TOP ATTACKS AND BREACHES

- Two major automotive manufacturers Hyundai and Toyota have disclosed significant data breaches. Hyundai's Italian and French car owners were affected, along with individuals who booked a test drive. The leaked data consists of clients' personal information including emails, addresses, phone numbers, and vehicle chassis numbers. The Japanese automaker Toyota confirmed that the breach on their side exposed a large amount of sensitive information including API tokens for the software business Mapbox as well as credentials to digital marketing platform Salesforce Marketing Cloud, which could be used to reach out to the company's clients.

- The media player maker Kodi has disclosed a data breach that caused a leakage of more than 400K records of its users' forum. The threat actors published the organization's MyBB forum database for sale on underground forums, including usernames, email addresses, encrypted (hashed and salted) passwords, public forum posts, staff forum posts, and private messages.

- Ukrainian hacktivists group Cyber Resistance has leaked personal information of Sergey Morgachev, the alleged leader of the Russian state-sponsored group APT28 (Fancy Bear) and Russia's Main Intelligence Directorate of the GRU. The leaked data consists of email, social media, and personal accounts.

  Check Point Harmony Endpoint provides protection against this threat (APT.Win.Fancybear)

- Karakurt ransomware extortion group claims to have attacked two US medical entities: Medicalodges in Kansas, and Petaluma Health Center in California. The threat actors claimed they have access to 170GB of Medicalodges data, including social security numbers, client NDAs, and medical diagnoses.

- Belgian HR and Payroll Company SD Worx has been a victim of a cyber-attack that caused a shutdown of IT systems in its UK and Ireland divisions. It is still unclear whether any sensitive data was stolen during this incident.

- German biotech company Evotec has suffered a cyber-attack prompted the company to shut down its digital infrastructure. The company confirms that business is continuing at all sites, although the systems are currently not connected to the network.

- Intelligence documents containing "Top Secret" information were leaked through online Discord channels. The leaked information includes data related to Russia's invasion of Ukraine, analysis of potential UK policies on the South China Sea and the activities of a Houthi figure in Yemen.

VULNERABILITIES AND PATCHES

- Check Point Research has discovered three vulnerabilities (CVE-2023-28302, CVE-2023-21769 and CVE-2023-21554) in the "Microsoft Message Queuing" service, commonly known as MSMQ. The most severe of these, dubbed QueueJumper by CPR (CVE-2023-21554), is a critical vulnerability that could allow unauthenticated attackers to remotely execute arbitrary code in the context of the Windows service process mqsvc.exe.

  Check Point IPS provides protection against this threat *(Microsoft Message Queuing Remote Code Execution (CVE-2023-21554))*

- Microsoft's Patch Tuesday fixes 97 flaws, including one actively exploited zero-day vulnerability (CVE-2023-28252), a privilege elevation vulnerability in the Windows CLFS driver that elevates privileges to SYSTEM, the highest user privilege level in Windows. This vulnerability was first spotted used by Nokoyawa ransomware group.

- Enterprise software vendor SAP has released its April 2023 security updates for several of its products, including three critical-severity vulnerabilities (CVE-2023-27267, CVE-2023-28765 and CVE-2023-29186) impact SAP NetWeaver, SAP BusinessObjects Business Intelligence Platform and OSCommand Bridge of SAP Diagnostics Agent.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports that Emotet which had new malware campaigns during the last month, rose to become the second most prevalent malware. Ahmyth Remote Access Trojan (RAT) was the most prevalent mobile malware and Log4j took top spot once again as the most exploited vulnerability, impacting 44% of organizations globally.

  Check Point Harmony Endpoint, Threat Emulation, and IPS provide protection against those threats *(Trojan.Win.Emotet; Exploit_Linux_CVE-2021-44228; Apache Log4j Remote Code Execution (CVE-2021-44228))*

- Check Point Research flags a sharp increase in cyberattacks targeting IoT Devices, with 41% increase in the average number of weekly attacks per organization during the first two months of 2023, compared to 2022. On average, every week, 54% of organizations suffer from attempted cyber-attacks targeting IoT devices, mostly in Europe followed by APAC and Latin America.

  Check Point Quantum IoT Protect provides protection against this threat

- Check Point Research warns about an increase in discussions and in trade of stolen ChatGPT accounts, with a focus on Premium accounts. Cyber criminals leak credentials to ChatGPT accounts, trade premium ChatGPT account and use Bruteforcing tools for ChatGPT, which allow cyber criminals to get around OpenAI's geofencing restrictions and get access to the previous queries of existing ChatGPT accounts.