

Report S10 L1

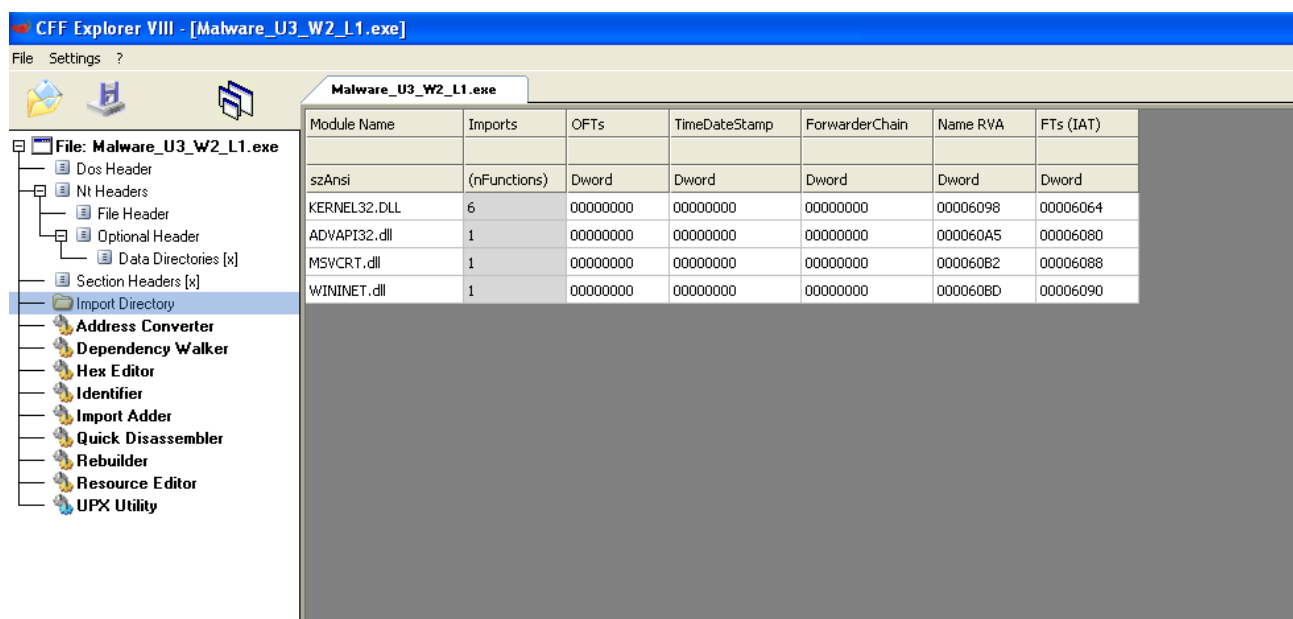
Analisi Statica Basica

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:

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

Come richiesto dall'esercizio, andiamo ad analizzare le librerie e le funzioni che vengono importate con questo Malware, per fare ciò utilizziamo CFF Explorer, un tool che ci permette di controllare librerie e funzioni che ogni malware o programma importa quando eseguito:



CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	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

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

Le librerie che vengono importate quindi sono:

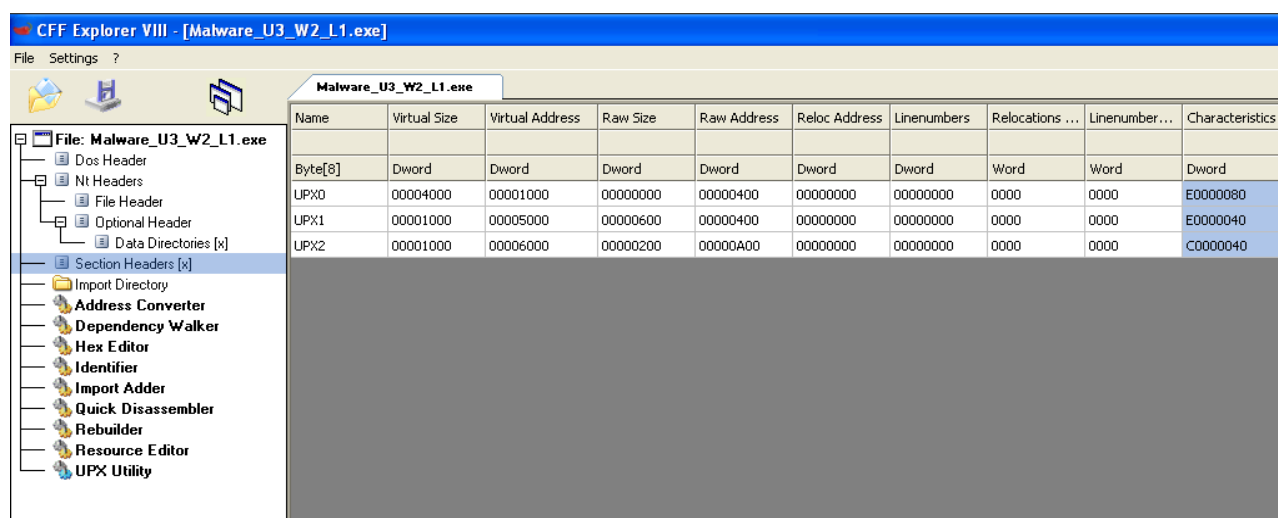
Kernel32.dll : Libreria piuttosto comune che contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.

Advapi32.dll : Libreria che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft.

Wininet.dll: Libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

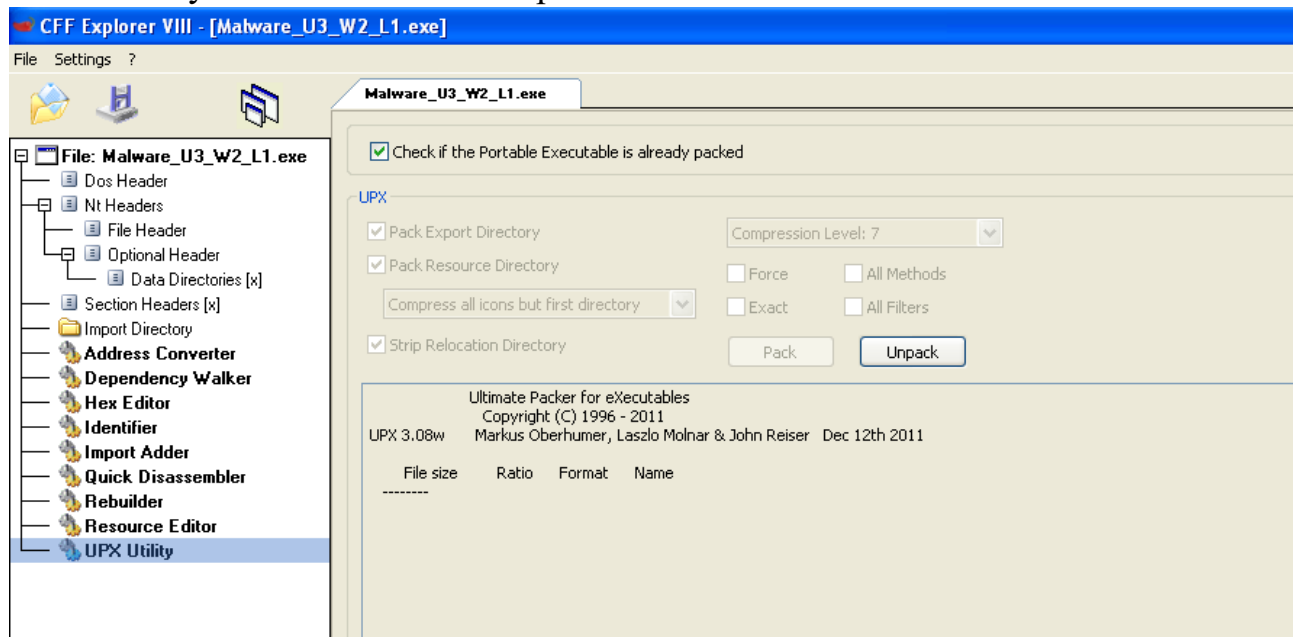
MSVCRT.dll: Libreria che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output in stile linguaggio C.

A questo punto, utilizzando lo stesso tool possiamo procedere con l'analisi delle sezioni di cui si compone il malware.

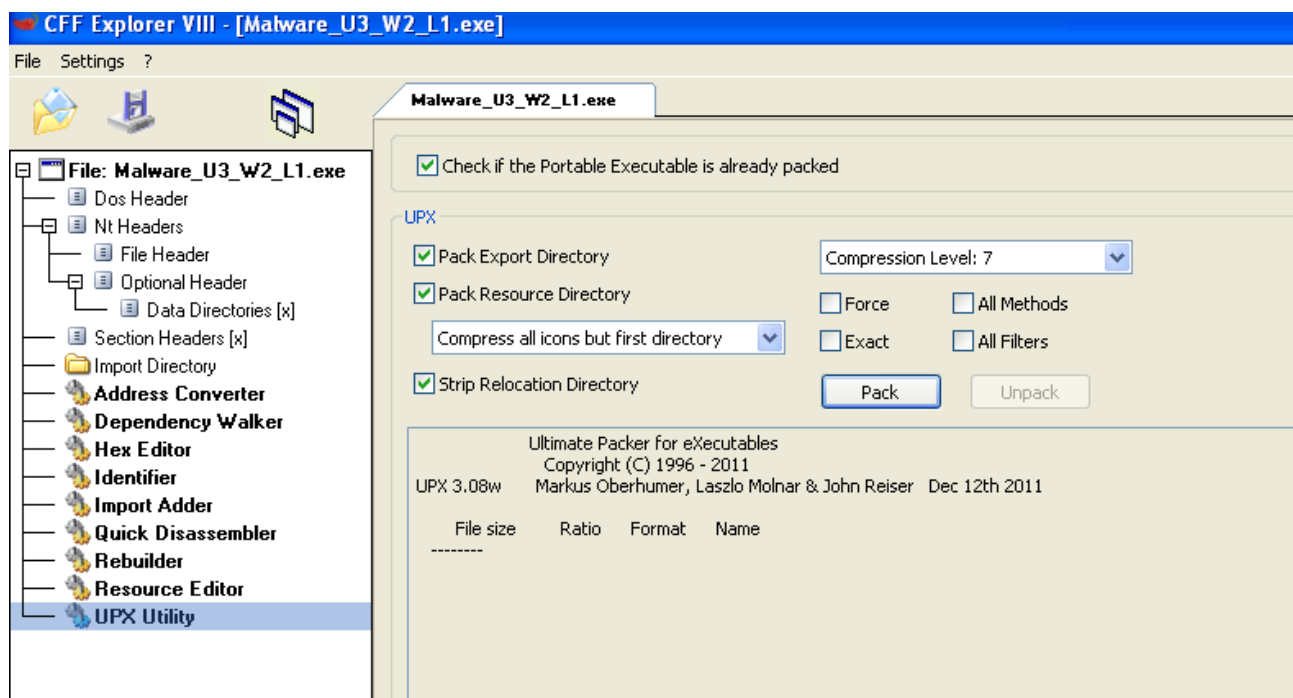


Le sezioni riportate sono state compresse utilizzando il tool UPX, tale tool comprime gli eseguibili rendendo inaccessibile il formato PE della sezione.

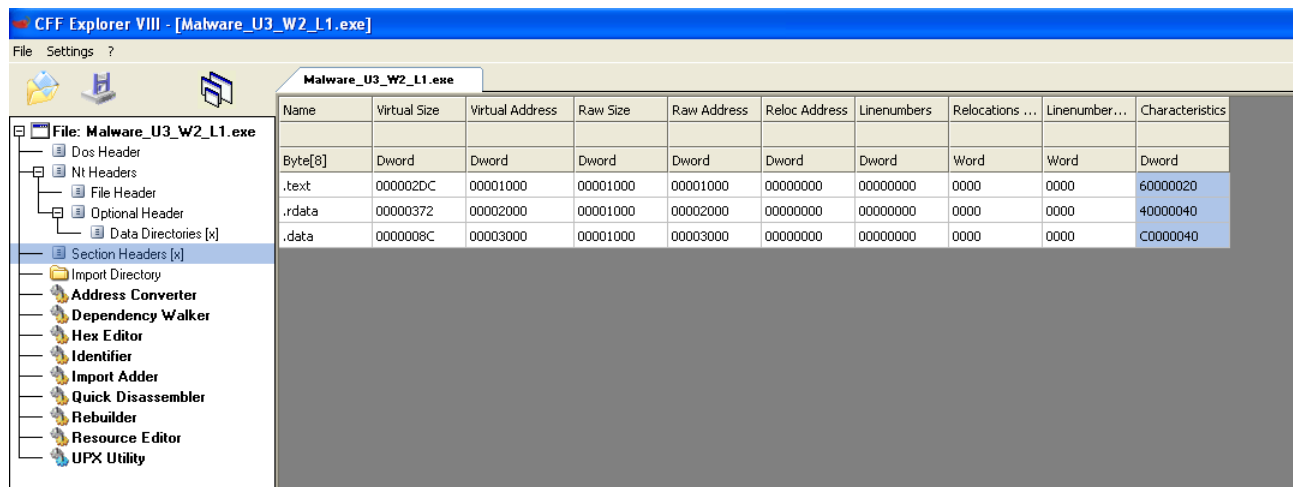
Per decomprimere il formato PE, possiamo recarci dal menù a sinistra nella scheda “UPX Utility” e clicchiamo su “Unpack”.



Successivamente dovrebbe apparire una schermata del genere.



A questo punto, recandoci nuovamente sulla scheda “Section Headers” possiamo analizzare ogni singola sezione.



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
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

I formati che abbiamo rilevato sono:

.text: La sezione «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, in quanto tutte le altre sezioni contengono dati o informazioni a supporto.

.rdata: La sezione «rdata» include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer. (modificato)

.data: La sezione «data» contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma. Ricordate che una variabile si dice globale quando non è definita all'interno di un contesto di una funzione, ma bensì è globalmente dichiarata ed è di conseguenza accessibile da qualsiasi funzione dell'eseguibile.

A questo punto, analizzando singolarmente ogni sezione, ci rendiamo conto che la sezione .text e .rdata sono crittate e indecifrabili senza l'ausilio di altri tool, tuttavia abbiamo scoperto tramite l'analisi della sezione .data che il malware si connette, dopo aver creato un servizio "MalService HGL345", all'url <http://www.malwareanalysisbook.com> utilizzando internet explorer alla versione 8.0 come tramite.

.data	0000008C	00003000	00001000	00003000	00000000	00000000	0000	0000	C0000040
-------	----------	----------	----------	----------	----------	----------	------	------	----------

This section contains:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000010	4D	61	6C	53	65	72	76	69	63	65	00	00	4D	61	6C	73	MalService..Mals
00000020	65	72	76	69	63	65	00	00	48	47	4C	33	34	35	00	00	ervice..HGL345..
00000030	68	74	74	70	3A	2F	2F	77	77	77	2E	6D	61	6C	77	61	http://www.malwa
00000040	72	65	61	6E	61	6C	79	73	69	73	62	6F	6F	6B	2E	63	reanalysisbook.c
00000050	6F	6D	00	00	49	6E	74	65	72	6E	65	74	20	45	78	70	om..Internet,Exp
00000060	6C	6F	72	65	72	20	38	2E	30	00	00	00	01	00	00	00	lorer.8.0...I...
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Con le nostre conoscenze attuali non ci è possibile analizzare cosa il servizio creato fa.