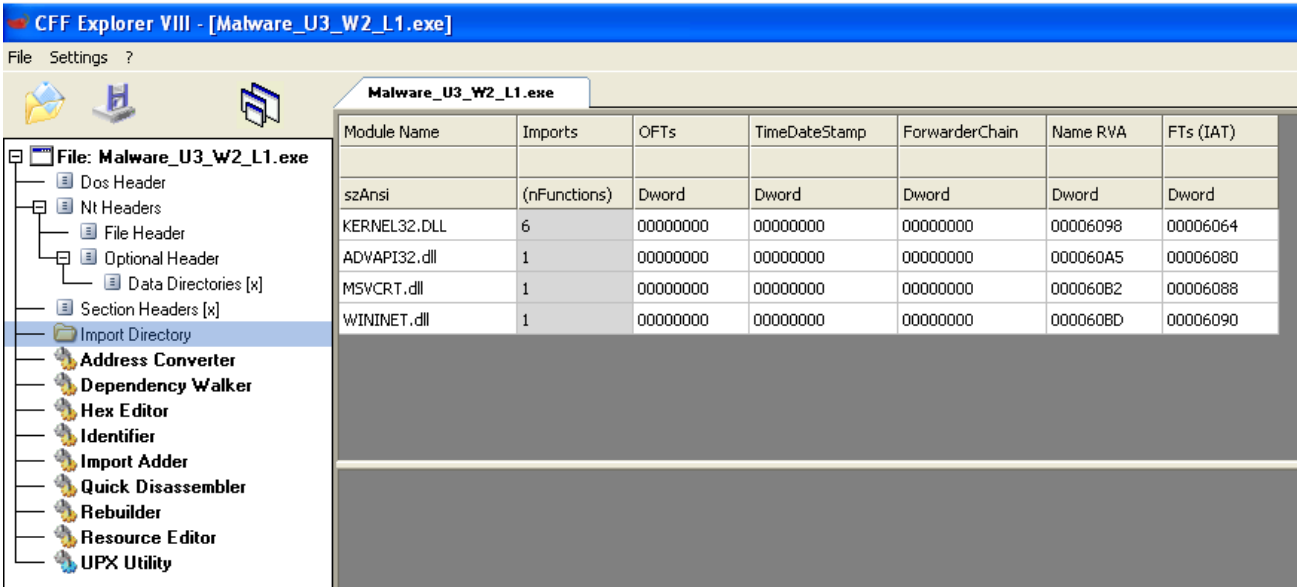
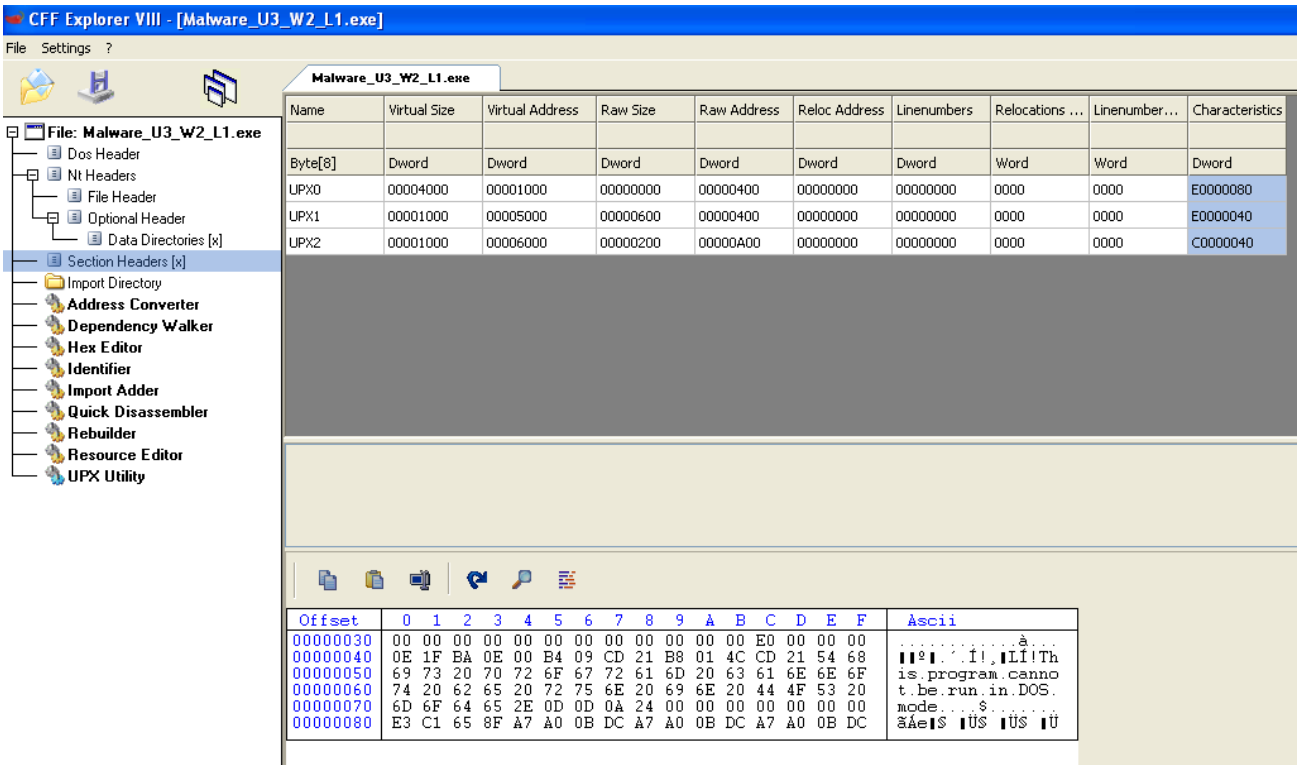


Analisi statica basica

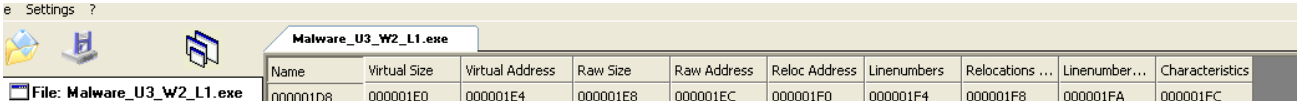
Dopo aver aperto l'esercizio sulla macchina, procedo con un'analisi statica basica

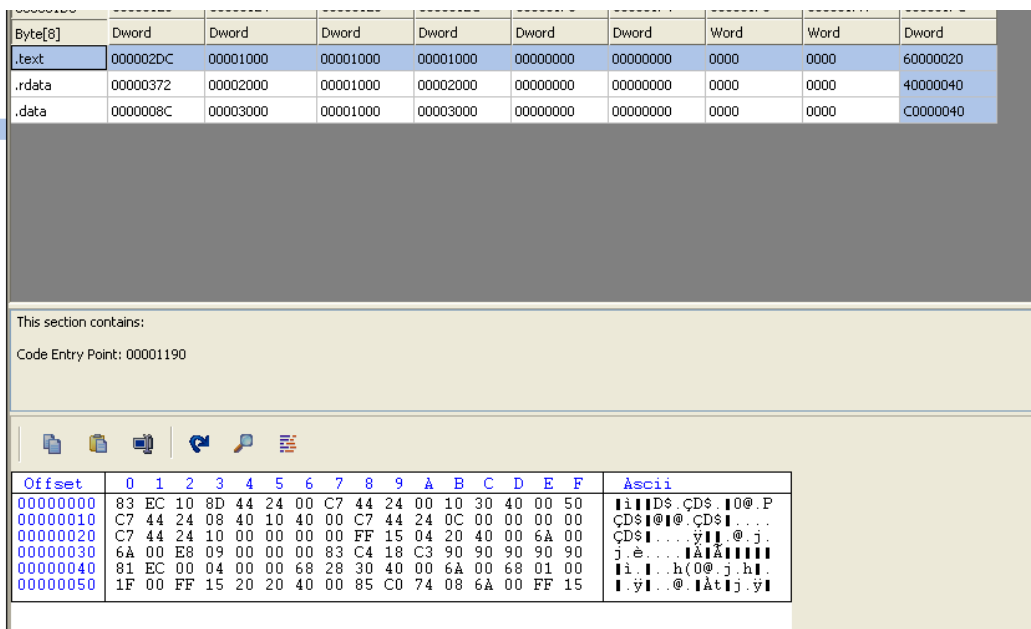


In section headers vediamo che il file eseguibile è composto da 3 sezioni, il cui vero nome è nascosto. La dicitura UPX infatti ci suggerisce che il file è compresso.



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:





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	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...

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

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' analysisDo you want to automate checks?

ESET

Malware

Fortinet

Malware

Tuttavia, possiamo dare in pasto a Virus total anche l'MD5 che troviamo nella sezione "Dependency Walker" dopo aver spaccettato il file iniziale. Ci accorgeremo che si tratta quasi certamente di un Trojan

FileMacchinaVisualizzaInserimentoDispositiviAiuto

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

FileSettings?

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

Malware_U3_W2_L1.exe

KERNEL32.DLL

ADVAPI32.dll

MSVCRT.dll

WININET.dll

Property	Value
File Name	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W...
File Type	Portable Executable 32
File Info	No match found.
File Size	3.00 KB (3072 bytes)
PE Size	16.00 KB (16384 bytes)
Created	Tuesday 16 August 2022, 14:37:31
Modified	Wednesday 19 January 2011, 11:10:41
Accessed	Tuesday 28 March 2023, 14:20:07
MD5	AE4CA70697DF5506BC610172CFC288E7
SHA-1	31E8A82E497058FF14049CF283B337EC51504819

Property	Value
Empty	No additional info available

8bcbe24949951d8aae6018b87b5ca799efe47aeb623e6e5d3665814c6d59aeae

Sign inSign up

54 / 69

54 security vendors and no sandboxes flagged this file as malicious

8bcbe24949951d8aae6018b87b5ca799efe47aeb623e6e5d3665814c6d59aeae

16.00 KBSize

2023-03-27 15:40:41 UTC23 hours ago

Lab01-02.exe

peexechecks-disk-spacedetect-debug-environmentidlearmadillochecks-user-inputlong-sleeps

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY 16

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

Popular threat labeltrojan.ulise/trojanclickerThreat categoriestrojanspywareFamily labelsulisetrojanclickeradwarex

Security vendors' analysisDo you want to automate checks?

AhnLab-V3

Trojan/Win32.StartPage.C26214

Alibaba

TrojanClicker.Win32/Tnega.f5b4d3af

ALYac

Gen.Variant.Ser.Ulise.216

Antiy-AVL

Trojan/Win32.TSGeneric

Arcabit

Trojan.Ser.Ulise.216

Avast

Win32:AdwareX-gen [Adw]

AVG

Win32:AdwareX-gen [Adw]

Avira (no cloud)

TR/Dowm.7734716

AhnLab-V3	Trojan/Win32.StartPage.C26214	Alibaba	TrojanClicker.Win32/Tnega.f5b4d3af
ALYac	Gen.Variant.Ser.Ulise.216	Antiy-AVL	Trojan/Win32.TSGeneric
Arcabit	Trojan.Ser.Ulise.216	Avast	Win32:AdwareX-gen [Adw]
AVG	Win32:AdwareX-gen [Adw]	Avira (no cloud)	TR/Dowm.7734716

AVG	Win32:AdwareX-gen [Adw]	Avira (no cloud)	I/Rogue.1/34/1b
BitDefender	Gen:Variant.Ser.Ulise.216	BitDefenderTheta	Gen:NN.ZexaF.36344.bmW@aG9@v0b
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Agent.DJC.gen[Eldorado
DrWeb	Trojan.Click3.12740	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Ser.Ulise.216 (B)	eScan	Gen:Variant.Ser.Ulise.216
ESET-NOD32	A Variant Of Win32/TrojanClicker.Agent....	F-Secure	Heuristic.HEUR/AGEN.1223661
Fortinet	W32/Agent.NVMltr	GData	Gen:Variant.Ser.Ulise.216
Google	Detected	Ikarus	Trojan.Win32.TrojanClicker
Jiangmin	Trojan.Generic.fxlq	K7AntiVirus	Spyware (0049d4ee1)

In conclusione, a dispetto delle analisi fatte successivamente, non totalmente inerenti all'analisi statica, 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.

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	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

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.