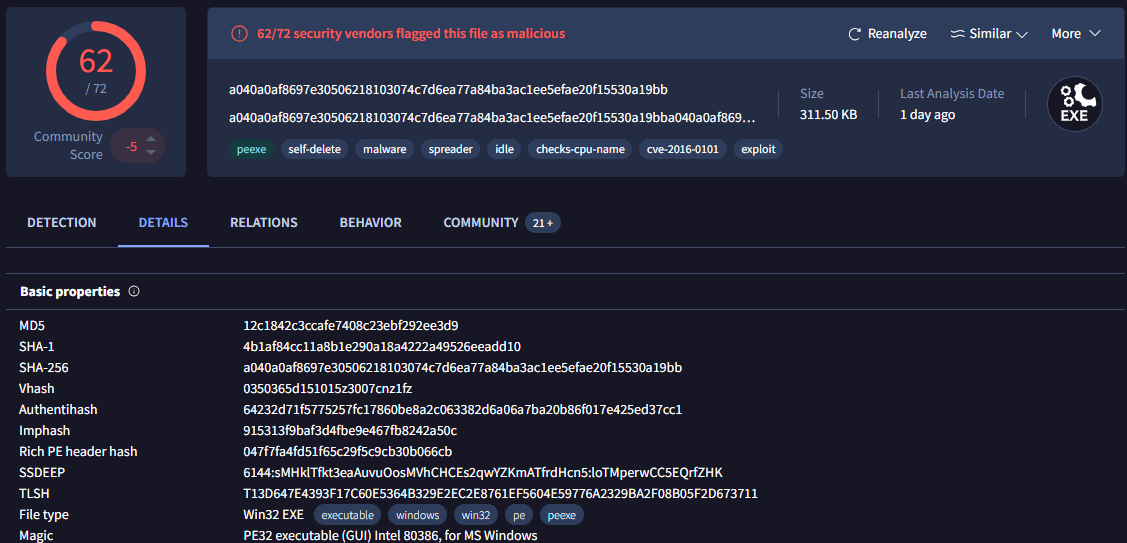
### ****Suspicious File Hash Analysis****

**Objective:**  
Analyze the hash of a file using public tools to identify its nature and behavior, as part of a standard threat detection and analysis procedure.

**MD5 Hash:** 12c1842c3ccafe7408c23ebf292ee3d9

**Procedure:** Verify the hash using [virustotal.com](https://www.virustotal.com" \t "C:\\Users\\diego\\AppData\\Local\\Temp\\_new)



· **Determining the creation time of the malware can provide insights into its origin. What was the time of malware creation?**  
**Answer:** 2022-09-28 17:40:46 UTC

· **Identifying the command and control (C2) server that the malware communicates with can help trace back to the attacker. Which C2 server does the malware in the PPT file communicate with?**  
**Answer:** 171.22.28.221  
To validate whether the IP is malicious, you can use the following website: [https://abuseipdb.com/](https://abuseipdb.com/" \t "C:\\Users\\diego\\AppData\\Local\\Temp\\_new)  
**IP location (AbuseIPDB):** United States of America

· **Identifying the initial actions of the malware post-infection can provide insights into its primary objectives. What is the first library that the malware requests post-infection?**  
**Answer:** sqlite3.dll

· **By examining the MITRE ATT&CK techniques displayed in the Any.run sandbox report, identify the main MITRE technique (not sub-techniques) the malware uses to steal the user’s password.**  
**Answer:** T1555