



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



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)
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

Utilizzando **CFF Explorer** analizziamo librerie e funzioni importate dall'eseguibile che stiamo analizzando

Le librerie richiamate sono:

- kernel32.dll
- advapi32.dll
- wininet32.dll
- msvcrt.dll



Approfondimento: DLL

un "Dynamic Link Library" o DLL è un tipo di file eseguibile in ambiente Windows che contiene codice e dati che possono essere utilizzati da più programmi contemporaneamente.

A differenza di un'applicazione autonoma, una DLL non può essere eseguita direttamente, ma fornisce funzionalità condivise che possono essere richiamate da diverse applicazioni.

kernel32.dll:

- Fornisce funzioni di basso livello che gestiscono memoria, file, processi e altri aspetti fondamentali del sistema operativo.
- Include funzioni per la gestione dei processi, sincronizzazione, allocazione di memoria e la gestione delle eccezioni.
- È una delle DLL principali di Windows e molte altre DLL fanno riferimento a sue funzioni

advapi32.dll:

- Contiene funzioni per la gestione dei servizi, la sicurezza e le operazioni relative al registro di sistema.
- Fornisce un'interfaccia per interagire con il sottosistema di sicurezza di Windows.
- Include funzionalità per la gestione degli account utente, l'accesso alle informazioni sul sistema e la manipolazione del registro di sistema.



wininet.dll:



- Offre funzioni per la gestione delle operazioni di rete, inclusi protocolli come HTTP, FTP e altri.
- È coinvolta nella gestione delle connessioni Internet e fornisce un'interfaccia per le operazioni di navigazione e download.
- Utilizzata da molti programmi per interagire con il Web e le risorse Internet.

MSVCRT.dll:

- La libreria di runtime di Microsoft Visual C++, che fornisce funzioni standard del linguaggio C.
- Contiene implementazioni delle funzioni standard della libreria C come quelle per la gestione della memoria, le stringhe, l'input/output e altre operazioni di base.
- È essenziale per l'esecuzione di programmi scritti in linguaggio C++ che utilizzano il compilatore Microsoft Visual C++.





CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

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
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

File: Malware_U3_W2_L1.exe

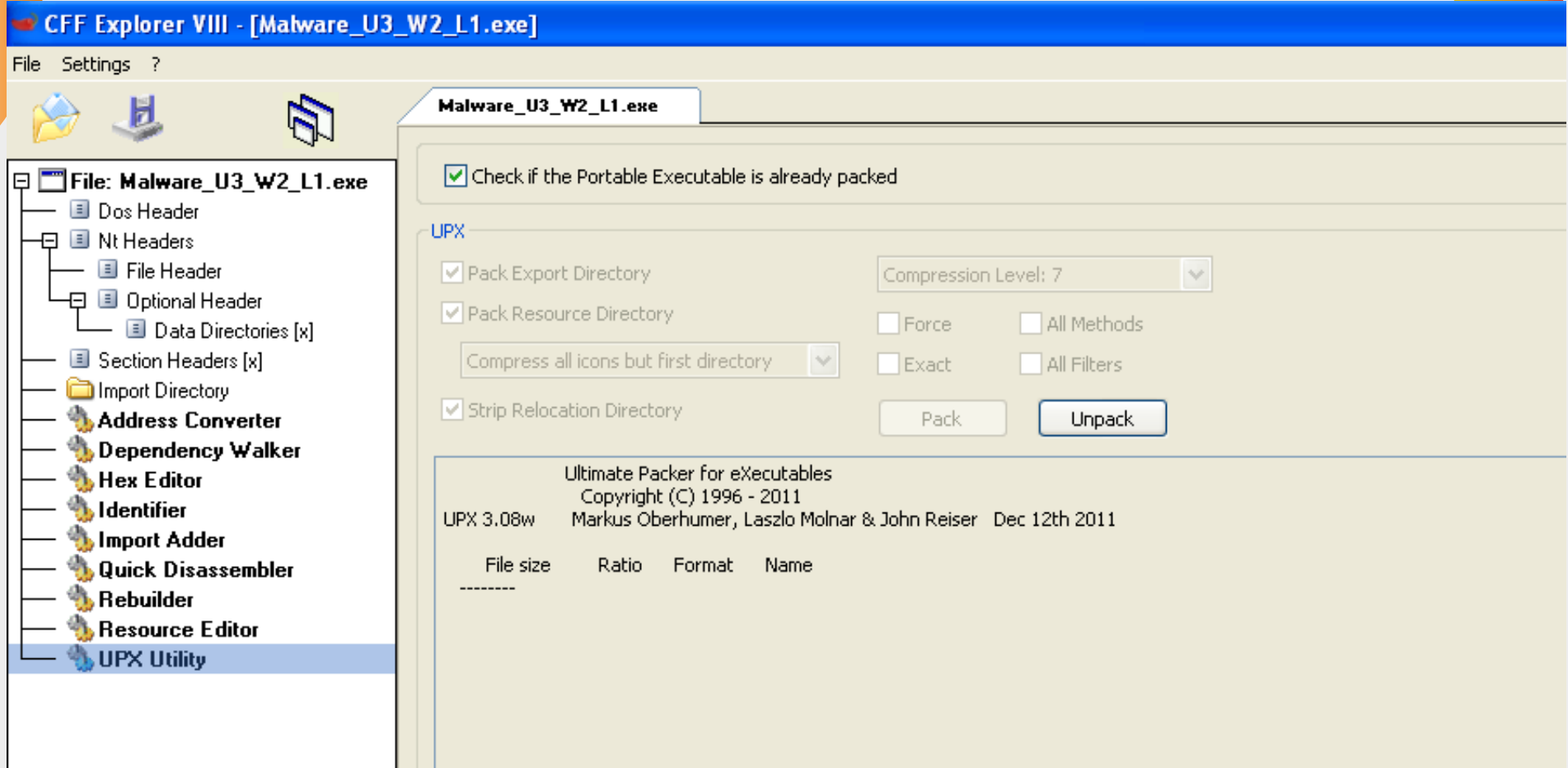
- Dos Header
- Nt Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F Ascii

00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZyy..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	E0	00	00	00
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	? Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is.program.canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t.be.run.in.DOS.
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode...\$
00000080	E3	C1	65	8F	A7	A0	0B	DC	A7	A0	0B	DC	A7	A0	0B	DC	3Ae \$ U\$ U\$ U
00000090	4F	BF	01	DC	AC	A0	0B	DC	24	BC	05	DC	A6	A0	0B	DC	Oz U~ U\$ U U
000000A0	4F	BF	0F	DC	A5	A0	0B	DC	A7	A0	0B	DC	A3	A0	0B	DC	Oz U~ U\$ U\$ U
000000B0	A7	A0	0A	DC	EC	A0	0B	DC	C5	BF	18	DC	A2	A0	0B	DC	\$ U~ U\$ U\$ U
000000C0	4F	BF	00	DC	A5	A0	0B	DC	52	69	63	68	A7	A0	0B	DC	Oz U~ U\$ U\$ U
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000E0	50	45	00	00	4C	01	03	00	01	0D	37	4D	00	00	00	00	PE..L ...7M...
000000F0	00	00	00	00	E0	00	0F	01	0B	01	06	00	00	10	00	00	...&P
00000100	00	10	00	00	00	40	00	00	10	54	00	00	00	50	00	00	...@... T...P
00000110	00	60	00	00	00	00	40	00	00	10	00	00	00	02	00	00	...@...

Con lo stesso tool possiamo continuare con l'analisi delle sezioni che compongono il malware

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



Per ovviare a questo problema, utilizziamo la funzione UPX utility per decomprimere il PE tramite il tasto "unpack"

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

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

Tornando alla sezione "section headers" possiamo procedere ad analizzare le sezioni trovate:

.text: La sezione "text" comprende le istruzioni, ovvero le linee di codice, che la CPU eseguirà una volta avviato il software. Di solito, questa è l'unica sezione di un file eseguibile che la CPU esegue, poiché tutte le altre sezioni contengono dati o informazioni di supporto.

.rdata: La sezione "rdata" contiene informazioni sulle librerie e sulle funzioni importate o esportate dall'eseguibile.

.data: La sezione "data" contiene i dati o le variabili globali del programma eseguibile. Si noti che una variabile viene considerata globale quando non è definita all'interno del contesto di una funzione, ma è dichiarata globalmente e, di conseguenza, è accessibile da qualsiasi funzione dell'eseguibile.



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
00001000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00001100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

analizzando ogni sezione, ci rendiamo conto che .text e .rdata sono crittate e indecifrabili, tuttavia abbiamo scoperto tramite .data che il malware si connette, dopo aver creato un servizio “MalService HGL345”, all'url “http://www.malwareanalysisbook.com”