

Consegna S10-L1

Analisi Malware

Traccia

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:

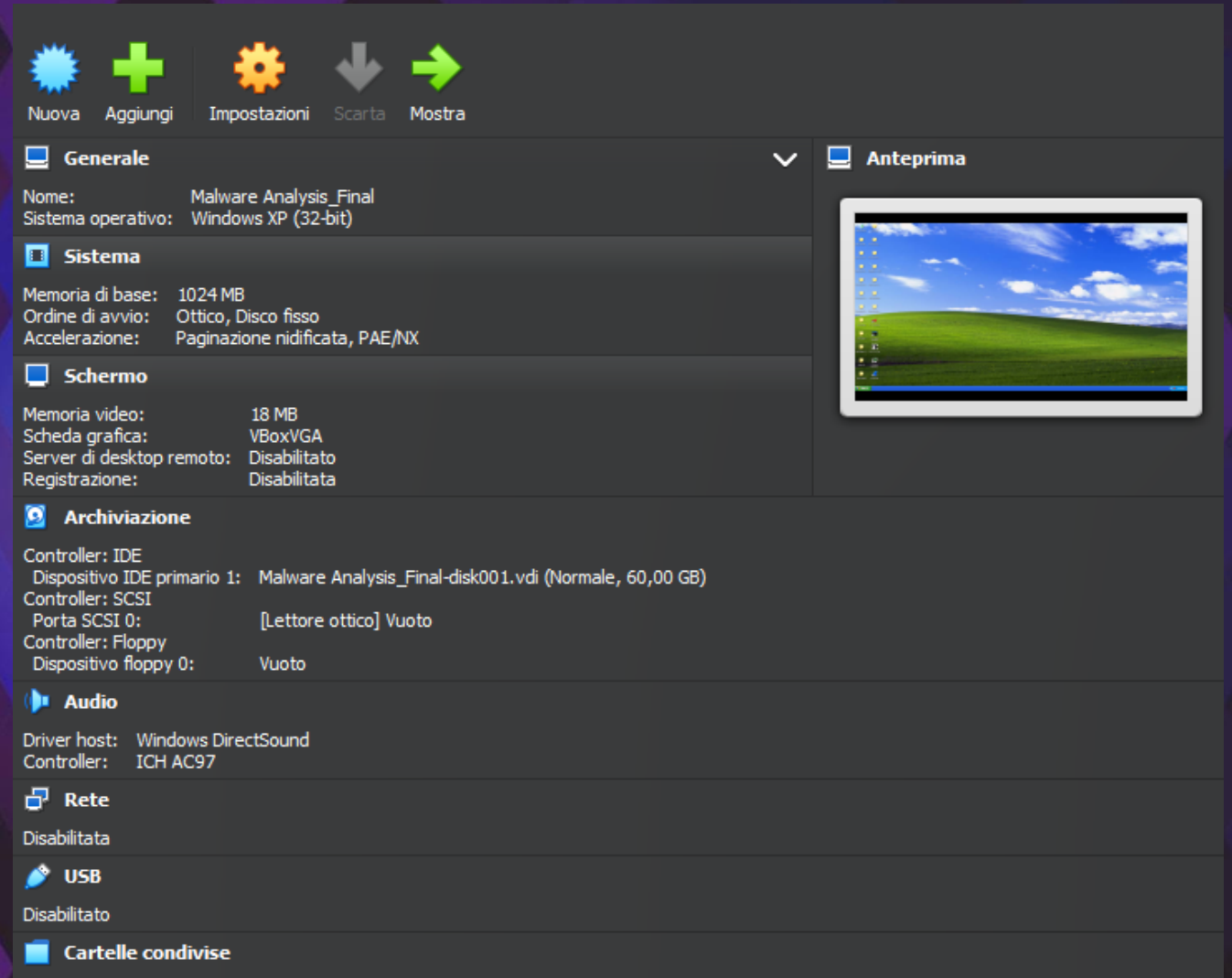
Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse

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

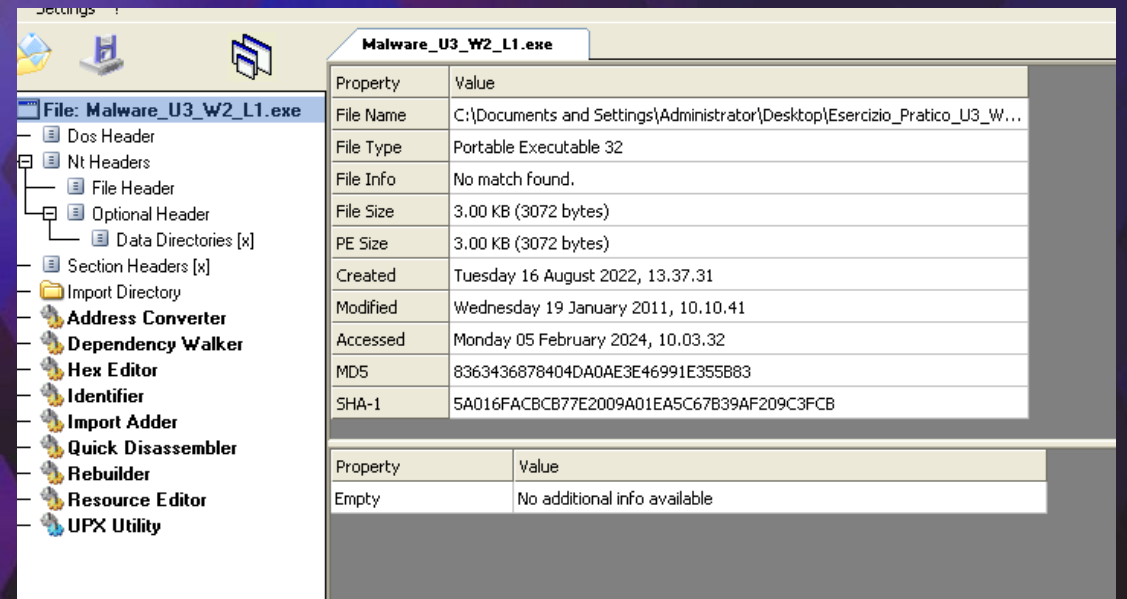
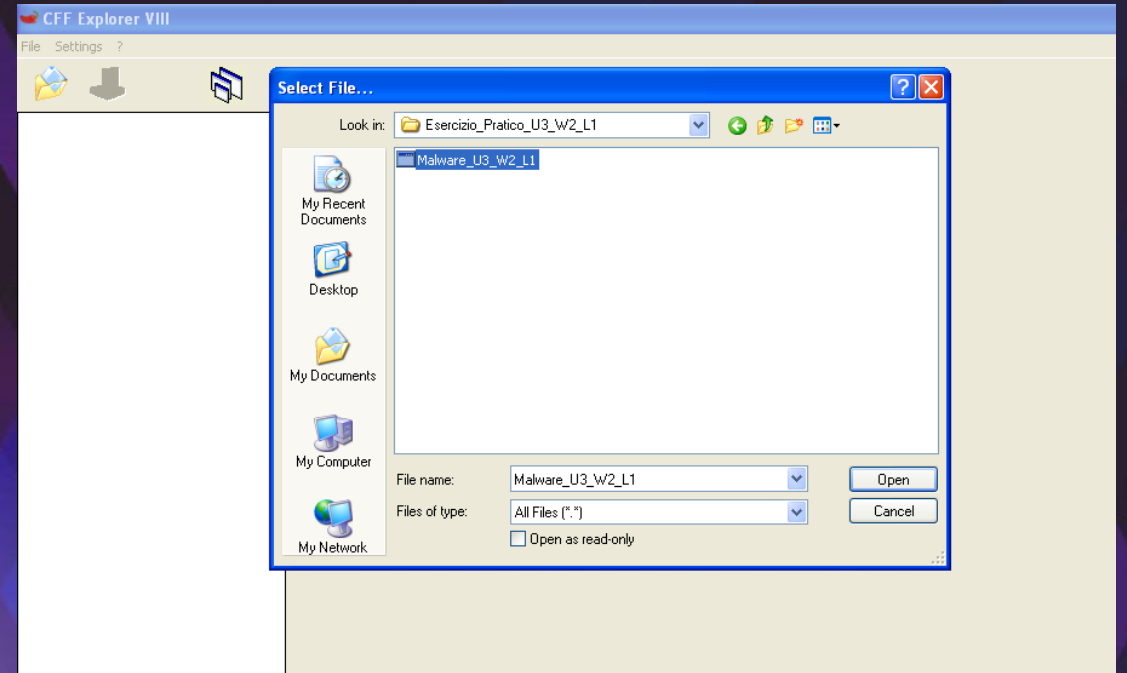
Installazione macchina virtuale

Per svolgere l'esercizio in sicurezza, dato che si ha a che fare con file dannosi, è stato necessario installare la macchina virtuale Malware Analysis su VirtualBox con rete disabilitata. Il sistema operativo della macchina è WindowsXP.



Utilizzo di CFF Explorer

Dopo che CFF Explorer è stato avviato, è stato aperto il file richiesto dalla traccia. CFF Explorer è un tool preinstallato nella macchina che permette di controllare le funzioni importate ed esportate di un malware.



Analisi Import Directory

Selezionando la cartella Import Directory, è stato possibile accedere alla lista delle librerie importate dal malware. La tabella in basso analizza nel dettaglio la libreria al momento evidenziata. In questo caso la KERNEL 32.DLL che contiene le funzioni principali per interagire con il sistema operativo, ad esempio la manipolazione dei file e la gestione della memoria.

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

File: Malware_U3_W2_L1.exe

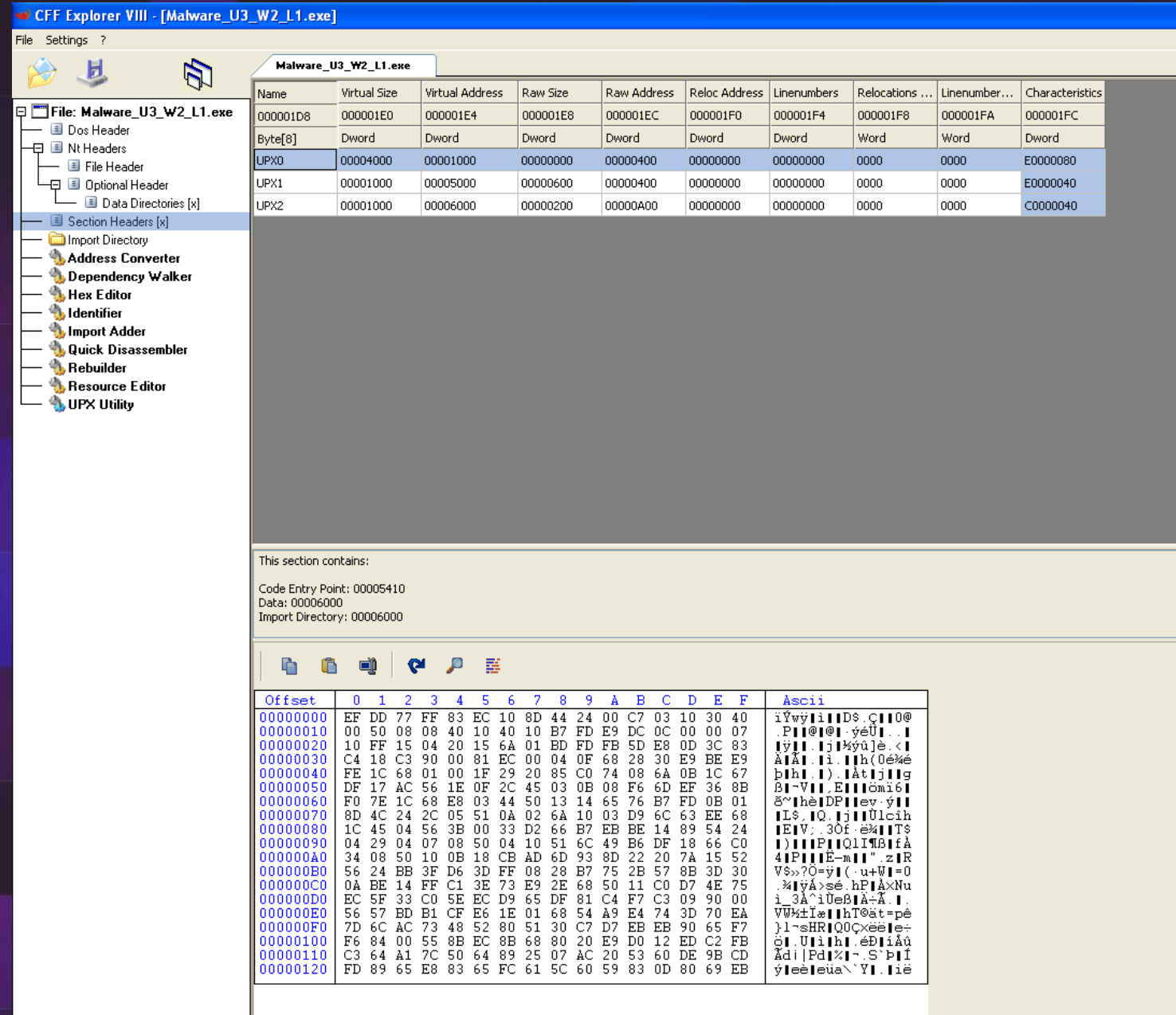
- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
 - Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

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

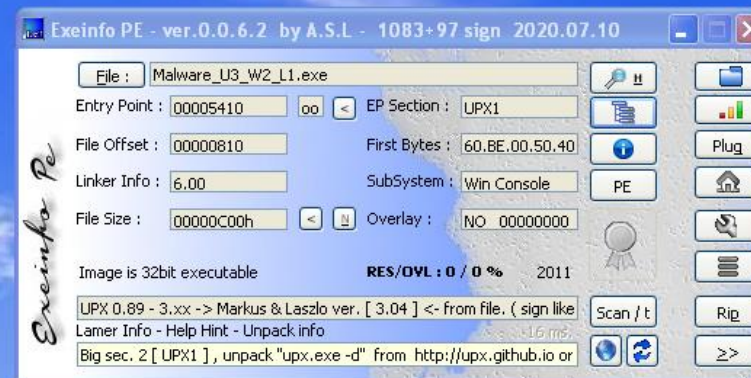
Analisi Section Headers

Nella sezione Section Headers è stato possibile controllare le informazioni circa le sezioni di cui si compone l'eseguibile. Il malware è diviso in tre parti, tutte compresse tramite lo strumento UPX.



Utilizzo ExeinfoPE

Per avere un secondo riscontro, è stato utilizzato anche il tool ExeinfoPE. Una volta caricato il file dannoso sul programma, c'è stato un riscontro sulle informazioni riguardanti le sezioni del malware



The screenshot shows the 'Sections viewer' window for the file 'Matware_U3_W2_1.exe'. The title bar indicates there are 3 sections with an alignment of 1000h. The main area contains a table with columns: Nr, Virtual ..., Virtual ..., RAW D..., RAW size, Flags, Name, First bytes (hex), First Ascii 20h ..., and sect. Stats.

Nr	Virtual ...	Virtual ...	RAW D...	RAW size	Flags	Name	First bytes (hex)	First Ascii 20h ...	sect. Stats
01	00001000	00004000	00000400	00000000	E0000080	UPX0	! Z E R O S I Z E !	?	
02 ep	00005000	00001000	00000400	00000600	E0000040	UPX1	EF DD 77 FF 83 EC 10 8D 44	w □ D\$ □ ...	
03 im	00006000	00001000	00000A00	00000200	C0000040	UPX2	00 00 00 00 00 00 00 00	` d` ...	

Below the table, the 'Overlay:' section shows 'No overlay data'. The 'End of file:' section displays a hex dump of zeros. The 'Section status:' section shows '03' selected, with checkboxes for Executable, Readable, and Writable. The 'Section size:' section shows '512 bytes'. The 'All sections size:' section shows '3 KB'. On the right, there are buttons for 'Cave', 'S-Stat', 'PreScan', and 'Close'.

Considerazioni

L'analisi statica non ha potuto fornirci molte informazioni sul malware. Alcuni malware, come quello in questione, utilizzano ad esempio il caricamento delle librerie durante l'esecuzione (runtime import) nascondendo di fatto all'analisi statica le funzioni e le librerie importate. Questi malware sono riconoscibili in quanto hanno generalmente poche entry nella sezione import, e tra esse figurano le funzioni «LoadLibrary e GetProcAddress» che vengono appunto utilizzate per caricare funzioni aggiuntive durante l'esecuzione.

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



Fine della presentazione

Amedeo Natalizi