Check Point Research
# WEEKLY INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- Check Point Research has published a report on APT-C-36, also known as Blind Eagle - a financially motivated threat group attacking citizens of various countries in South America since at least 2018. CPR has spotted a new campaign by this APT group targeting organizations and government entities in Ecuador with a new and advanced toolset.

  *Check Point Threat Emulation provides protection against this threat* *(Packer.Win.VBNetCrypter.H; Dropper.Win.DotNetDropper.*; Injector.Win.RunPE.A; RAT.Win.AsyncRAT; Trojan.Win.Msilzilla.glsf.C; Ransomware.Win.RMShadowCopy.A)*

- Cloud services provider Rackspace confirmed that a month ago it experienced a security incident in which the Play ransomware group exploited a previously unknown vulnerability (CVE-2022-41080) to gain access to Rackspace's Hosted Exchange email environment.

  *Check Point IPS provides protection against this threat* *(Microsoft Exchange Server Server-Side Request Forgery (CVE-2022-41080))*

- The Saint Gheorghe Recovery Hospital in Romania was hit by a ransomware attack in December, during which its medical records were locked and a ransom of 3 Bitcoins was demanded for their decryption. No ransomware group has yet claimed responsibility for the hack.

- A database containing over 14 million usernames and passwords was found on a dark web forum, and within this database were more than 100,000 logins for portals belonging to Australian government agencies.

- The Vice Society ransomware group has been conducting a series of widespread attacks targeting schools in both the United Kingdom and the United States. In response to these developments, the Federal Bureau of Investigation (FBI) has issued an official alert regarding the group's activities.

  *Check Point Threat Emulation provides protection against this threat* *(Trojan.Wins.ViceSociety.*)*

- The financially-motivated hacking group, Bluebottle, is suspected of being involved in a recent campaign that targeted banks in French-speaking countries using singed Windows drivers. Reports indicate that the threat actor was able to steal more than $11 million from various banks.

- Maternal & Family Health Services (MFHS) in Pennsylvania was hit by a ransomware attack in April 2022. Personal information, including Social Security Numbers, names, addresses and financial information, was accessed by the threat actors. No ransomware group has claimed responsibility.

# VULNERABILITIES AND PATCHES

- Zoho is warning its customers of a critical SQL Injection vulnerability in Password Manager Pro, PAM360 and Access Manager Plus. This vulnerability (tracked as CVE-2022-47523) is affecting multiple ManageEngine products.
- Synology has released security updates to address a critical RCE vulnerability (CVE-2022-43931) impacting VPN Plus Server that could be exploited to take over affected systems.
- Qualcomm Technologies has released patches to address five vulnerabilities, tracked from CVE-2022-40516 through CVE-2022-40520, in its chipsets. Some of the flaws could be exploited to cause information disclosure and memory corruption. Flaws also impact Lenovo ThinkPad X13s laptops, leading the Chinese PC maker to issue BIOS updates to plug the security holes.

# THREAT INTELLIGENCE REPORTS

- Check Point Research reports that threat actors in hacking forums have started making use of AI tools like ChatGPT, in order to create malware and attack tools such as info-stealers and encryptors.
- Check Point reports a 38% increase in global cyberattacks in 2022 compared to 2021. Global volume of cyberattacks reached an all-time high in Q4, and the top 3 most attacked industries in 2022 were Education/Research, Government and Healthcare. USA saw a 57% increase in overall cyberattacks in 2022, UK saw a 77% increase and Singapore saw a 26% increase.
- Security experts have developed a Decryptor for the MegaCortex ransomware family, which will allow individuals affected by this gang to recover their data at no cost.

  *Check Point Threat Emulation provides protection against this threat* (Ransomware.Win.MegaCortex.A)

- Security researchers have identified that the Russian nation-state group Turla is distributing ANDROMEDA malware from compromised USB devices, possibly to target Ukrainian entities

  *Check Point Threat Emulation provides protection against this threat* (APT.Win.Turla.*)

- Security researchers have identified a new info-stealer dubbed 'LummaC2' that targets crypto wallets, extensions, and two-factor authentication (2FA) through both Chrome and Mozilla-based browsers.
- A new variant of the Dridex banking malware has been observed targeting MacOS platforms with documents embedded with malicious auto-open macros, meaning the macro would run immediately when the user opens a Word document.