TOP ATTACKS AND BREACHES

- Cl0p ransomware gang claimed responsibility for a major exploitation of a managed file transfer tool - MOVEit. The gang leveraged zero-day SQL injection vulnerability (CVE-2023-34362) that potentially exposed the data of hundreds of companies. One of the victims was the payroll services provider Zellis, what caused to exposure of employees' personal data at eight of Zellis's clients in the UK and Ireland, including the BBC, Boots and British Airways. Earlier this year, Cl0p leveraged vulnerability in another managed file transfer tool, Fortra GoAnywhere, for large scale exploitation campaign.

  Check Point IPS blade, Harmony Endpoint and Threat Emulation provide protection against this threat *(MOVEit Transfer SQL Injection (CVE-2023-34362); Webshell.Win.Moveit, Ransomware.Win.Clop, Ransomware_Linux_Clop; Exploit.Wins.MOVEit)*

- Japanese pharmaceutical giant Eisai disclosed a ransomware attack that encrypted some of the company's servers and took systems offline both in and outside of Japan. According to the company, the possibility of data leakage is currently under investigation.

- The Spanish bank Globalcaja has been a victim of a ransomware attack conducted by Play ransomware gang. The threat actors claim to have access to an undisclosed amount of private and personal confidential data including clients' and employees' documents, passports, contracts and more.

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

- The Estonia-based cryptocurrency wallet service Atomic Wallet has confirmed a cyber-attack that compromised customers' wallets, resulting in the loss of more than 35M dollars. Researchers suggest with high confidence that the North Korean state-backed Lazarus Group is responsible for the attack.

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

- Pink Drainer hacking group has been linked to phishing attacks that compromised nearly 2,000 Discord and Twitter accounts from which they stole more than 3M dollars. Among the victims are Evomos, Pika Protocol, OpenAI CTO, and Orbiter Finance.

- The pro-Ukrainian hacktivist group Cyber Anarchy Squad claimed responsibility for launching a distributed denial-of-service (DDoS) attack against the Russian telecom provider, Infotel JSC.

VULNERABILITIES AND PATCHES

- Google has released a security update for an actively exploited zero-day flaw in Chrome web browser. The vulnerability (CVE-2023-3079), classified as highly severe, could lead to type confusion that can cause to the program misinterpreting the data type it is handling. An attacker could exploit this flaw to gain unauthorized system access to conduct information disclosure.
- Google has delivered security patches for 56 Android vulnerabilities. The most severe flaw is a critical security vulnerability in the System component that could lead to remote code execution over Bluetooth, if HFP support is enabled, with no additional execution privileges needed.
- Cisco has addressed a high-severity vulnerability (CVE-2023-20178) discovered in their Cisco Secure Client software (previously known as AnyConnect Secure Mobility Client). An attacker could exploit this vulnerability by abusing a specific function of the Windows installer process.

THREAT INTELLIGENCE REPORTS

- Check Point Research has identified an ongoing operation against targets in North Africa involving a previously undisclosed multi-stage backdoor called Stealth Soldier. The backdoor primarily operates surveillance functions such as file exfiltration, screen and microphone recording, keystroke logging and stealing browser information.

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

- Check Point Research has released May 2023's threat index, highlighting a new version of shellcode-based downloader GuLoader, which was the fourth most prevalent malware. With fully encrypted payloads and anti-analysis techniques, the latest form can be stored undetected in well-known public cloud services, including Google Drive. Meanwhile, Qbot and Anubis are taking first place on their respective lists, and Education/Research remained the most exploited industry.
- Check Point Research warns about online phishing scams related to summer vacations and provides examples of vacation-related scams and tips on how to remain vigilant during the hot season.
- A new ransomware-as-a-service (RaaS) provider called Cyclops group has been observed on dark web forums, with the capability of infecting Windows, Linux, and macOS platforms. In addition to offering ransomware services, Cyclops also supplies a separate binary for data exfiltration purposes.

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

- Researchers have discovered a new variant of Android Spyware dubbed HelloTeacher, that disguises itself as a popular messaging application to target banking users in Vietnam. The spyware is armed with data exfiltration capabilities including capturing pictures and recording infected device's screen.