בס"ד

Using "Strings and Hashes" For Malware Detection

By: Tamir Maidani

In this task I will examine an executable file to check if he a safe executable file or does it only a disguise for a malicious software.

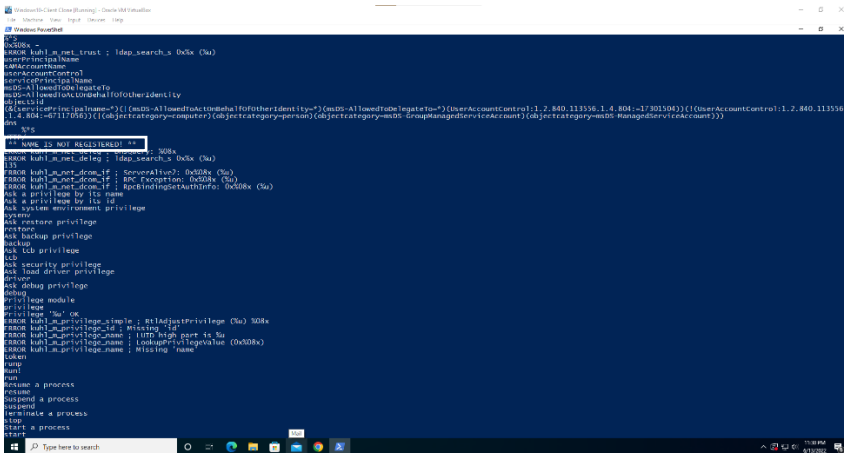
I will be using 2 tools in my arsenal in order to examine the "free.exe" file:

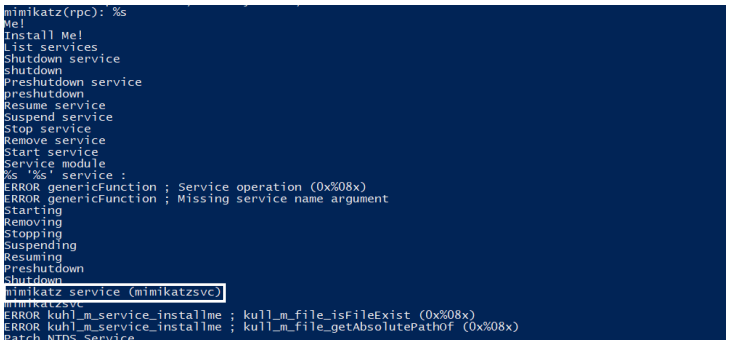
1.strings.exe – to extract and see any readable information from the file.

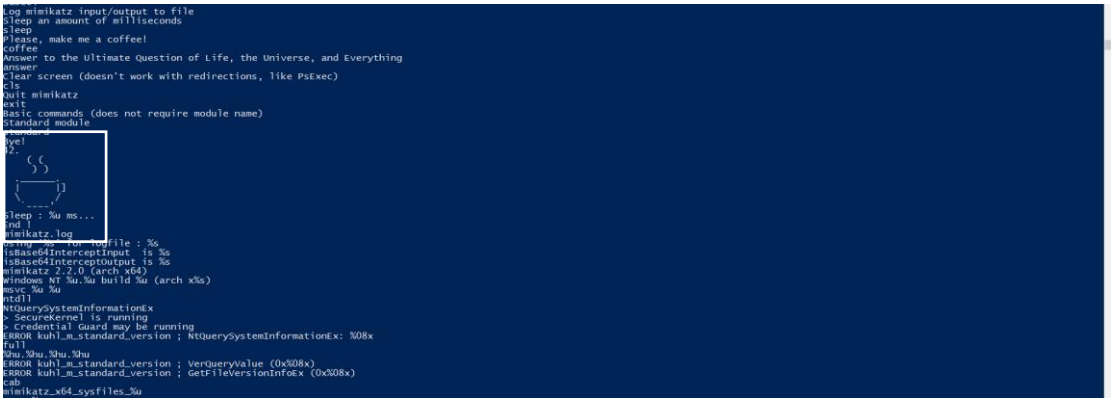
2.certutile.exe – to find the hash of the file and compare it to database that check for suspicious/malicious hashes that exists in the database, and maybe by doing so to find true information on the file.

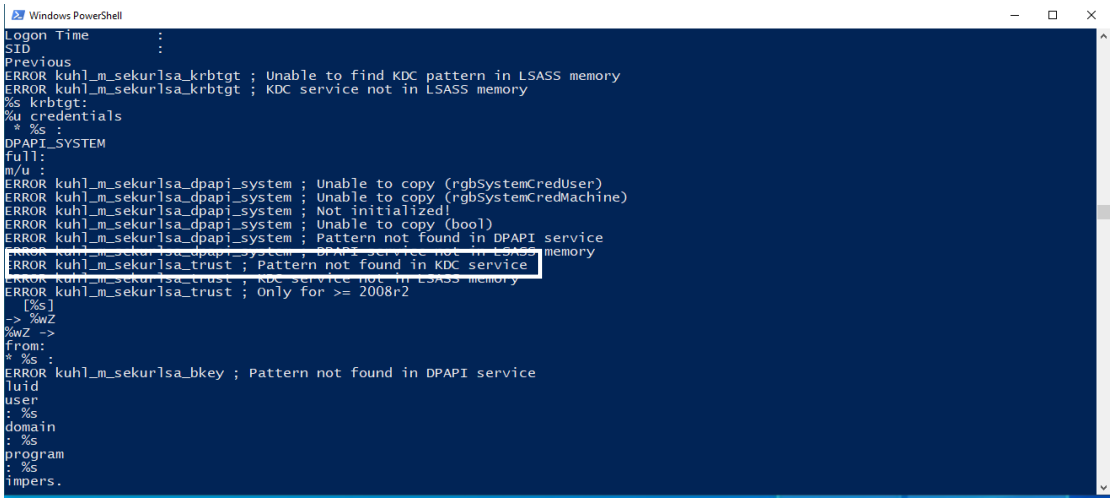
<u>The results:</u>

Checking with strings:









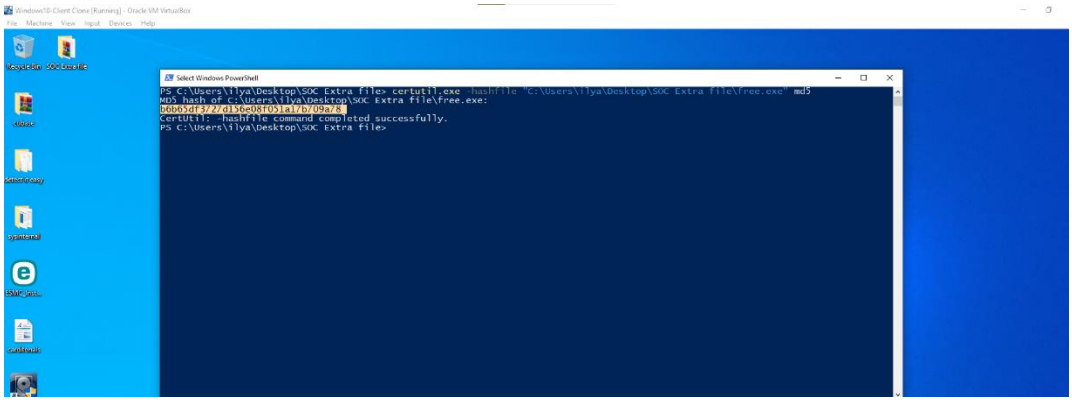
By that results themselves we can see that the malware "mimikatz" is mentioned in the file

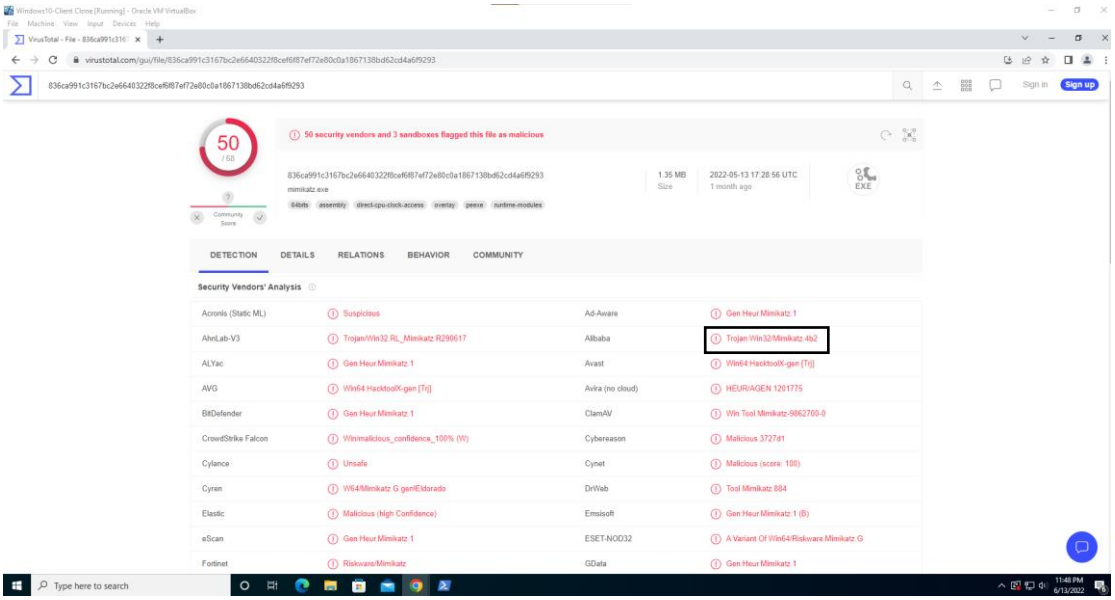
And its connection for creating a service on the system.

Plus we can see a suspicious error that say "pattern not found in kdc service" which should put us with a "warning sign".

Checking with certutile:

Now we will find the hash and put it into "virus-total" web for compering with his hashing database.





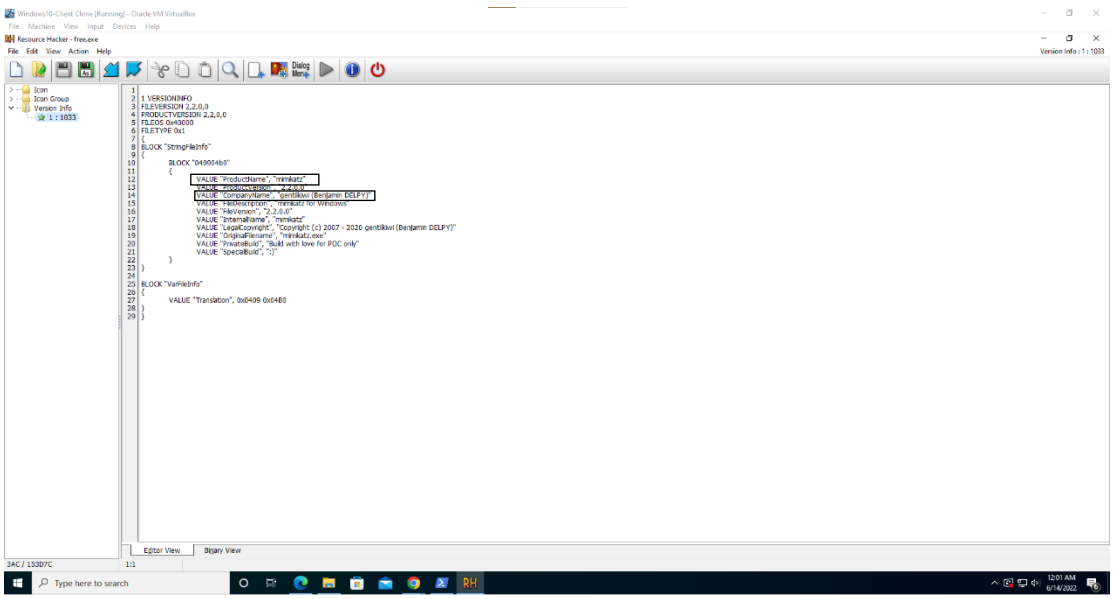
By now we can verify that indeed this file is a malicious Trojan that is known by the name "mimikatz".

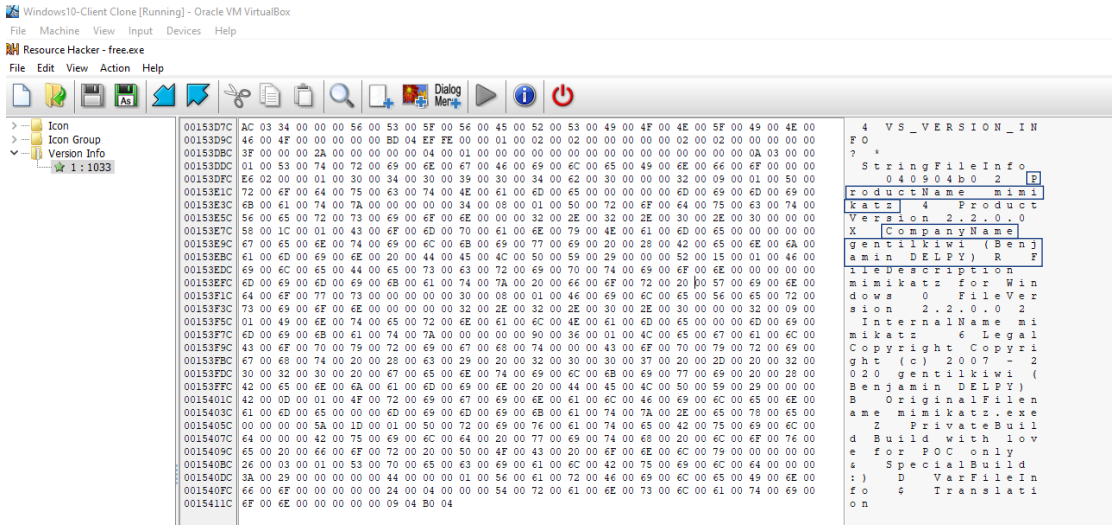
בס"ד

Using "Resource Hacker" For Malware Detection

In this task I will examine an executable file to investigate the content of it by the "Resource Hacker tool".

<u>The results:</u>





By the results above we can see the name of the real malicious software and who is it creator.