# TOP ATTACKS AND BREACHES

- Check Point researchers have detected a phishing campaign exploiting popular file-sharing program Dropbox. The threat actors use legitimate Dropbox pages to send official email messages to the victims, which will then redirect the recipients to credential stealing pages.

- Japanese entertainment giant Sony, as well as major Japanese telecom provider NTT Docomo have been the victims of ransomware attacks during the past week. The 'ransomed.vc' threat group has assumed responsibility for both attacks and has demanded millions of dollars in ransom from the two companies. The group threatens to sell or leak data exfiltrated in the breaches if its demands are not met.

- American conglomerate Johnson Controls has been hit by ransomware. Ransomware group Dark Angels is demanding $51M from the company in ransom and claims to have exfiltrated more than 25TB of data during the attack. The American Department of Homeland Security is reportedly investigating whether information regarding its facilities had been leaked in the attack, as Johnson Controls is a contractor for the department's buildings.

- Hong Kong cryptocurrency exchange firm Mixin has disclosed that $200M have been stolen in a breach of its network. According to the firm's statement, the threat actors have gained access by attacking a database belonging to the company's cloud provider in order to conduct the theft.

- Russian flight booking vendor Leonardo's services have been disrupted by a distributed-denial-of-service attack. As a result, multiple Russian airline companies, including the state-owned Aeroflot, were unable to process booking requests. Ukrainian hacktivist collective 'IT Army of Ukraine' has claimed responsibility for the attack.

- Kuwait's Ministry of Finance has acknowledged that its network had been breached in a cyber-attack. The ministry claims that financial data of its employees was not impacted in the attack. Ransomware group Rhysida has assumed responsibility and demands $400,000 in ransom.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat*
  *(Ransomware_Win_Rhysida; Ransomware.Wins.Rhysida; Ransomware.win.honey)*

- A campaign targeting Azerbaijani entities has been discovered. The threat actors have been using email messages containing supposed information regarding the Azerbaijan-Armenia conflict in Nagorno-Karabakh, which would deliver spyware if opened.

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

# VULNERABILITIES AND PATCHES

- Check Point researchers have discovered multiple critical vulnerabilities affecting the WEB3 social media platform Friend.tech. The set of vulnerabilities can allow attackers to access and modify database values belonging to the company, as well as gain access to paid features.

- Google and Mozilla have published advisories addressing a critical heap buffer overflow vulnerability that affects the companies' respective internet browser products. The vulnerability, which was assigned CVE-2023-5217, involves the libvpx library's VP8 video encoding feature, and may affect any product using this library. Google has noted that it is aware of targeted exploitation of the vulnerability in the wild by commercial spyware vendors.

- Six vulnerabilities (CVE-2023-42114-9) have been reported in the Exim mail transfer agent, of which four are considered critical and can allow remote code execution. Exim claims to have developed fixes for three of the vulnerabilities, but two remote code execution flaws remain unpatched. Researchers estimate that at least 250,000 Exim email servers are vulnerable worldwide.

- Software provider Progress has disclosed two critical vulnerabilities affecting its WS_FTP file transfer product. The vulnerabilities CVE-2023-40044 and CVE-2023-42657 allow remote code execution on the underlying operating system of WS_FTP servers. Progress also develops the similar MOVEit managed file transfer product, which was breached in a widespread attack by Cl0p ransomware gang earlier this year.

# THREAT INTELLIGENCE REPORTS

- A campaign targeting employees of a Spanish aerospace company has been discovered. The North Korean APT group Lazarus impersonated a Meta recruiter to establish rapport with the victims and delivered 'coding challenges' that contained malicious backdoors as part of the 'recruitment' process.

- American and Japanese security agencies have published a joint report detailing the activity of Chinese threat actor group BlackTech. The group has attacking entities in the United States and in Japan by targeting Cisco routers to gain initial access and maintain persistence in the target environments.

- Chinese APT group Budworm has been observed targeting an Asian country's government and a telecom company in the Middle East. The group has used DLL sideloading with the legitimate INISafeWebSSO application to deploy its SysUpdate malware, which serves as a multipurpose backdoor.

- Researchers detail a campaign by unknown threat actors who have managed to compromise hundreds of GitHub repositories. The threat actors gained access using owners' personal access tokens, and then committed malicious infostealing code disguised as Dependabot, GitHub's automatic security feature.

- Researchers have analyzed ZenRAT, a RAT with built-in information stealer tools target Windows platforms. The malware is distributed by malicious installers of the BitWarden password manager.