

## 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.certutil.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.

The results:

### Checking with strings:

[illegible]

```

Log mimikatz input/output to file
Sleep an amount of milliseconds
Sleep
Please, make me a coffee!
Coffee
Answer to the Ultimate Question of Life, the Universe, and Everything
Clear screen (doesn't work with redirections, like PsExec)
Exit
Quit mimikatz
Exit
Basic commands (does not require module name)
Standard module
Bye!
2.2.0
((
((
((
((
Sleep : %u ms...
end
mimikatz.log
mimikatz.log : %s
isBase64InterceptInput : %s
isBase64InterceptOutput : %s
mimikatz 2.2.0 (arch x64)
Windows NT %u.%u build %u (arch x64)
mimikatz_x64_sysfiles_%u
ntdll
NtQuerySystemInformationEx
SecureKernel is running
Credential Guard may be running
ERROR kuhl_m_standard_version ; NtQuerySystemInformationEx: %08x
Full
%u.%u.%u.%u
ERROR kuhl_m_standard_version ; VerQueryValue (0x%08x)
ERROR kuhl_m_standard_version ; GetFileVersionInfoEx (0x%08x)
cab
mimikatz_x64_sysfiles_%u

```

```

Windows PowerShell
Logon Time :
SID :
Previous :
ERROR kuhl_m_sekurlsa_krbtgt ; Unable to find KDC pattern in LSASS memory
ERROR kuhl_m_sekurlsa_krbtgt ; KDC service not in LSASS memory
%$ krbtgt:
%u credentials
* %$ :
DPAPI_SYSTEM
Full:
m/u :
ERROR kuhl_m_sekurlsa_dpapi_system ; Unable to copy (rgbSystemCredUser)
ERROR kuhl_m_sekurlsa_dpapi_system ; Unable to copy (rgbSystemCredMachine)
ERROR kuhl_m_sekurlsa_dpapi_system ; Not initialized!
ERROR kuhl_m_sekurlsa_dpapi_system ; Unable to copy (bool)
ERROR kuhl_m_sekurlsa_dpapi_system ; Pattern not found in DPAPI service
ERROR kuhl_m_sekurlsa_dpapi_system ; DPAPI service not in LSASS memory
ERROR kuhl_m_sekurlsa_trust ; Pattern not found in KDC service
ERROR kuhl_m_sekurlsa_trust ; KDC service not in LSASS memory
ERROR kuhl_m_sekurlsa_trust ; Only for >= 2008r2
[ %s ]
-> %wZ
%wZ ->
from:
* %$ :
ERROR kuhl_m_sekurlsa_bkey ; Pattern not found in DPAPI service
fluid
user : %s
domain : %s
program : %s
impers.

```

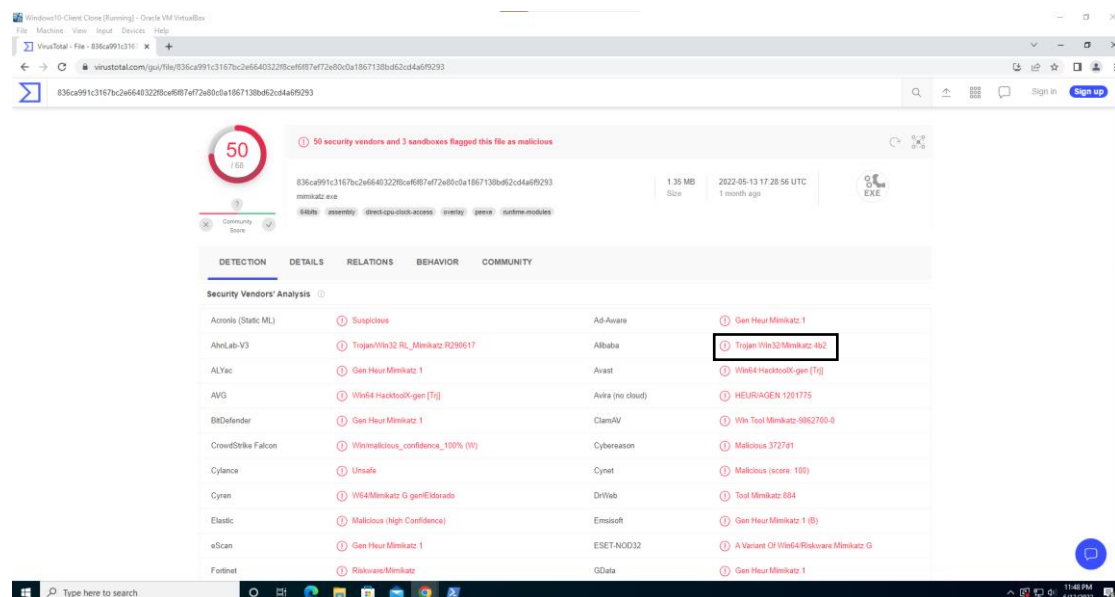
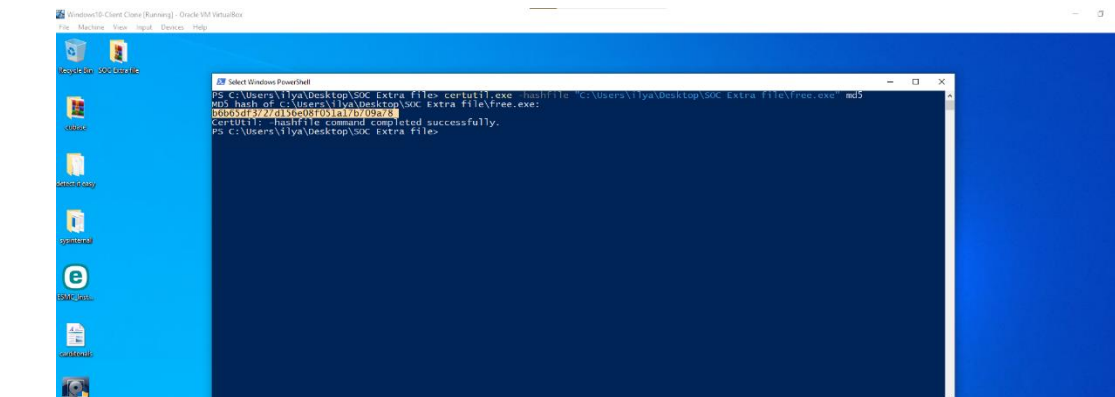
By that results themselves we can see that the malware "mimikatz" is mentioned in the file

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 certutil:

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

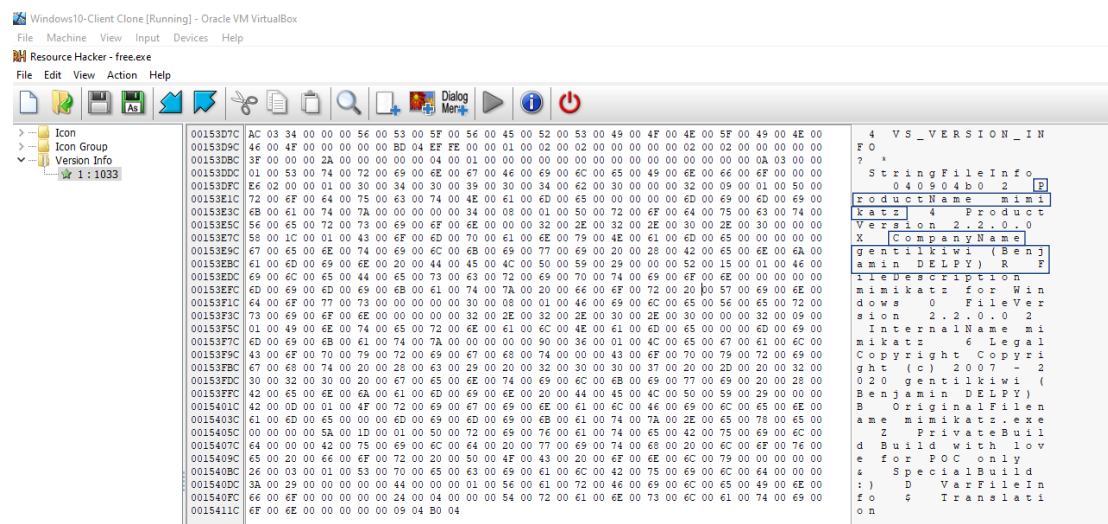
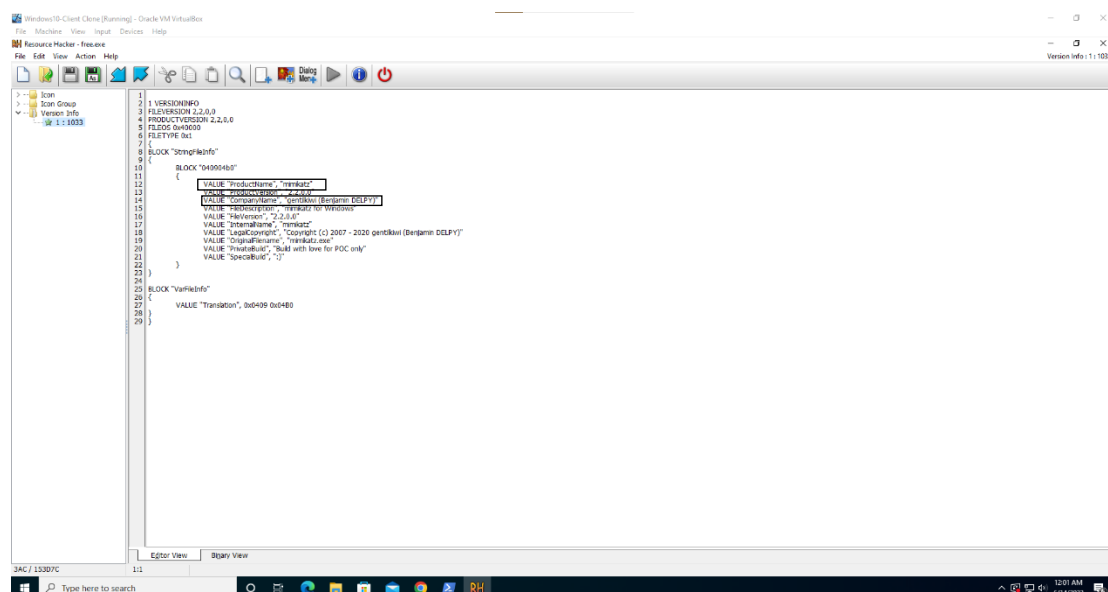


By now we can verify that indeed this file is a malicious Trojan that is known by the name "mimikatz".

## 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".

### The results:



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