# TOP ATTACKS AND BREACHES

- One of the United States' largest dental insurers, MCNA, has notified regulators that information of 8.9 million of the company's customers has been leaked as a result of a ransomware attack. Notorious ransomware gang LockBit has claimed the attack, and has allegedly posted the data in its shame blog.

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

- Greece's Ministry of Education has been the victim of a sustained distributed denial of service attack, described as the most extensive in the country's history. The attack, which reportedly originated from hosts in more than 100 countries, has disrupted a platform used for hosting high school exams, and delayed year end exams for several hours.

- The Russian FSB has accused the American NSA of a years-long spyware campaign on iPhone devices, targeting prominent Russian individuals worldwide. The FSB has also claimed that Apple had collaborated with the NSA in the development of the spyware tool, which Apple denies. Earlier this week, Russian cybersecurity firm Kaspersky has discovered that iPhone spyware infection affected some of the company's employees' devices.

- Jimbos Protocol, a cryptocurrency project, has suffered a flash loan attack causing losses of Ethereum tokens worth more than $7.5M. The attackers have exploited a lack of slippage-control mechanism in the platform, allowing them to loan tokens and manipulate their value before returning them. The attack has also harmed the platform's reputation, causing a large drop in the valuation of its tokens.

- The superintendent of Middlesex County Public Schools in Virginia has confirmed that the organization has fallen victim to a ransomware attack. According to the statement, the disruption in school activity had been minimal. However, the Akira ransomware gang who has taken responsibility for the attack claims to have exfiltrated over 500GB of sensitive data in the breach.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat*
  *(Ransomware.Win.Akira.A; Trojan.Win.Krap.gl.D)*

- Iranian hacktivists affiliated with Iran's opposition group MEK have gained access to Iran's presidential network. The hacktivists defaced websites by replacing the president with opposition figures, and leaked confidential information taken in the attack, including alleged diplomatic correspondence.

# VULNERABILITIES AND PATCHES

- A zero-day SQL injection vulnerability (CVE-2023-34362) affecting MOVEit Transfer, a managed file transfer platform, has been widely exploited in the wild for weeks. The vulnerability could lead to information disclosure, and experts worry that a large number of organizations have had their data stolen. Experts are concerned about a potential large-scale extortion campaign, similar to the Fortra GoAnywhere zero-day campaign by Cl0P ransomware group earlier this year.

  *Check Point IPS blade provides protection against this threat* *(MOVEit Transfer SQL Injection (CVE-2023-34362))*

- Hidden firmware code that automatically downloads updates from the internet has been discovered in hundreds of Gigabyte Motherboard models, which are installed in millions of computers. While the code is designed for legitimate purposes, its implementation is considered insecure, and experts warn that threat actors could potentially hijack the process to stealthily install malicious content. Gigabyte claims to have released firmware updates that include stronger safeguards against this threat.

- Website platform WordPress has pushed an update to Jetpack, a popular plugin used in WordPress, to more than 5 million websites. The vulnerability, which is considered critical, could allow an attacker to abuse Jetpack's API to manipulate WordPress files.

# THREAT INTELLIGENCE REPORTS

- Check Point Research has published an analysis of a backdoor tool used by the Chinese APT group Camaro Dragon. The backdoor tool, dubbed TinyNote, is written in Go and includes a feature bypassing Indonesian antivirus software SmadAV, which is popular in Southeast Asian countries. The APT group's victims likely include embassies in Southeast Asian countries.

  *Check Point Threat Emulation provides protection against this threat* *(APT.Wins.MustangPanda.ta.*)*

- Researchers have analyzed a new botnet targeting Spanish speaking users in the Central and South America. The botnet, dubbed Hoarbot, takes control of victims' exchange accounts to propagate the botnet via spam email, and also has credential theft capabilities that are used to gain access to victims' financial accounts. The researchers estimate that the threat actor behind the botnet is based in Brazil.

- A potentially malicious spyware module embedded in Android apps has been discovered. The module sends detailed technical information about the device upon its first initialization, and can access and copy files. Applications containing this module have a total of more than 420 million installations.

  *Check Point Harmony Mobile provides protection against this threat.*

- United States and Korean security agencies have released a joint advisory warning against North Korea's social engineering methods used to gain initial access to think tanks, media and academia organizations.