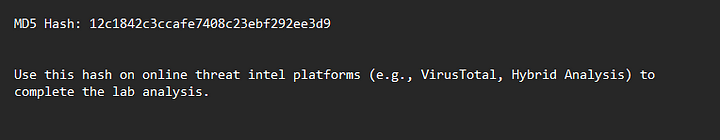
### **Oski Lab — CyberDefenders**

**Scenario:** The accountant at the company received an email titled “Urgent New Order” from a client late in the afternoon. When he attempted to access the attached invoice, he discovered it contained false order information. Subsequently, the SIEM solution generated an alert regarding downloading a potentially malicious file. Upon initial investigation, it was found that the PPT file might be responsible for this download. Could you please conduct a detailed examination of this file?

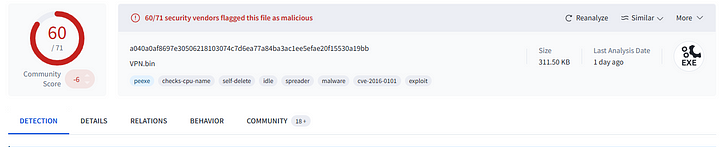


**Hash:** 12c1842c3ccafe7408c23ebf292ee3d9

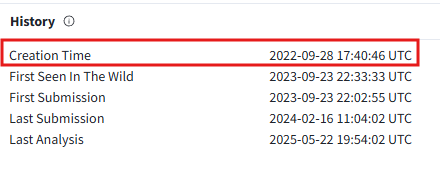
#### **TASKS**

1. **Determining the creation time of the malware can provide insights into its origin. What was the time of malware creation?**

Submit the hash to VirusTotal to find more information about the file.



In VirusTotal, head to “Details” tab and check the “History” section.



**Answer:** 2022–09–28 17:40

**2. 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?**

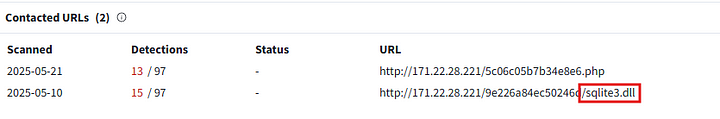
Head to the “Relations” tab and check for the URL’s contacted by the malware under the “Contacted URL’s” section.



**Answer:** http://171.22.28.221/5c06c05b7b34e8e6.php

**3. 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?**

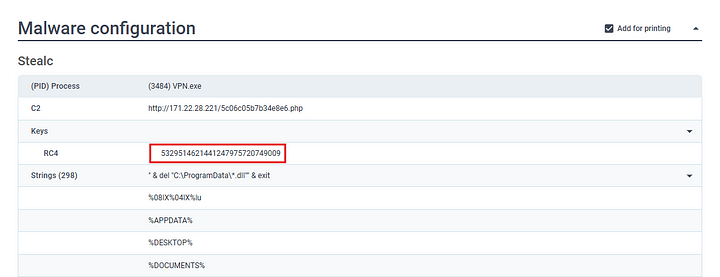
We can see the file in the above screenshot.



**Answer:** sqlite3.dll

**4. Upon examining the malware, it appears to utilize the RC4 key for decrypting a base64 string. What specific RC4 key does this malware use?**

For more information about the malware, we need to use the hybrid analysis platforms. We can search Any. Run with the hash of the file.

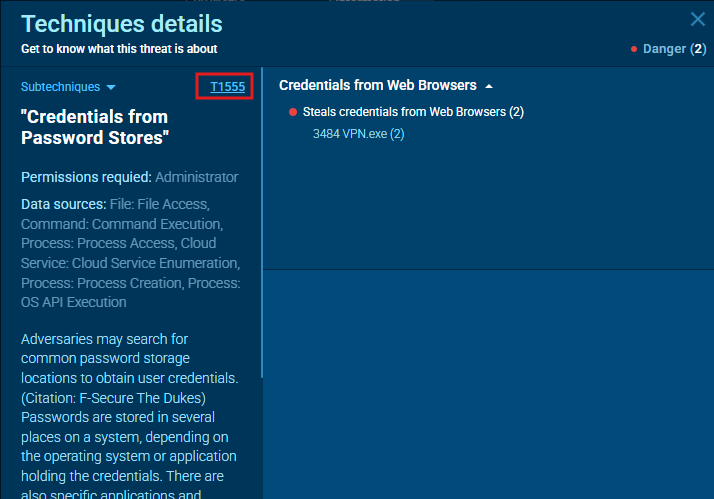


As we can see, in the text report under the “Malware Configuration” section the key is mentioned.

**Answer:** 5329514621441247975720749009

**5. Identifying an adversary’s techniques can aid in understanding their methods and devising countermeasures. Which MITRE ATT&CK technique are they employing to steal a user’s password?**

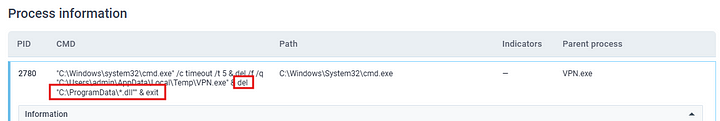
In Any Run full report, head to the ATT&CK section.



**Answer:** T1555

**6. Malware may delete files left behind by the actions of its intrusion activity. Which directory does the malware target for deletion?**

In the text report, we can find the commands executed by the malware.



**Answer:** C:\ProgramData

**7. Understanding the malware’s behavior post-data exfiltration can give insights into its evasion techniques. After successfully exfiltrating the user’s data, how many seconds does it take for the malware to self-delete?**

In the above command, we can see that the malware set a timeout of 5.



**Answer:** 5

This is the end of this investigation.