

Obiettivo:

Con riferimento al file eseguibile contenuto nella cartella «**Esercizio_Pratico_U3_W2_L1**» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

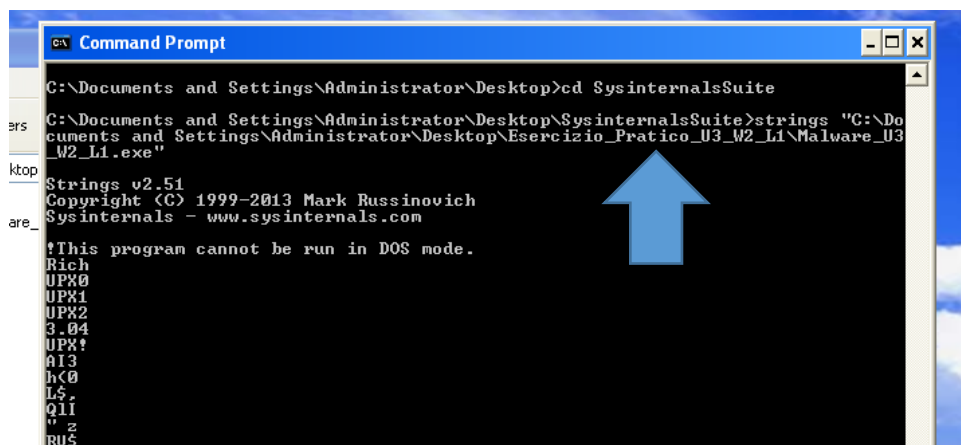
- Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse
- Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

Premessa: Andremo ad effettuare un'**analisi statica base**, quindi non avvieremo il Malware ma analizzeremo solamente il suo contenuto su un VM completamente isolata.

Prima fase

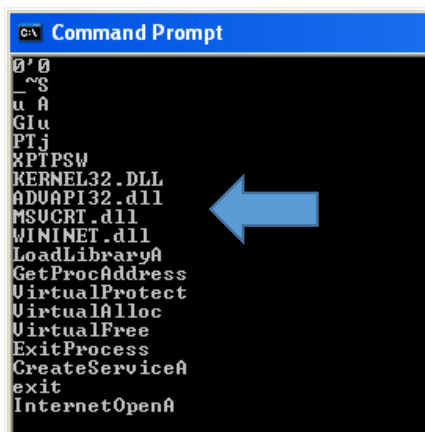
Nella prima fase della nostra esercitazione andiamo ad analizzare il Malware dato come esercitazione, cercando al suo interno eventuali librerie importate che richiamo funzioni dannose per il sistema attaccato.

Utilizziamo l'utility Strings, che abbiamo di default sulla nostra VM nella cartella Sysinternalsuits. Per utilizzare useremo il prompt dei comandi, apriamo la cartella da esso ed inseriamo il path del nostro file eseguibile da analizzare.



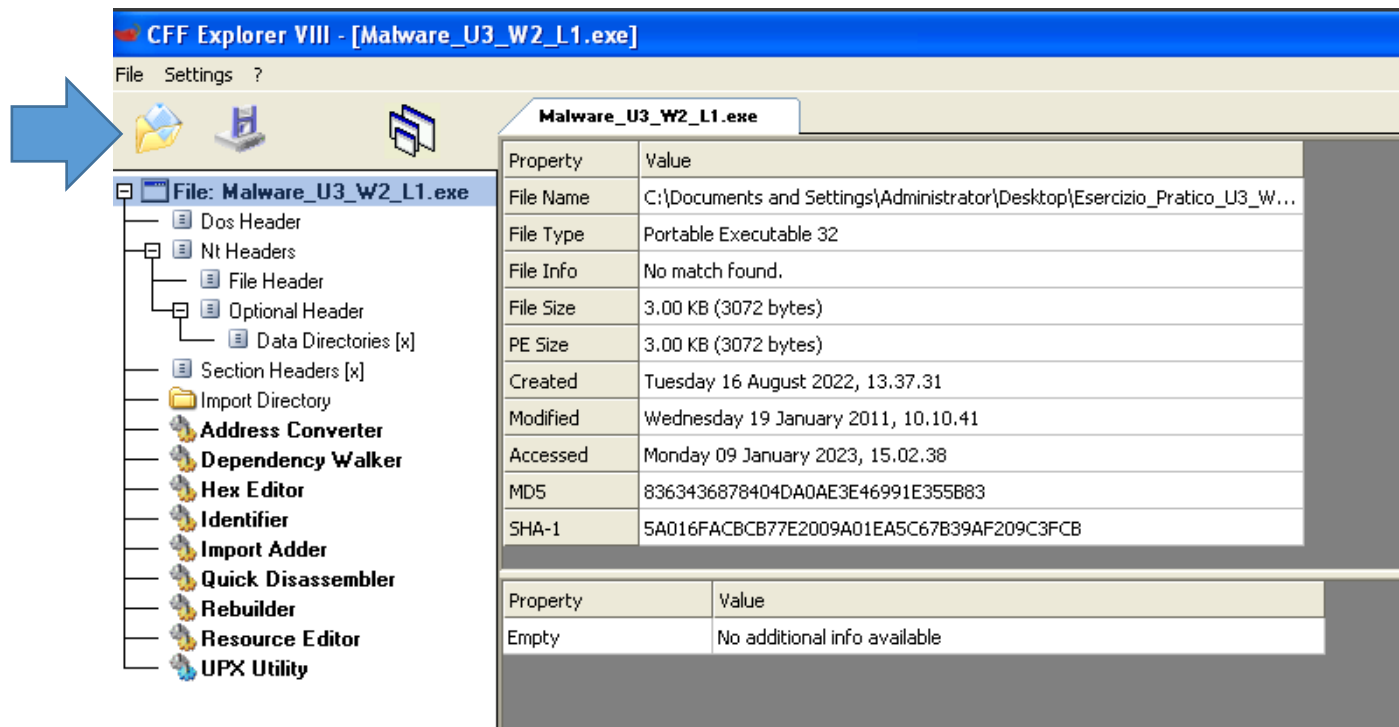
```
C:\Documents and Settings\Administrator\Desktop>cd SysinternalsSuite
C:\Documents and Settings\Administrator\Desktop\SysinternalsSuite>strings "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe"
Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com
!This program cannot be run in DOS mode.
Rich
UPX0
UPX1
UPX2
3.04
UPX!
A13
h<0
L$,
Q11
" z
RU$
```

Otteniamo come risposta tutte le stringhe contenute nel file, compresi le eventuali librerie importate dal nostro malware.



```
0'0
~$
u A
Glu
PTj
XPIPSW
KERNEL32.DLL
ADVAPI32.dll
MSUCRT.dll
WININET.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
CreateServiceA
exit
InternetOpenA
```

Andiamo anche ad utilizzare il tool **CFF explorer**, che ci conferma gli elementi trovati con strings. Essendo un tool, basterà caricare il nostro file eseguibile (attraverso la cartella in alto a sinistra) e ci tirerà fuori tutte le informazioni.



CFF Explorer VIII - [Malware_U3_W2_L1.exe]

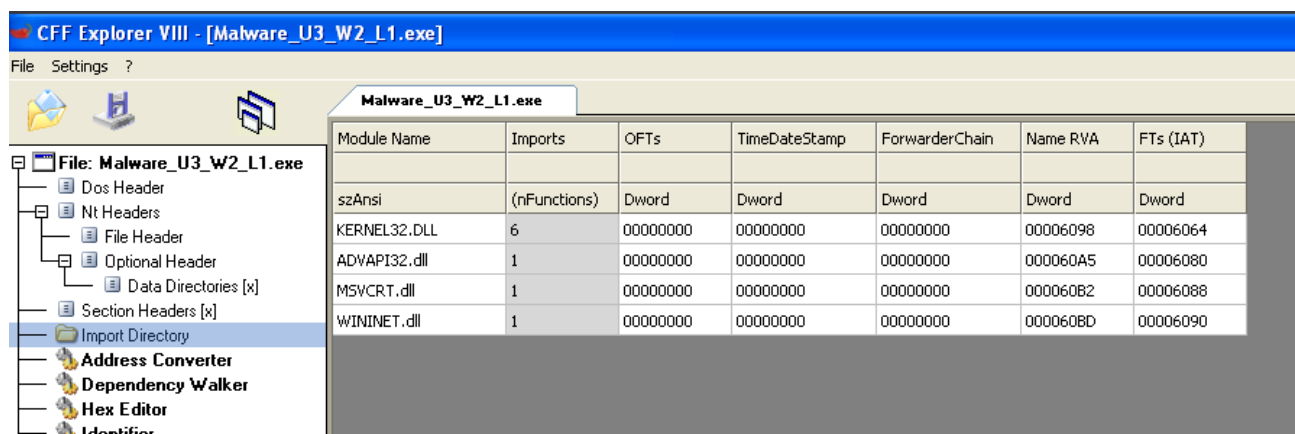
File Settings ?

Malware_U3_W2_L1.exe

Property	Value
File Name	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W...
File Type	Portable Executable 32
File Info	No match found.
File Size	3.00 KB (3072 bytes)
PE Size	3.00 KB (3072 bytes)
Created	Tuesday 16 August 2022, 13.37.31
Modified	Wednesday 19 January 2011, 10.10.41
Accessed	Monday 09 January 2023, 15.02.38
MD5	8363436878404DA0AE3E46991E355B83
SHA-1	5A016FACBCB77E2009A01EA5C67B39AF209C3FCB

Property Value

Empty No additional info available



CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

Abbiamo conferma delle librerie trovate in precedenza e possiamo notare che sono tra le più conosciute che hanno lo scopo di prendere il controllo del sistema operativo come KERNEL32.DLL e ADVAPI 32.DLL, oppure MSVCRT.DLL che permette la manipolazione di stringhe con codici in C e infine WININWT.DLL che permette di controllare protocolli http, ntp,ftp.

Possiamo anche notare che soprattutto la prima libreria importa 6 funzioni che analizzandole scopriamo sono **loadlibraryA** e **GetprocessAddress**. Cioè vengono importate in **runtime** quando il sistema è in esecuzione, quindi difficili da individuare. Entrambi le avevamo già trovate anche con Strings.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	000060C8	0000	LoadLibraryA
N/A	000060D6	0000	GetProcAddress
N/A	000060E6	0000	VirtualProtect
N/A	000060F6	0000	VirtualAlloc
N/A	00006104	0000	VirtualFree
N/A	00006112	0000	ExitProcess

Seconda Fase

Infine abbiamo utilizzato un altro tool analogo che ci permette le stesse funzioni CFF explorer, solo per mostrare un altro strumento alternativo, con il quale abbiamo individuato le sezioni che componevano il Malware. Il tool è Exeinfo.PE.

Carichiamo sempre il file di nostro interesse e abbiamo così individuato 3 sezioni.

Exeinfo PE - ver.0.0.6.2 by A.S.L - 1083+97 sign 2020.07.10

File : Malware_U3_W2_L1.exe

Entry Point : 00005410 oo < EP Section : UPX1

File Offset : 00000810 First Bytes : 60.BE.00.50.40

Linker Info : 6.00 SubSystem : Win Console

File Size : 00000C00h < N Overlay : NO 00000000

Image is 32bit executable RES/OVL : 0 / 0 % 2011

UPX 0.89 - 3.xx -> Markus & Laszlo ver. [3.04] <- from file. (sign like

Lamer Info - Help Hint - Unpack info

Big sec. 2 [UPX1], unpack "upx.exe -d" from http://upx.github.io or

