



Compito S10/L1



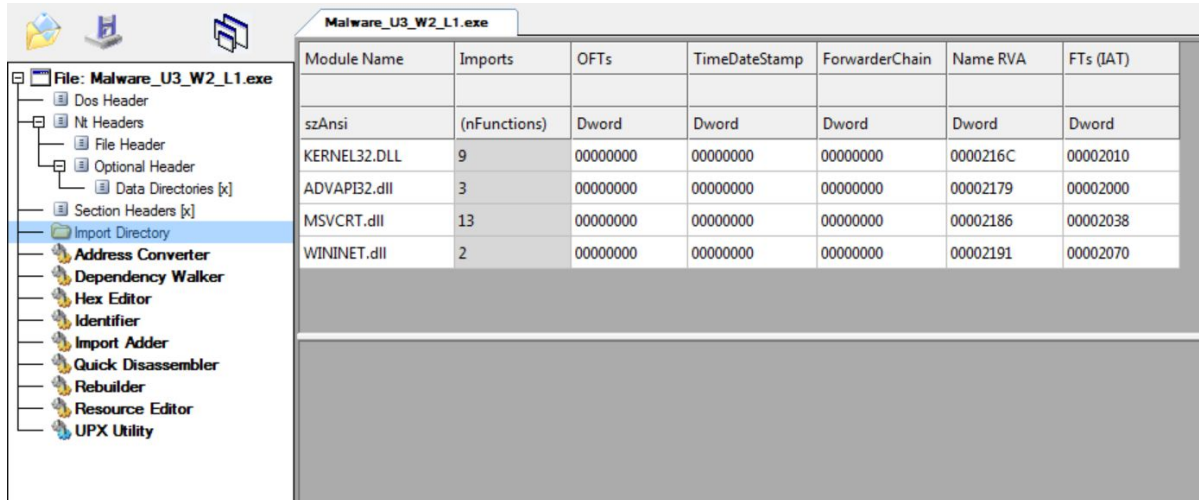
Traccia

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

Esercizio

Andiamo nella VM, apriamo il programma CFF Explorer e andiamo ad aprire il malware dalla cartella Esercizio_Pratico_U3_W2_L1. Successivamente, dirigiamoci nella sezione Import Directory.



The screenshot shows the CFF Explorer interface with the file **Malware_U3_W2_L1.exe** open. The left-hand tree view shows the file's structure, with the **Import Directory** section selected. The right-hand pane displays a table of imported modules.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	9	00000000	00000000	00000000	0000216C	00002010
ADVAPI32.dll	3	00000000	00000000	00000000	00002179	00002000
MSVCRT.dll	13	00000000	00000000	00000000	00002186	00002038
WININET.dll	2	00000000	00000000	00000000	00002191	00002070



Esercizio

In questa sezione possiamo vedere le librerie di questo malware. Andiamo a descriverle una per una:

- **Kernel32.dll**: contiene le funzioni principali per interagire con il sistema operativo, come la manipolazione dei file e la gestione della memoria.
- **Advapi32.dll**: contiene le funzioni per interagire con i servizi e i registri del sistema operativo.
- **MSVCRT.dll**: contiene funzioni per la manipolazione di stringhe, l'allocazione di memoria e altre operazioni, come le chiamate per input/output, tipiche del linguaggio C.
- **Wininet.dll**: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP e NTP.

Esercizio

Se clicchiamo su una libreria, verrà visualizzata una lista delle funzioni richieste all'interno della libreria selezionata.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00002179	N/A	000020A0	000020A4	000020A8	000020AC	000020B0
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	9	00000000	00000000	00000000	0000216C	00002010
ADVAPI32.dll	3	00000000	00000000	00000000	00002179	00002000
MSVCRT.dll	13	00000000	00000000	00000000	00002186	00002038
WININET.dll	2	00000000	00000000	00000000	00002191	00002070

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	0000223C	0000	CreateServiceA
N/A	0000224C	0000	StartServiceCtrlDispatcherA
N/A	0000226A	0000	OpenSCManagerA

Esercizio

Andiamo nella sezione 'Section Headers'. Possiamo vedere le sezioni, ma le visualizziamo in formato UPX. Quindi, procediamo con l'utilizzo di UPX utility per decomprimerle e poterle leggere.

The screenshot displays the CFF Explorer VIII interface for the file 'Malware_U3_W2_L1.exe'. The 'Section Headers [x]' are expanded in the left sidebar. The main pane shows a table of sections:

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

Below the table, the 'UPX Utility' window is open, showing options for packing or unpacking. The 'Unpack' button is highlighted with a red rectangle.

UPX Utility Options:

- ☒ Check if the Portable Executable is already packed
- ☒ Pack Export Directory
- ☒ Pack Resource Directory
- ☐ Force
- ☐ All Methods
- ☐ Exact
- ☐ All Filters
- ☒ Strip Relocation Directory
-
-

Esercizio

Ora vediamo cosa fanno queste sezioni:

- **.text:** contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente, questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, poiché tutte le altre sezioni contengono dati o informazioni di supporto.
- **.rdata:** include generalmente informazioni sulle librerie e sulle funzioni importate ed esportate dall'eseguibile. Come abbiamo visto, possiamo estrarre queste informazioni utilizzando CFF Explorer.
- **.data:** contiene tipicamente i dati e le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma. Una variabile si dice globale quando non è definita all'interno di un contesto di una funzione, ma è globalmente dichiarata ed è quindi accessibile da qualsiasi funzione all'interno dell'eseguibile.

Malware_U3_W4_L1.exe									
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
00000228	00000230	00000234	00000238	0000023C	00000240	00000244	00000248	0000024A	0000024C
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000002DC	00001000	00001000	00001000	00000000	00000000	0000	0000	60000020
.rdata	00000372	00002000	00001000	00002000	00000000	00000000	0000	0000	40000040
.data	0000008C	00003000	00001000	00003000	00000000	00000000	0000	0000	C0000040