summary

Summary of Findings

The malware sample analyzed using **VirusTotal** was identified as a **high-risk malicious file**. The SHA-256 hash `4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a` was detected as malicious by **61 out of 70 security vendors**, confirming its harmful nature.

The file is a **Win32 DLL executable**, commonly used by attackers for stealthy execution. Behavior analysis revealed that the malware exhibits characteristics of **Trojan, Ransomware, Stealer, and Defense-Evasion malware**. It performs multiple malicious actions such as **dropping additional payload files**, **modifying system behavior for persistence**, **injecting into processes**, and **encrypting data for impact**.

Network analysis showed that the malware communicates with **external domains and IP addresses**, indicating **Command-and-Control (C2)** activity. The malware also uses **anti-analysis and sandbox evasion techniques**, including long execution delays, environment detection, and code obfuscation.

Overall, the analysis confirms that the malware follows a **complete malware lifecycle**, from delivery and execution to persistence, payload execution, and impact. This practical helped in understanding **malware behavior indicators, detection reports, spreading techniques, and prevention methods**, thereby improving basic malware awareness and detection skills.