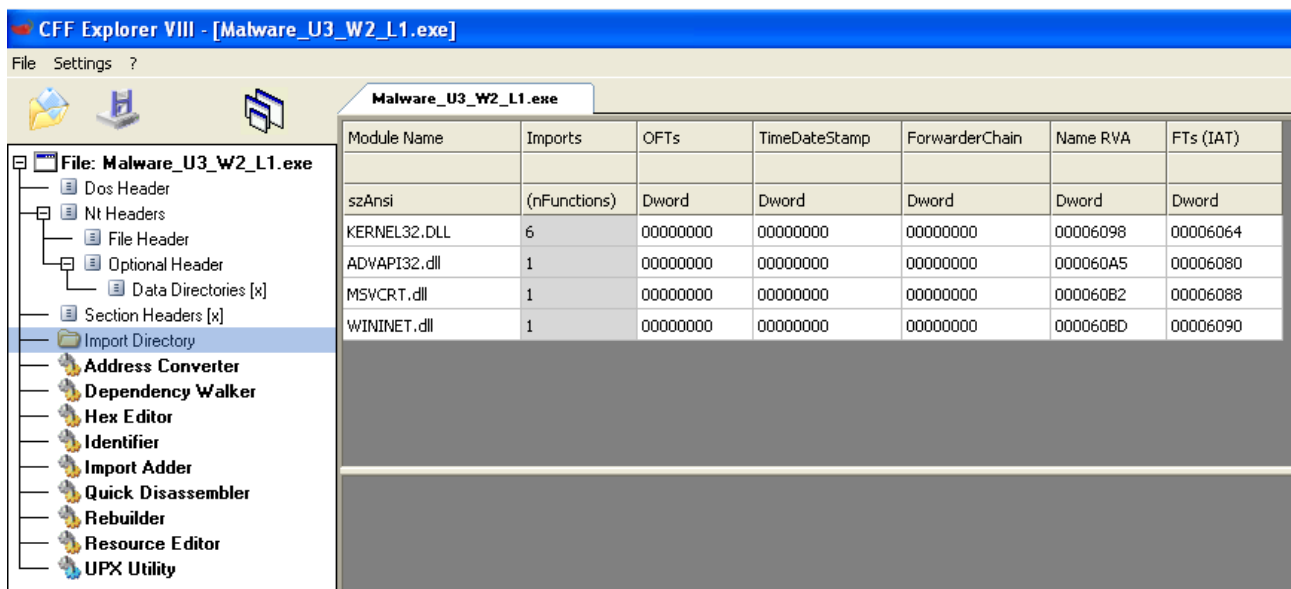
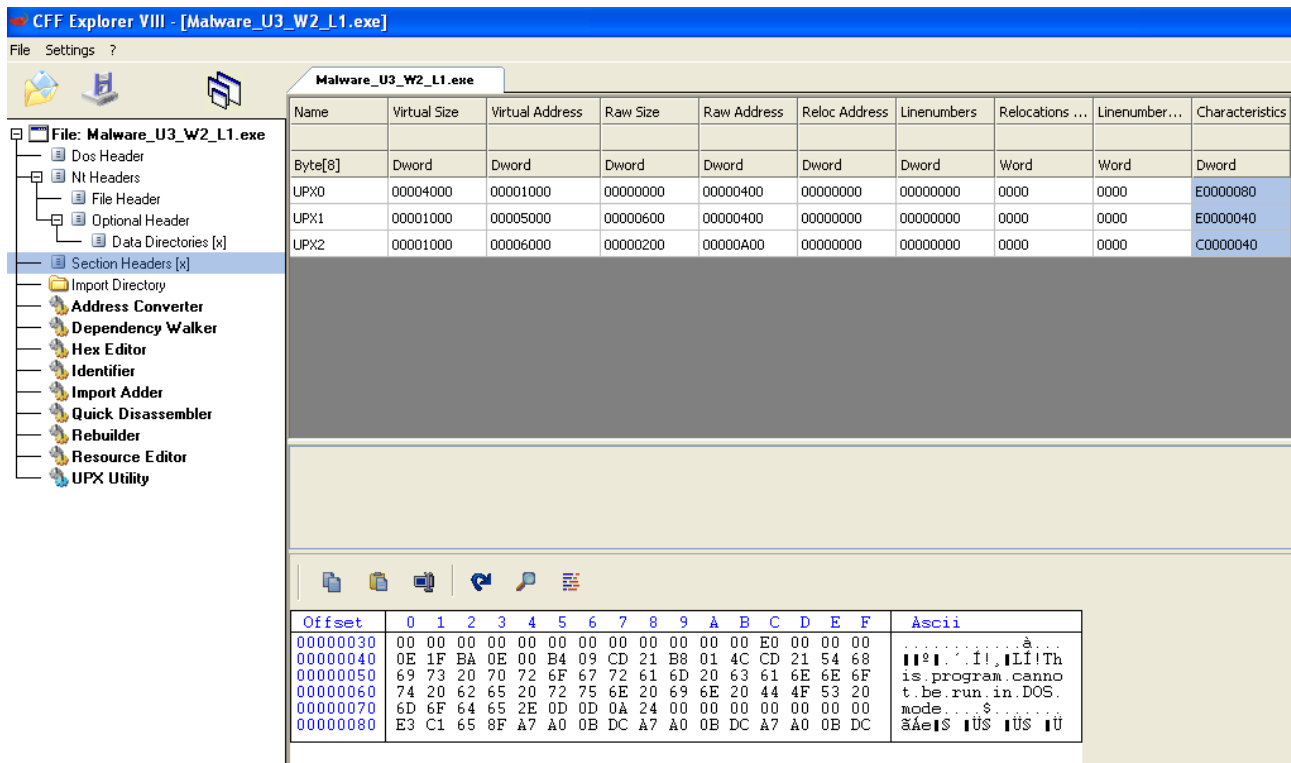


Analisi statica basica

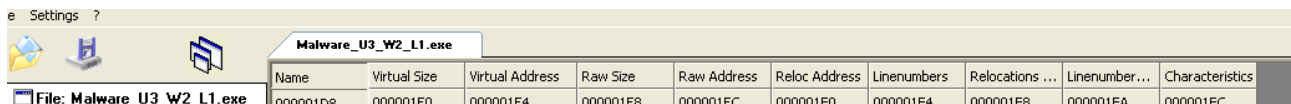
Dopo aver aperto l'esercizio sulla macchina, procedo con un'analisi statica basica



In section headers vediamo che il file eseguibile è composto da 3 sezioni, il cui vero nome è nascosto. La dicitura UPX infatti ci suggerisce che il file è compresso.



Per scoprire ulteriori informazioni sull'eseguibile si può andare nella sezione "UPX Utility" e selezionare l'opzione "unpack". Dopo aver effettuato questa operazione, tornando su section headers avremo le seguenti informazioni:



- 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

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

This section contains:

Code Entry Point: 00001190

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	83	EC	10	8D	44	24	00	C7	44	24	00	10	30	40	00	50	i i i D s . c D s . i 0 @ . P
00000010	C7	44	24	08	40	10	40	00	C7	44	24	0C	00	00	00	00	c D s i @ i @ . c D s i
00000020	C7	44	24	10	00	00	00	00	FF	15	04	20	40	00	6A	00	c D s i y i i . @ . j .
00000030	6A	00	E8	09	00	00	00	83	C4	18	C3	90	90	90	90	90	j . e i i i i i i i i
00000040	81	EC	00	04	00	00	68	28	30	40	00	6A	00	68	01	00	i i . . . h (0 @ . j . h i .
00000050	1F	00	FF	15	20	20	40	00	85	C0	74	08	6A	00	FF	15	i . y i . . . @ . i a t i j . y i

E in questo modo troviamo un link in chiaro che può essere googato

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

This section contains:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000010	4D	61	6C	53	65	72	76	69	63	65	00	00	4D	61	6C	73	M a l S e r v i c e . . M a l s
00000020	65	72	76	69	63	65	00	00	48	47	4C	33	34	35	00	00	e r v i c e . . H G L 3 4 5 . .
00000030	68	74	74	70	3A	2F	2F	77	77	77	2E	6D	61	6C	77	61	h t t p : / / w w w . m a l w a
00000040	72	65	61	6E	61	6C	79	73	69	73	62	6F	6F	6B	2E	63	r e a n a l y s i s b o o k . c
00000050	6F	6D	00	00	49	6E	74	65	72	6E	65	74	20	45	78	70	o m . . I n t e r n e t . E x p
00000060	6C	6F	72	65	72	20	38	2E	30	00	00	00	01	00	00	00	l o r e r . 8 . 0

Dal momento in cui non mi fido molto di googlare questo risultato, lo mando in pasto a VirusTotal. 2 Vendors l'hanno idenfiticato come un malware, tuttavia non hanno specificato la tipologia.

<http://www.malwareanalysisbook.com/>

2 / 90

2 security vendors flagged this URL as malicious

200 Status

2023-02-09 05:23:19 UTC 1 month ago

Community Score

DETECTIONDETAILSCOMMUNITY 4

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘDo you want to automate checks?

ESET

Malware

Fortinet

Malware

In conclusione:

File Settings ?

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

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeStamp	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

La presenza delle due librerie evidenziate tra quelle importate, ci fa capire che si tratta di un malware che importa librerie runtime, nascondendo le informazioni sulle librerie importate a monte.

Sappiamo, pertanto, con l'analisi statica basica, semplicemente che si tratta di un malware avanzato che non ci consente di recuperare molte informazioni sul suo comportamento.