Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Cyber criminals who breached Australian Medibank's systems have released another batch of data onto the dark web, claiming that the files contain all data harvested in the former heist that impacted 9.7 million customers in October 2022. Medibank has confirmed the data breach.
- Colombian healthcare provider Keralty, operating as an international network of 12 hospitals and 371 medical centers around the world, has suffered a RansomHouse ransomware attack that disrupted the websites and operations of the company and its subsidiaries.
- Reporters claim Russian forces are abusing security flaws in Telegram for surveilling Telegram chats of Ukrainians in occupied or previously-occupied territories.
- A new campaign is abusing a trending TikTok challenge, in which users film themselves naked while using TikTok's "Invisible Body" filter, which removes the body from the video and replaces it with a blurry background. Hackers are exploiting the trend and offering a fake filter for download that removes the masking effect. The software then downloads the WASP Stealer malware, capable of stealing users' passwords, Discord accounts, and potentially cryptocurrency wallets.
- GoTo and LastPass, affiliated companies who share Cloud-Storage Services, disclosed they are handling a security breach after threat actors gained access to the third-party service and to GoTo's development environment. The incident is assumed to be related to the former breach to LastPass from August 2022.
- Judicial courts and mayor officers across several Russian regions have been hit by a previously unseen data wiper named CryWiper. CryWiper masquerades as ransomware, yet even after the victim pays, the files remain unrecoverable.
- Researchers found that over 300,000 users across 71 countries were effected by an Android campaign meant to steal Facebook credentials. This is by using Schoolyard Bully Mobile Trojan, deployed in legitimate education-themed applications, which were available in the official Google Play Store.

  Check Point Harmony Mobile provides protection against this threat
- An exploit framework was found to have planted spyware on targeted devices exposed to already patched zero-day flaws in Google Chrome, Mozilla Firefox, and Windows (Microsoft Defender security app). The framework has been linked to a Spain-based spyware vendor named Variston IT.

VULNERABILITIES AND PATCHES

- Google has released an update of Chrome to address a single high-severity security flaw, a zero-day vulnerability tracked CVE-2022-4262, exploited in the wild and patched. This marked the Ninth Chrome zero-day patched this year.
- A critical, exploited in the wild, flaw impacting Oracle Fusion Middleware has been reported. The flaw is tracked as CVE-2021-35587 and impacts Oracle Access Manager (OAM) versions 11.1.2.3.0, 12.2.1.3/4.0.

  Check Point IPS provides protection against this threat *(Oracle Access Manager Authentication Bypass (CVE-2021-35587))*
- Three Android applications - PC Keyboard, Lazy Mouse and Telepad - apps that allow users to use mobile devices as remote keyboards for their computers, have been found to have critical flaws that could expose key presses and enable remote code execution. The count of installs from the Google Play store stands at over two million.
- NVIDIA released an update for its GPU display driver for Windows, to fix 29 security flaws that can be used for code execution and privilege escalation among others. The two most prominent vulnerabilities are tracked CVE-2022-34669 and CVE-2022-34671.

THREAT INTELLIGENCE REPORTS

- Researchers have published a blog on cyber espionage activity, tracked UNC4191 and suspected to be originated from China, which leverages USB devices as an initial infection vector and targeting the Philippines.
- A new joint advisory from CISA and the FBI reveals that the Cuba ransomware gang managed to extort more than $60 million in ransom payments from victims between December 2021 and August 2022, after breaching more than 100 victims worldwide.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Wins.Cuba.*)*
- Researches encountered a new phishing campaign that uses Discord content delivery network (CDN) to host malicious files and get users to download NjRAT malware.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Trojan.Win.Njrat.*)*