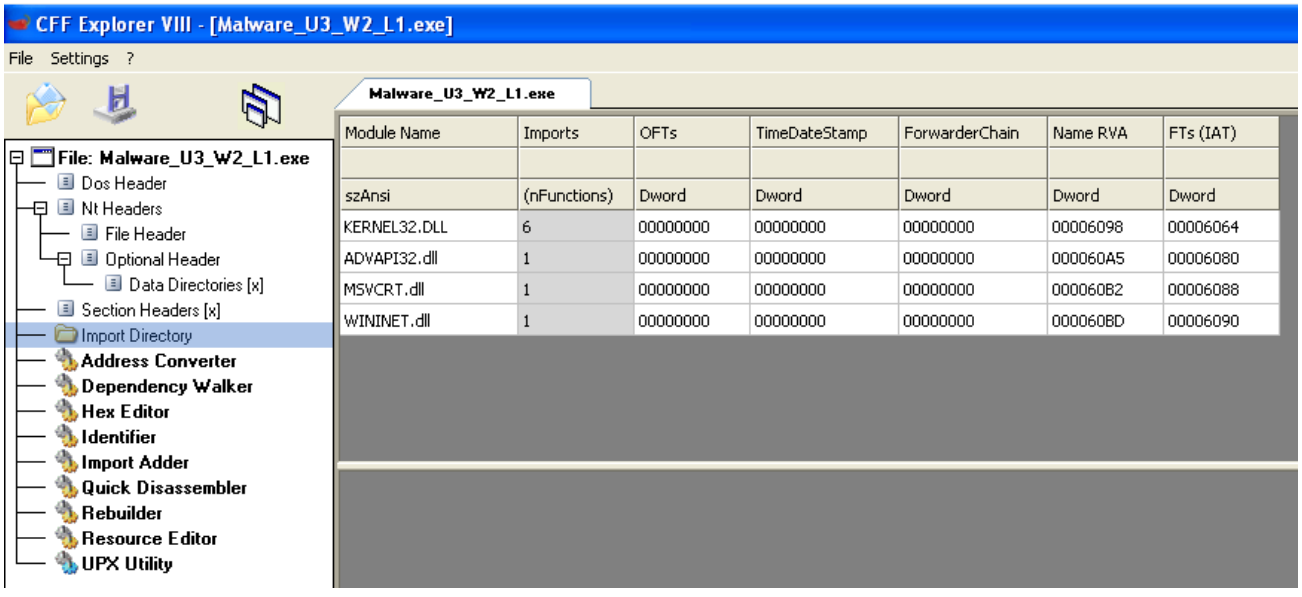
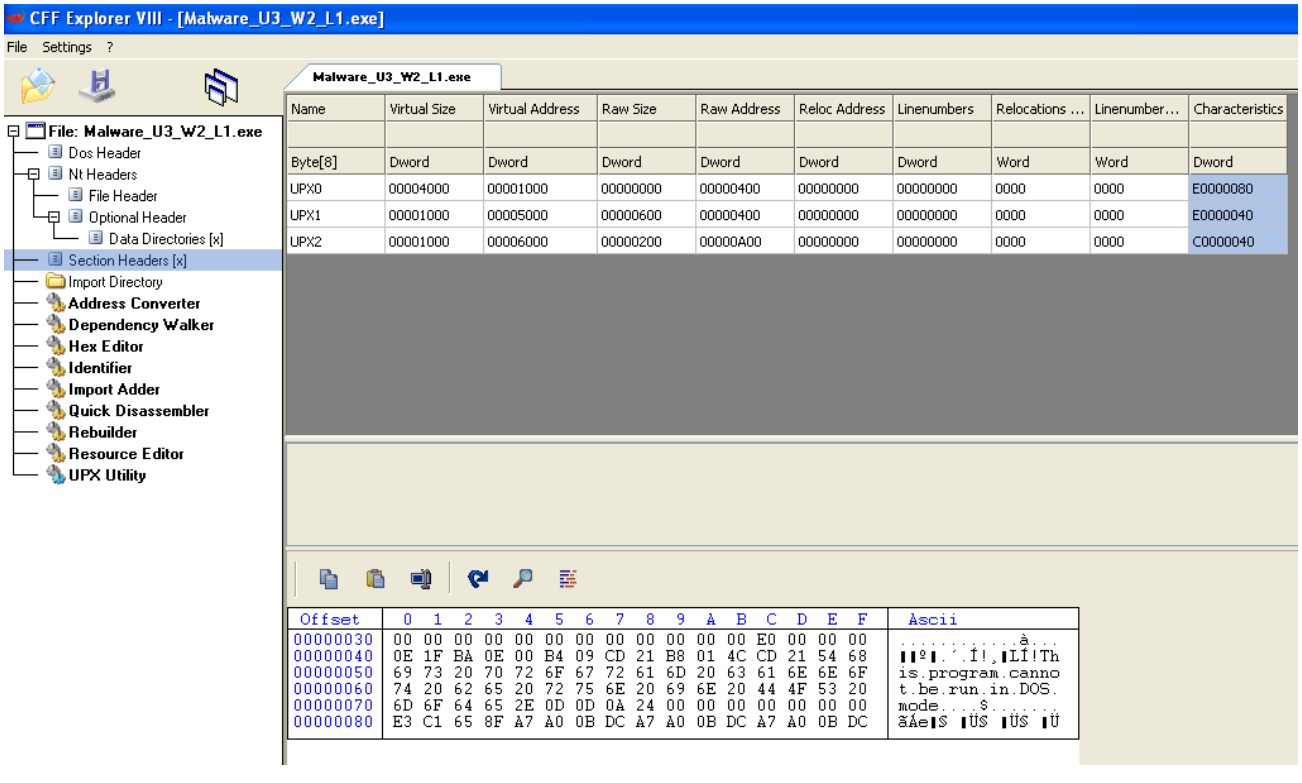
Analisi statica basica

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



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

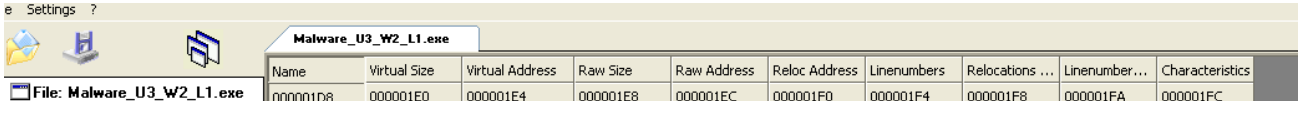
In section headers vediamo che il file eseguibile è composto da 3 sezioni, il cui vero nome è nascosto. La dicitura UPX infatti ci suggerisce che il file è compresso.



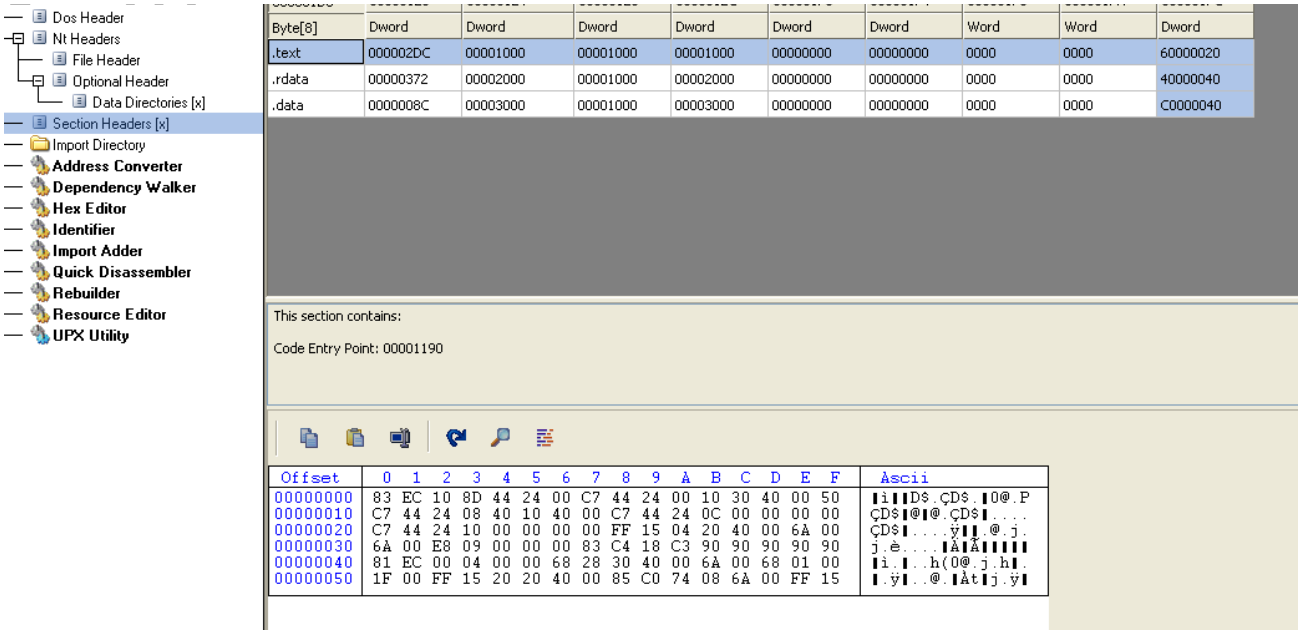
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400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

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000030	00	00	00	00	00	00	00	00	00	00	00	00	E0	00	00	00	..... à...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	▮▮º▮.´.Í!¸▮LÍ!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	ãÁe▮§ ▮Ü§ ▮Ü§ ▮Ü

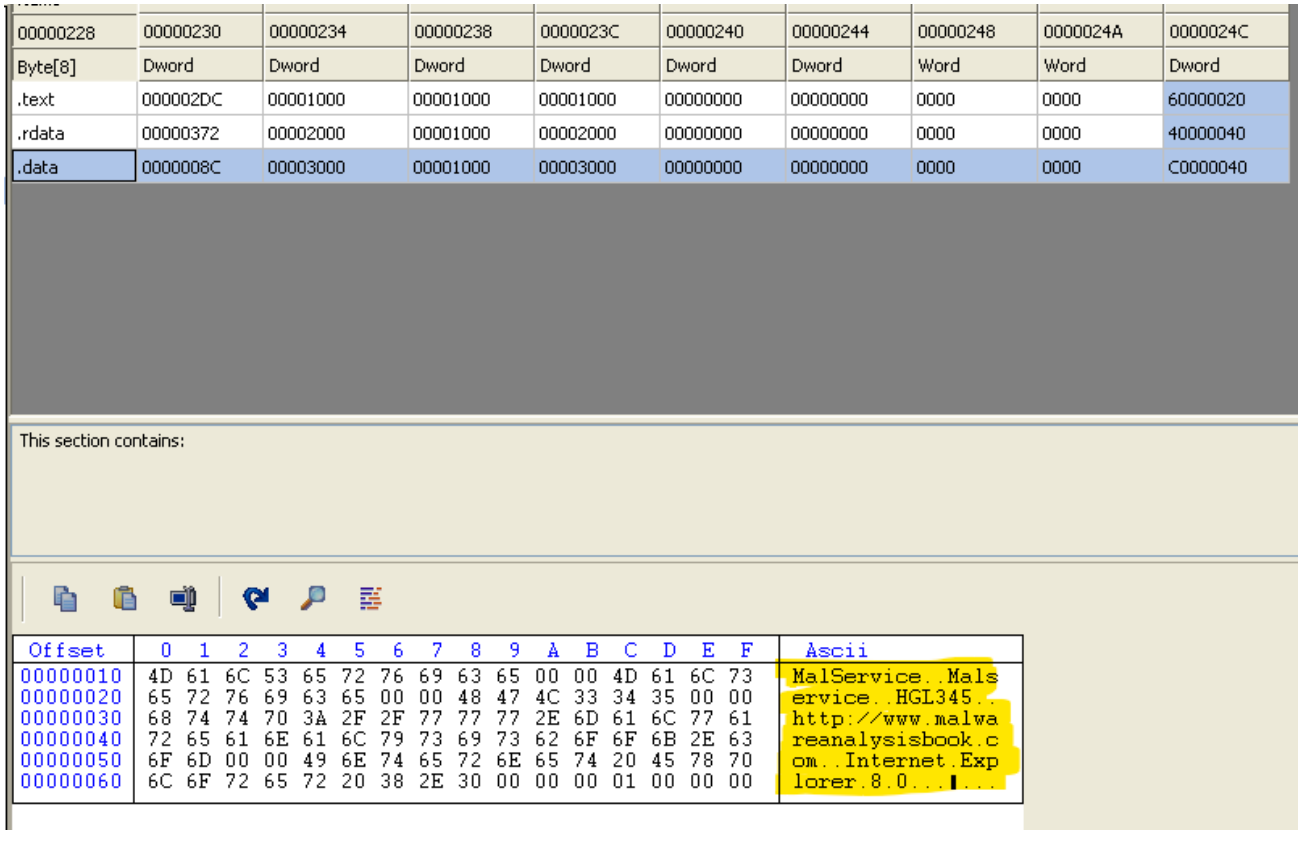
Per scoprire ulteriori informazioni sull'eseguibile si può andare nella sezione "UPX Utility" e selezionare l'opzione "unpack". Dopo aver effettuato questa operazione, tornando su section headers avremo le seguenti informazioni:



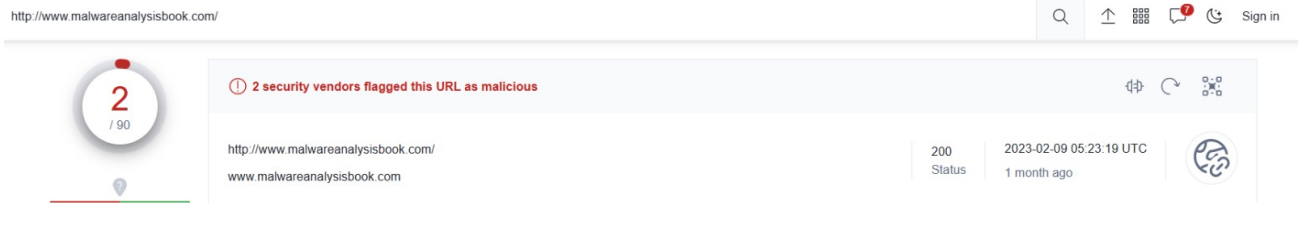
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
000001D8	000001E0	000001E4	000001E8	000001EC	000001F0	000001F4	000001F8	000001FA	000001FC

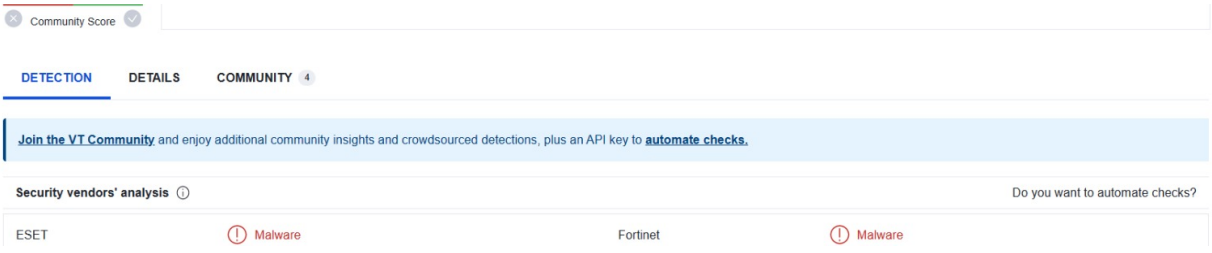


E in questo modo troviamo un link in chiaro che può essere googlato

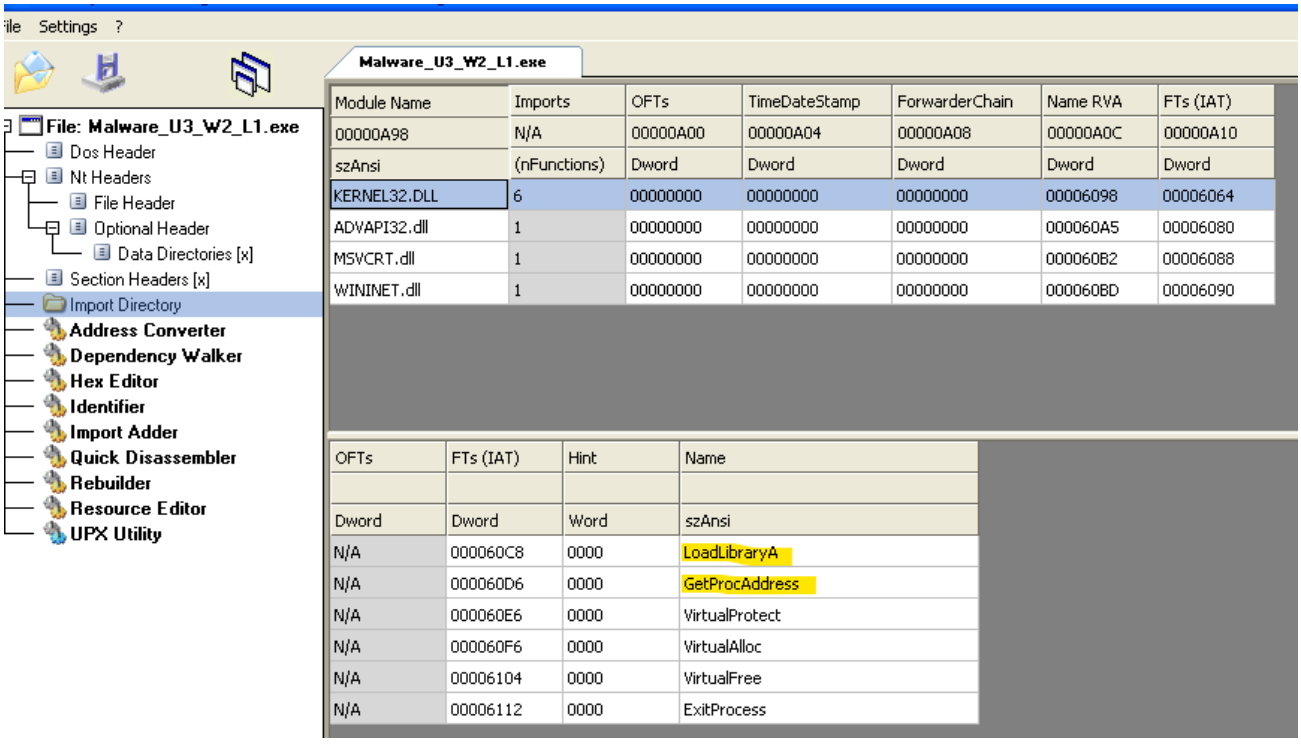


Dal momento in cui non mi fido molto di googlare questo risultato, lo mando in pasto a VirusTotal. 2 Vendors l'hanno idenfiticato come un malware, tuttavia non hanno specificato la tipologia.





In conclusione:



La presenza delle due librarie 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.