TOP ATTACKS AND BREACHES

- The Swedish-Swiss multinational automation company ABB has been a victim of a ransomware attack conducted by the Russian Black Basta ransomware group. The threat actors have attacked the company's Windows Active Directory, affecting hundreds of devices. To prevent the spread of ransomware to its customers, ABB terminated VPN connections with other networks.

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

- The Japanese automaker Toyota has suffered a ten years long data breach resulting in the exposure of vehicles information of more than 2M clients in Japan. The breach was due to a cloud database misconfiguration that allowed anyone to access its contents without a password. The exposed data includes car locations with time stamps, chassis numbers and the in-vehicle GPS navigation terminal ID number.

- The US healthcare software provider NextGen Healthcare has informed of a data breach that compromised the personal data of more than 1M patients. The threat actors managed to access patients' names, dates of birth, addresses and Social Security numbers.

- Sysco, the American food distribution company, has disclosed a data breach that exposed the data of customers and suppliers in the US and Canada, as well as Social Security numbers and account numbers of its US employees.

- The data storage giant Western Digital has confirmed a data breach that exposed the personal information of the company's clients. The leaked data includes names, billing and shipping addresses, email address and phone numbers. The threat actors claimed they are not affiliated with the AlphV (aka Black Cat) ransomware gang but would use that group's leak site to threaten and extort the company.

- The online chat platform Discord has notified about a data breach caused by a third-party ticket support agent account that was hacked. The attack has exposed users' data, including email addresses, customer service messages, and tickets attachments.

- The Korean Seoul National University Hospital (SNUH) has been a victim of a data breach, affecting 831K patients and employees. The attack has conducted by North Korean threat actors, which targeted the hospital's internal network to gain sensitive medical information and personal details. Local media in South Korea linked the attack to the Kimsuky APT group.

VULNERABILITIES AND PATCHES

- Microsoft's Patch Tuesday fixes 38 flaws, including three zero-day vulnerabilities. Among those is the Windows OLE flaw (CVE-2023-29325) in Microsoft Outlook that can be exploited using specially crafted emails. Successful exploitation could result in the execution of remote code on the victim's machine.

  Check Point IPS provides protection against this threat *(Microsoft Windows OLE Remote Code Execution (CVE-2023-29325))*

- Researchers have discovered a new Linux NetFilter kernel flaw (CVE-2023-32233) that allows unprivileged local users to escalate privileges and gain complete control on the affected system.

- An unauthenticated privilege escalation vulnerability (CVE-2023-32243) has been disclosed in the popular Wordpress plugin Essential Addons for Elementor. The flaw allows unauthenticated users to elevate their privilege to reset the password of any user, including administrators.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released April 2023's threat index, highlighting a substantial malspam campaign of Trojan Qbot, which came second in the index. Meanwhile, Internet-of-Things (IoT) malware Mirai made it back on the list for the first time in a year, and Healthcare moved up to become the second most attacked industry.

  Check Point Harmony Endpoint and Threat Emulation provide protection against those threats *(Trojan.Wins.Qbot; Trojan.Downloader.Win.Qbot; Banker.Wins.Qbot; Trojan.Wins.Mirai)*

- A new ransomware family dubbed Maori has been analyzed by researchers. The variant, written in Go, targets Linux platforms, and encrypts only the Home directory, which allows a very quick encryption process.

- Researchers have discovered a new APT dubbed Red Stinger (aka Bad Magic), targeting military, transportation and critical infrastructure related to the Russo-Ukrainian conflict. The threat actors managed to exfiltrate snapshots, USB drives, keyboard strokes, and microphone recordings for surveillance and data collection purposes.

  Check Point Threat Emulation provides protection against this threat *(Technique.Win.PowerShellBase64.D, Trojan.Win.PowerMagic.A, Technique.Win.MalScript.Ia.B, Dropper.Win.GenDrop.Ia.J, Technique.Win.MalMsi.Ia.A)*

- A joint cybersecurity advisory regarding the Russian FSB's Snake malware has been published by American, English, Canadian and Australian security agencies. The malware is used to gather intelligence from sensitive targets, and its infrastructure been observed by security agencies in more than 50 countries.