TOP ATTACKS AND BREACHES

- Check Point warns of a recent Email phishing campaign abusing the data visualization tool - Google Looker Studio. Attackers use the tool to send slideshow emails to victims from official Google accounts, instructing them to visit 3rd party websites to collect cryptocurrency. The websites will then prompt the victims to input their credentials and thus to steal them.

  Check Point Harmony Email provides protection against this threat.

- $41M in cryptocurrency have been hijacked from the Curaçao based online casino Stake.com. According to the company, only its own funds were impacted, while customers' accounts were not compromised. The FBI has attributed the attack to the North Korean Lazarus APT group, which is notorious for having stolen large amounts of cryptocurrency in recent years.

- Ransomware group Ragnar Locker has leaked 400GB of information that it claims to have exfiltrated in a breach of an Israeli hospital Mayanei HaYeshua last month. The attack forced the hospital to suspend its network operations a brief period. The group allegedly holds a total of 1TB of information, including patients' medical details, and threatens to disclose it if its ransom demands are not met.

- United States security agencies have uncovered an Iranian nation-state cyber campaign operated by multiple threat groups, and targeting a US aeronautical organization. The attackers exploited Zoho ManageEngine vulnerability CVE-2022-47966 to gain access to the organization's network, as well as Fortinet vulnerability CVE-2022-42475 to establish persistence on the organization's firewall.

  Check Point IPS provides protection against those threats *(Zoho ManageEngine Remote Code Execution (CVE-2022-47966), Fortinet FortiOS Heap-Based Buffer Overflow (CVE-2022-42475))*

- The city of Seville, Spain, has suspended all digital activity after being hit by a ransomware attack. The city has announced that it refuses to negotiate with the ransomware group LockBit, which had assumed responsibility for the attack and demanded a ransom of $1.5M.

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

- Hong Kong high technology business compound Cyberport has disclosed a breach of its network. The Trigona ransomware group has assumed responsibility for the attack.

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

VULNERABILITIES AND PATCHES

- Apple has released security patches for two zero-day remote code execution vulnerabilities affecting its products, which were actively exploited in the wild. The vulnerabilities allow attackers to gain control of victims' devices by sending malicious images, without any interaction required on the victim's side ("zero-click"). The usage of the vulnerabilities was attributed to Israeli company NSO's Pegasus spyware.
- Cisco has published advisories for multiple vulnerabilities affecting the company's products. The vulnerability CVE-2023-20238 is a critical pre-authentication remote code execution vulnerability which affects the BroadWorks Application Delivery and Xtended Services platforms. Another vulnerability, CVE-2023-20269, is a credential-theft vulnerability affecting Cisco ASA and Cisco FTD, and according to Cisco is active exploited by the Akira ransomware group, and has yet to be patched.
- Redwood Software has patched its JSCAPE MFT Server product to cover a Java deserialization arbitrary code execution vulnerability, CVE-2023-4528. MFT servers are increasingly targeted by ransomware groups recently, as breaching them allows access to data held by many companies.
- Google has published Android's September security advisory, which includes fixes for 33 vulnerabilities. Among the vulnerabilities addressed is CVE-2023-35674, a high severity privilege escalation vulnerability that has been actively exploited in the wild prior to the patch.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have analyzed the potential impact of the emerging generative AI technology on election influencing operations. Generative AI is capable of constructing individually tailored audio-visual propaganda to target voters on a massive scale, causing a heightened risk to democratic election integrity. To combat the issue, Google will require disclosure on political advertisements involving AI.
- Ukraine's CERT has identified a campaign operated by the Russian nation state group APT-28 targeting a Ukrainian critical energy infrastructure facility. The threat actors used targeted phishing emails as the initial attack vector to distribute the malware.
- Researchers have found a novel attack targeting an organization using the MinIO cloud framework. The attackers managed to convince the target to update its environment to a vulnerable version, and used a series of vulnerabilities discovered this year to try and gain control of the victims' network.
- An Android spyware campaign targeting the Uyghur minority has been discovered. The campaign, which was attributed to a Chinese APT group, utilized modified versions of the Telegram and Signal Android apps that were available on the official Google Play platform. When installed, the apps allowed the attackers to spy on victims' devices.