the market; zero-click attacks and Smishing attacks (SMS Phishing) become more common than ever, and application stores prove as less and less safe.
- Researchers found that Quantum and BlackCat ransomware gangs are using Emotet malware to deploy their payloads, similarly to the way Conti gang has used the infrastructure in the past.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
  (Ransomware.Wins.BlackCat)

- The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) announced sanctions against individuals and entities sponsored by Iran's IRGC, including three Iranian personas who have targeted hundreds of victims - including critical infrastructure organizations - in the U.S., the UK and Israel since October 2020.
- Researchers share detailed findings on OriginLogger malware, a variant with similar features and behavior of the widely used information stealer and RAT, Agent Tesla.

  Check Point Threat Emulation and IPS provide protection against this threat *(Trojan.Win.AgentTesla; Trojan.Win.Agenttesla; Agent Tesla Panel Remote Code Execution; Agent Tesla Exploitation Attempt)*