Challenge: Oski Lab

Platform: CyberDefenders

Category: Threat Intel

Difficulty: Easy

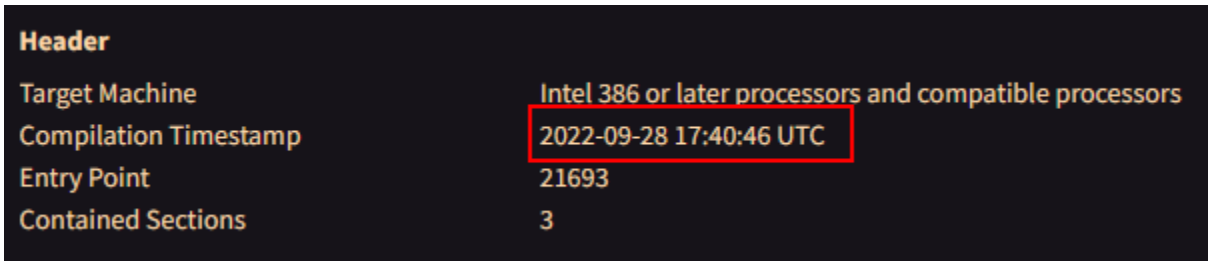
Tools Used: VirusTotal, ANY.RUN

Summary: This lab involves using VirusTotal and ANY.RUN reports to analyse a malicious PPT file. I personally found this threat intelligence challenge to be relatively boring, however, those new to VirusTotal and ANY.RUN reports may find use in doing it.

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?

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

VirusTotal is a feature rich threat intelligence platform. If you search for the given hash and navigate to “Details” tab, you can see the compilation timestamp:



Answer: 2022-09-28 17:40

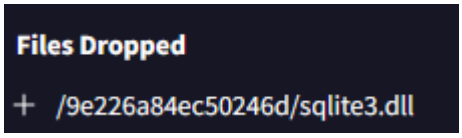
Identifying the command and control (C2) server that the malware communicates with can help trace back to the attacker. Which C2 server does the malware in the PPT file communicate with?

The “Behaviour” tab on VirusTotal details key information about the behaviour of the file, including network communications, registry activity, etc. Under the “HTTP Requests” section, we can see it makes a series of GET and POST requests to one domain:

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

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?

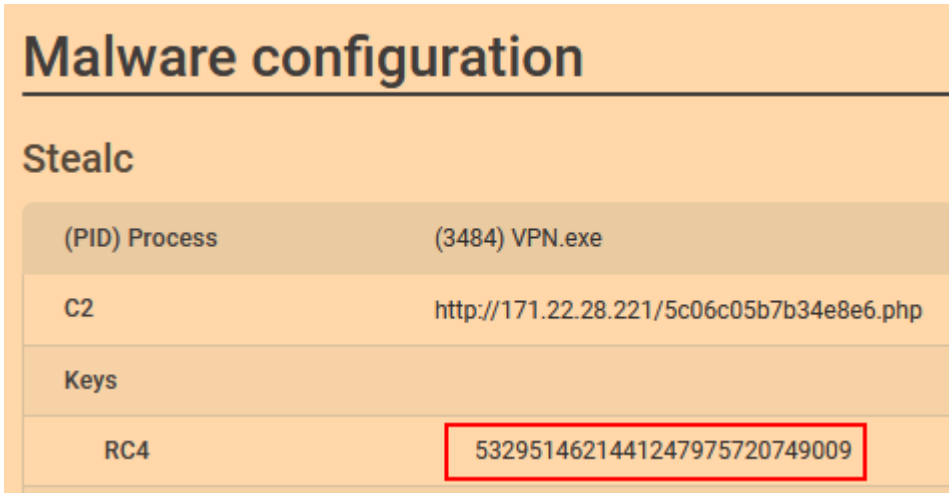
Under the "Files Dropped" section, we can see that this malware dropped a DLL file called sqlite3.dll:



Answer: sqlite3.dll

By examining the provided Any.run report, what RC4 key is used by the malware to decrypt its base64-encoded string?

Under the "Malware configuration" section of the Any.run report, you can find the RC4 key used to decrypt its bae64-encoded string:

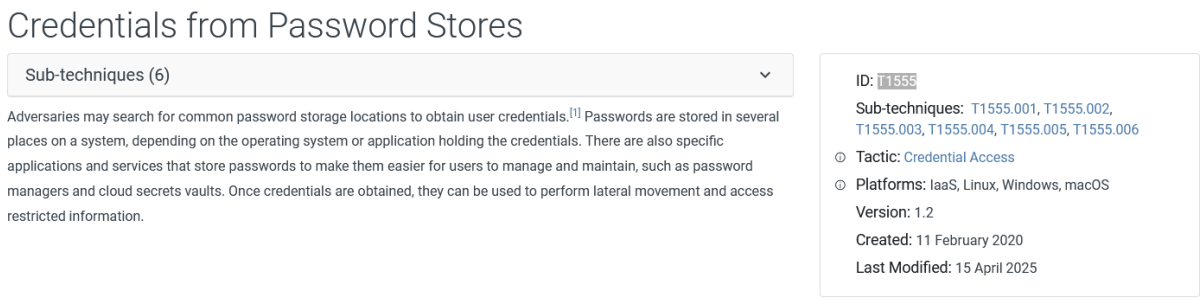


Answer: 532951462144124797572074900 9

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.

If you take a look at the "Behaviour activities" section, we can see that the malware steals credentials from web browsers:

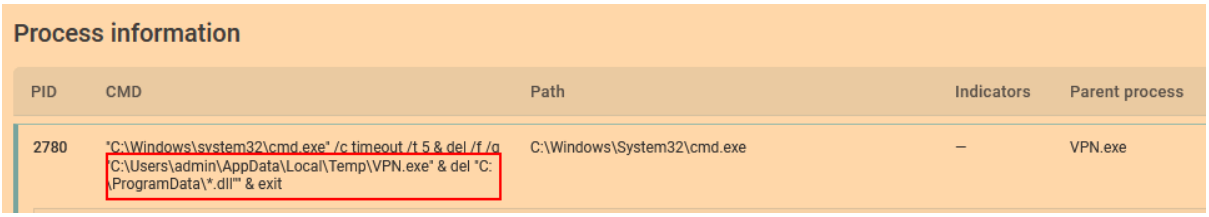
If you search this technique and append MITRE ATT&CK, you will come across T1555:



Answer: T1555

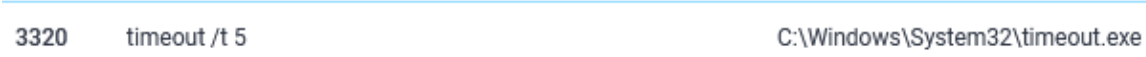
By examining the child processes displayed in the Any.run sandbox report, which directory does the malware target for the deletion of all DLL files?

If you look under the "Process information" section, you can see an executed command that contains a delete statement:



Answer: C:\ProgramData\

Understanding the malware's behavior post-data exfiltration can give insights into its evasion techniques. By analyzing the child processes, after successfully exfiltrating the user's data, how many seconds does it take for the malware to self-delete?



Answer: 5