TOP ATTACKS AND BREACHES

- Shared Services Connected Ltd, a payroll contractor for the UK Ministry of Defense has been breached, assumingly by China. Around 270k records that include names and bank details of both current and past armed forces members were exposed.

- US major healthcare operator Ascension, which operates 140 hospitals in 19 states, has disclosed a cyber-attack that has affected its systems, causing disruptions to its clinical operations. The threat actors blocked access to electronic health records, phone systems and various systems utilized to order certain tests, procedures, and medications.

- Technology giant Dell has disclosed a data breach impacting approximately 49M customers, after the company's database was advertised on a dark-web hacking forum. The exposed data includes purchase details such as full names, home addresses, and order information. According to Dell, contact information and financial data remains uncompromised.

- The City of Wichita, US, was hit by a ransomware attack that resulted in the shutdown of WiFi and departure screens at the city's airport and forced city services to revert to cash payments. LockBit ransomware group claimed responsibility for the attack.

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

- The known threat actor IntelBroker claimed responsibility for significant data breach on the Europol Platform for Experts (EPE) portal. Europol confirmed the breach but claimed that no operational data was stolen.

- Threat actor has breached and leaked the personal and biometric data of over 5M El Salvador's citizens. The exposed data includes sensitive personal information such as full names, email addresses, date of birth, residential addresses, identification documents (DUI), and IDs.

- MedStar Health has confirmed a significant data breach that led to the exposure of sensitive data of approximately 183K patients. The leaked data includes patients' names, email address, dates of birth, dates of service, provider names and health insurance information.

- Scottish healthcare system NHS Dumfries and Galloway has experienced a ransomware attack that led to the exposure of children's health records. The attack is currently attributed to the INC Ransom group, who posted some of the sensitive data on its extortion site as evidence.

VULNERABILITIES AND PATCHES

- Google releases a patch to the Chrome browser for both Mac and Windows to address the fifth zero-day exploited in the wild since early 2024. The flaw, CVE-2024-4671, is a high-severity "use after free" vulnerability in the Visuals component that handles the rendering and display of content on Chrome browser. Successful exploitation could lead to various outcomes, from resulting a crash to enabling arbitrary code execution.

- Citrix has disclosed a security flaw, CVE-2024-31497, in the PuTTY SSH client bundled with XenCenter for Citrix Hypervisor 8.2 CU1 LTSR. This flaw could potentially enable attackers to gain access to the private SSH keys of XenCenter administrators.

- Two high-severity command injection vulnerabilities, CVE-2024-21793 and CVE-2024-26026, have been observed in F5 BIG-IP Next Central Manager. Successful exploitation could allow a remote attacker to get admin access to create accounts that wouldn't be visible from the Next Central Manager itself, enabling ongoing malicious persistence within the environment.

THREAT INTELLIGENCE REPORTS

- Check Point Research's April 2024 Most Wanted Malware report highlights a surge in Androxgh0st attacks, a Trojan affecting Windows, Mac, and Linux systems to steal sensitive data. Concurrently, LockBit3, despite its active status in April, experienced a 55% decline in public extortion from the start of the year, dropping its global impact from 20% to 9% in the ranking of ransomware groups.

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

- Law enforcement agencies from the US, the UK and Australia have unmasked and sanctioned Dmitry Khoroshev, known as LockBitSupp, who leads the LockBit ransomware group. This revelation is part of a broad international effort involving law enforcement collaborations against LockBit group.

- Polish CERT reports a large-scale malware campaign conducted by Russian threat group APT28, which is linked to the Russian GRU, targeting Polish government entities. The attacks involve deceptive emails and malicious software designed to compromise official communications and gather sensitive data.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (APT.Win.APT28.; APT.Wins.APT28.ta.*)*

- The FBI has issued a warning about Storm-0539 hacking group, that has been targeting US retail companies' gift card departments since January 2024. The group employs sophisticated phishing techniques to compromise employee accounts, enabling them to bypass multi-factor authentication, access corporate systems, and facilitate the creation and redemption of fraudulent gift cards.