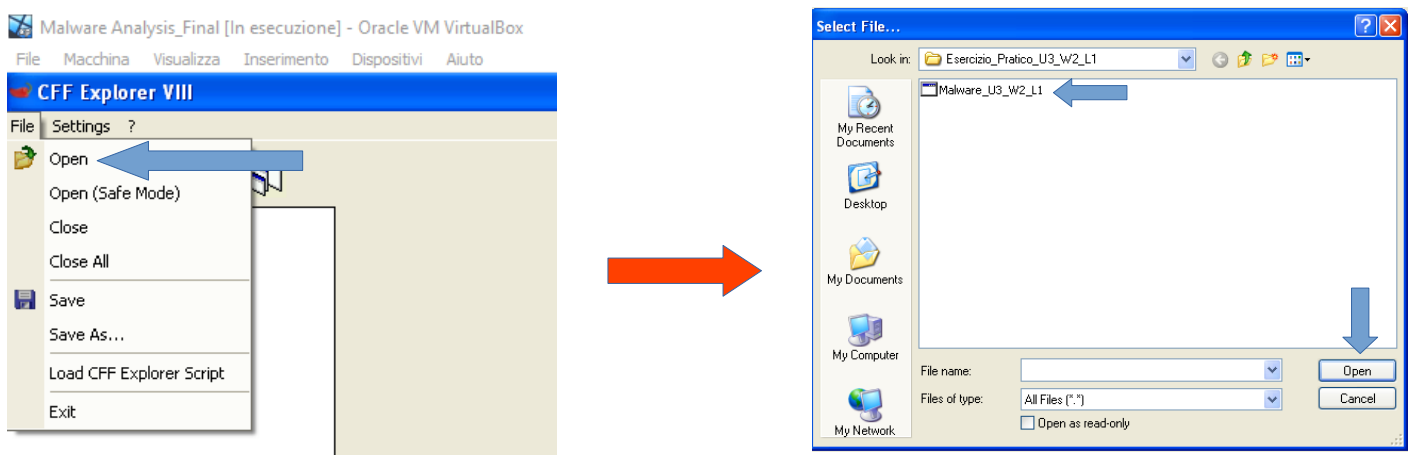


TASK:

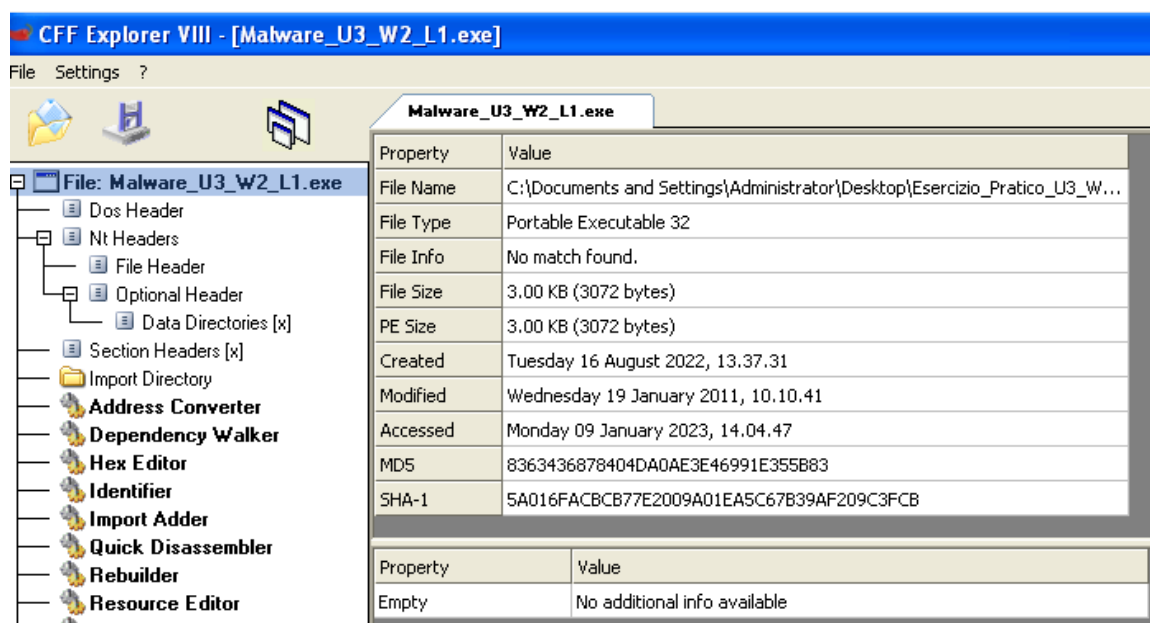
Con riferimento al file eseguibile “Esercizio_Pratico_U2_W2_L1” rispondere ai seguenti quesiti:

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

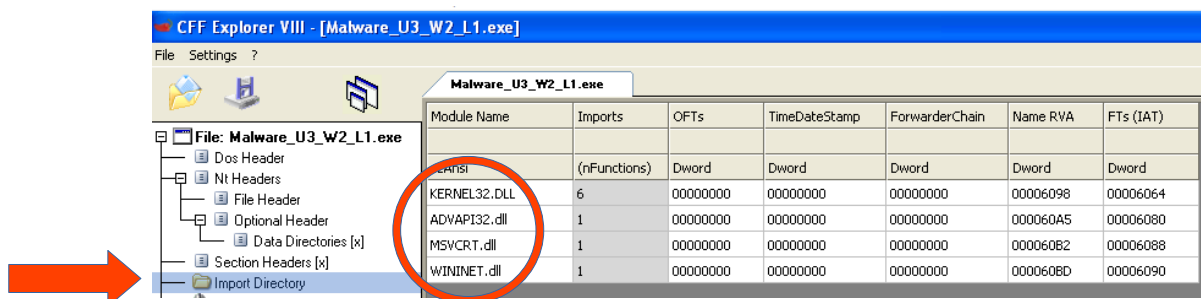
Come prima cosa sono andato ad analizzare il malware tramite il tool CFF Explorer:



La schermata che mi restituisce il programma è la seguente:



A questo punto mi sono spostato sulla sezione Import Directory per vedere le librerie che vengono importate dal malware:



Come possiamo vedere dall'immagine qui sopra vengono importate un totale di 9 funzioni da un totale di 4 librerie che sono:

- **KERNEL32.dll:**
Kernel32.dll è un modulo del kernel di Windows. È una libreria a collegamento dinamico a 32 bit utilizzata nei sistemi operativi Windows. All'avvio del sistema, kernel32.dll viene caricato in una memoria protetta in modo che non venga danneggiato da altri processi di sistema o utente. Funziona come un processo in background e svolge funzioni importanti come la gestione della memoria, operazioni di input/output e interruzioni.
- **ADVAPI32.dll:**
Advapi32.dll è un file DLL (Dynamic Link Library): Memorizza i file importanti moduli di sistema che vengono caricati con i file di sistema eseguibili durante la procedura di avvio. Il file memorizza fondamentalmente moduli per sistemi operativi Windows Servizi avanzati come i file di registro, spegnimento del PC, riavvio del computer, e di lancio, creando o terminano un processo di Windows. Il file dunque, è una componente critica del sistema. Senza questo file, procedura di avvio non verrà completata. Servizi di Windows potranno anche riuscire a lanciare, e altri processi che si basano sui moduli del file sarà anche riuscire a caricare.
- **MSVCRT.dll:**
Il file Msvcrtdll è relativo a Microsoft C Runtime Library. I moduli carica i file per i programmi Visual C e C + +. Microsoft Visual C + + Runtime è parte del software per i sistemi operativi Windows.
- **WININET.dll:**
L'API (Application Programming Interface) di Windows Internet (WinINet) consente all'applicazione di interagire con i protocolli FTP e HTTP per accedere alle risorse Internet.

A questo punto sono andato ad analizzare le sezioni che compongono il malware spostandomi nella “Section Header”:

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
[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	0000A000	00000000	00000000	0000	0000	C0000040

Possiamo vedere come il malware sia composto da 3 sezioni che non sono nominate in chiaro in quanto sono compresse:

- **UPX0:** corrisponde alla sezione “text”, contenente le istruzioni che la CPU eseguirà quando il software verrà avviato.

[illegible]

- UPX1: corrispondente alla sezione “data”, contenente i dati e le variabili globali del programma eseguibile. Esse devono essere disponibili da qualsiasi parte del programma.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii	Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii		
00000000	EF	DD	77	FF	83	EC	10	8D	44	20	C7	03	10	30	40		iyvny1p0d8sC1000	00000370	6F	6C	66	70	B3	0B	42	9C	66	BD	70	53	D4	33	BA	B0	olc1p1B1t8p8038*		
00000001	00	50	08	08	40	10	40	10	B7	DF	9C	DC	0C	00	00	07	PIPIPIPI yeu11	00000380	ED	55	E8	41	11	41	C8	FE	CB	0C	50	45	4C	01	03		10e0A1E0C0EPEL1		
00000002	00	50	08	08	40	10	40	10	B7	DF	9C	DC	0C	00	00	07	PIPIPIPI yeu11	00000390	00	01	0D	37	4D	E0	00	0F	01	08	03	06	03	D9	11		1785 1111111101		
00000003	00	50	08	08	40	10	40	10	B7	DF	9C	DC	0C	00	00	07	PIPIPIPI yeu11	00000400	3F	00	20	13	90	11	00	0F	4D	BE	BC	3C	73	0B	0F	04		1111111111111111	
00000004	00	50	08	08	40	10	40	10	B7	DF	9C	DC	0C	00	00	07	PIPIPIPI yeu11	00000410	00	07	1A	36	08	ED	BD	17	00	55	84	10	07	E5	25	F5		1111111111111111	
00000005	FE	17	AC	5E	10	1F	2C	45	03	08	F6	6D	5F	3E	8B		PI-VII E1111111111	00000420	06	06	41	8C	20	24	D0	50	64	57	7C	36	7B	75	0C		11A1 371111111111		
00000006	FE	17	AC	5E	10	1F	2C	45	03	08	F6	6D	5F	3E	8B		PI-VII E1111111111	00000430	25	34	74	07	DC	02	93	03	D8	C2	A7	6C	42	60	25	72		41111111081911	
00000007	8D	4C	24	2C	05	51	0A	02	6A	10	03	D9	63	EE	68		IL8 111111111111	00000440	64	AE	61	10	72	10	1B	08	93	03	13	F2	32	0F	72		d0e1111111111111		
00000008	1C	45	04	56	3B	00	33	2D	66	B7	EB	BE	14	89	54		IE4V 30f e0e11111	00000450	2A	2E	6F	10	30	27	30	00	5F	7E	53	CD	13	6C	21		e0&110111111111		
00000009	8D	4C	24	2C	05	51	0A	02	6A	10	03	D9	63	EE	68		IE4V 30f e0e11111	00000460	CD	31	00	00	00	00	00	00	00	00	00	00	00	00	00	00		1111111111111111	
0000000A	34	08	50	10	18	CB	AD	66	93	8D	22	20	74	15	52		4FPI1E1111111111	00000470	60	BE	0E	50	40	00	8D	BE	0C	00	FF	F7	57	EB	0B		1111111111111111		
0000000B	54	2B	BB	3F	D6	3F	ED	78	28	67	5B	8D	30	30		V8y70=V11 u=U10	00000480	8A	06	46	88	07	47	01	DB	75	07	08	1E	83	EE	FC		1111111111111111			
0000000C	1C	45	04	56	3B	00	33	2D	66	B7	EB	BE	14	89	54		K4p4e=H4B13u	00000490	DB	02	ED	ED	01	00	00	00	01	DB	75	07	08	1E	83	EE		1111111111111111	
0000000D	8D	4C	24	2C	05	51	0A	02	6A	10	03	D9	63	EE	68		4FPI1E1111111111	000004A0	FC	11	11	11	00	00	00	00	7B	FE	75	09	1B	83	EE	FC		1111111111111111	
0000000E	56	57	BD	B1	CE	F6	E1	68	54	A9	E4	F7	03	90	00		V8H4t1E1111111111	000004B0	11	DB	73	E4	C1	C9	83	ED	03	72	0D	C1	E0	08	8A	06		10a111111111111	
0000000F	7D	6C	6F	73	48	52	60	51	30	C7	D7	EB	9C	05	E7		11s8H4Q0C=ete11	000004C0	46	30	F0	FF	74	89	05	C1	DB	75	07	08	1E	83	EE		10e111111111111		
00000010	00	50	08	08	40	10	40	10	B7	DF	9C	DC	0C	00	00	07	PIPIPIPI yeu11	000004D0	DB	02	ED	ED	01	00	00	00	01	DB	75	07	08	1E	83	EE		1111111111111111	
00000011	3C	64	A1	7C	50	64	89	25	07	4C	20	53	6D	9B	CD		Ad11Pd124C= S-PI	000004E0	11	C9	75	20	41	01	DB	75	07	08	1E	83	EE	FC	11	DB		1111111111111111	
00000012	78	65	EB	83	65	6C	61	5C	60	59	83	0D	00	69	EB		1111111111111111	000004F0	11	C9	01	DB	73	FE	75	09	1B	83	EE	FC	11	DB	73			1111111111111111	
00000013	78	65	EB	83	65	6C	61	5C	60	59	83	0D	00	69	EB		1111111111111111	00000500	E4	83	C1	02	91	FD	0B	F3	FE	F3	D1	01	0D	14	2F		1111111111111111		
00000014	AC	58	0D	78	A1	54	0C	00	A3	88	0E	E6	FE	06	C6		X-x1t1111111111	00000510	83	DF	7C	FE	0A	02	48	02	48	02	49	75	F7	E9	E3		1111111111111111		
00000015	02	8D	33	D	6C	0A	00	00	75	06	68	BE	6C	4F	C1	1E		PI=1 111111111111	00000520	04	FF	7F	08	ED	02	83	C2	04	89	07	83	C7	04	83	E9		1111111111111111
00000016	CE	50	19	48	68	0C	00	28	37	F7	EE	EE	EE	EE	EE		PI=111111111111	00000530	FF	F7	F1	0F	CE	83	4C	FE	FF	FE	89	F7	89	F7	89		1111111111111111		
00000017	00	50	08	08	40	10	40	10	B7	DF	9C	DC	0C	00	00	07	PIPIPIPI yeu11	00000540	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		1111111111111111		
00000018	00	50	08	08	40	10	40	10	B7	DF	9C	DC	0C	00	00	07	PIPIPIPI yeu11	00000550	8B	00	8A	5F	04	2C	00	00	00	00	00	00	00	00	00	00		1111111111111111	
00000019	4D	4D	4D	4D	85	75	ED	02	6D	1B	ED	CB	E4	E4	88		Du11111111111111	00000560	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111		
0000001A	43	43	43	43	85	75	ED	02	6D	1B	ED	CB	E4	E4	88		Du11111111111111	00000570	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111		
0000001B	00	50	08	08	40	10	40	10	B7	DF	9C	DC	0C	00	00	07	PIPIPIPI yeu11	00000580	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111		
0000001C	00	50	08	08	40	10	40	10	B7	DF	9C	DC	0C	00	00	07	PIPIPIPI yeu11	00000590	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111		
0000001D	00	50	08	08	40	10	40	10	B7	DF	9C	DC	0C	00	00	07	PIPIPIPI yeu11	000005A0	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111		
0000001E	2F	64	80	28	32	33	68	00	20	30	30	39	FF	80	7B	94		PI=1 111111111111	000005B0	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111	
0000001F	12	B2	04	41	91	AF	00	29	FF	8F	8A	6D	61	5C	63	65		PI=1 111111111111	000005C0	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111	
00000020	72	76	69	63	65	6E	6F	73	FA	73	48	47	4C	34	34	35		rv11111111111111	000005D0	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111	
00000021	72	76	69	63	65	6E	6F	73	FA	73	48	47	4C	34	34	35		rv11111111111111	000005E0	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111	
00000022	1E	77	61	72	65	61	6E	77	79	73	69	73	62	6F	6F	68		1111111111111111	000005F0	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111	
00000023	2E	63	6F	7D	DB	DF	6D	23	49	6E	74	36	65	65	74		coy001111111111	00000600	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111		
00000024	3C	01	20	01	40	C0	09	65	73	14	15	98	10	10	BF	9D		1111111111111111	00000610	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111	
00000025	6F	6F	51	53	79	73	74	65	6D	54	63	6D	54	64	6E		1111111111111111	00000620	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111		
00000026	6F	6F	51	53	79	73	74	65	6D	54	63	6D	54	64	6E		1111111111111111	00000630	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111		
00000027	12	4E	61	41	13	49	76	67	FD	ED	DF	0F	50	72	6F	63		1111111111111111	00000640	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111	
00000028	61	62	72	7C	12	45	48	78	FD	ED	DF	0F	50	72	6F	63		1111111111111111	00000650	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111	
00000029	65	73	27	0F	74	65	6E	4D	75	24	78	1F	5A	62				00000660	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111		
0000002A	65	73	27	0F	74	65	6E	4D	75	24	78	1F	5A	62				00000670	80	EB	08	01	F0	87	03	E8	08	C1	00	86	C4	29	F8		1111111111111111		
0000002B	65	73																																			

- UPX2: corrispondente alla sezione “rdata” che include generalmente le informazioni riguardanti le librerie e le funzioni importate ed esportate dall’eseguibile.

000005B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000005C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000005D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000005E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000005F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000600	00 00 00 00 00 00 00 00 00 00 00 00 98 60 00 00I`..
00000610	64 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00	d`.....
00000620	A5 60 00 00 80 60 00 00 00 00 00 00 00 00 00 00	#`.....
00000630	00 00 00 00 B2 60 00 00 88 60 00 00 00 00 00 002`..
00000640	00 00 00 00 00 00 00 00 BD 60 00 00 90 60 00 00k`..
00000650	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000660	00 00 00 00 C8 60 00 00 D6 60 00 00 E6 60 00 00E`O`æ`..
00000670	F6 60 00 00 04 61 00 00 12 61 00 00 00 00 00 00	ö`..la`la`....
00000680	20 61 00 00 00 00 00 00 30 61 00 00 00 00 00 00	a`.....0a`....
00000690	36 61 00 00 00 00 00 00 4B 45 52 4E 45 4C 33 32	6a`.....KERNEL32
000006A0	2E 44 4C 4C 00 41 44 56 41 50 49 33 32 2E 64 6C	.DLL.ADVAPI32.dll
000006B0	6C 00 4D 53 56 43 52 54 2E 64 6C 6C 00 57 49 4E	l.MSVCRT.dll.WIN
000006C0	49 4E 45 54 2E 64 6C 6C 00 00 4C 6F 61 64 4C 69	INET.dll..LoadLi
000006D0	62 72 61 72 79 41 00 00 47 65 74 50 72 6F 63 41	braryA..GetProcAddress
Offset	0 1 2 3 4 5 6 7 8 9 A B C D E F	Ascii
000006E0	64 64 72 65 73 73 00 00 56 69 72 74 75 61 6C 50	ddress..VirtualP
000006F0	72 6F 74 65 63 74 00 00 56 69 72 74 75 61 6C 41	rotect..VirtualA
00000700	6C 6C 6F 63 00 00 56 69 72 74 75 61 6C 46 72 65	lloc..VirtualFre
00000710	65 00 00 00 45 78 69 74 50 72 6F 63 65 73 73 00	e...ExitProcess.
00000720	00 00 43 72 65 61 74 65 53 65 72 76 69 63 65 41	..CreateServiceA
00000730	00 00 65 78 69 74 00 00 49 6E 74 65 72 6E 65 74	..exit..Internet
00000740	4F 70 65 6E 41 00 00 00 00 00 00 00 00 00 00 00	OpenA.....

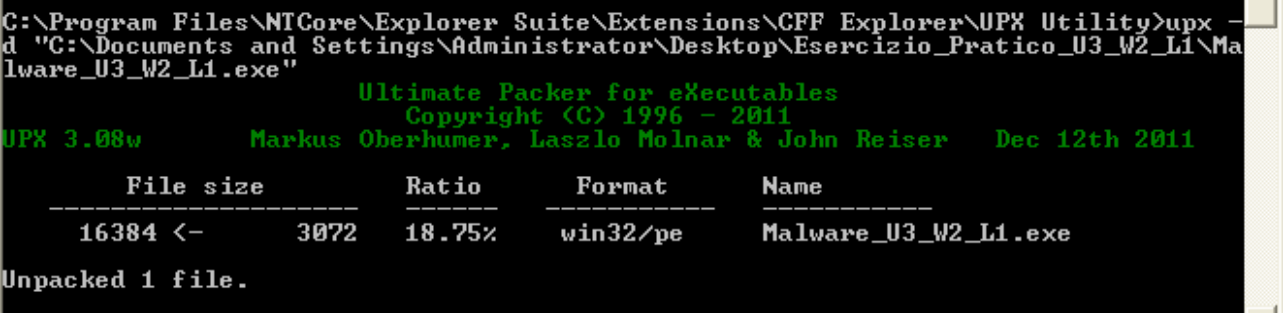
Possiamo vedere quindi dalle librerie e dalle rispettive funzioni che il programma mette in comunicazione la macchina vittima con un indirizzo url specifico tramite il servizio http. Sono andato anche ad utilizzare l’utility strings per avere una visione a schermo più chiara di quanto contenuto nel programma:

```
C:\Documents and Settings\Administrator\Desktop\SysinternalsSuite>strings "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_U2_L1\Malware_U3_U2_L1.exe"

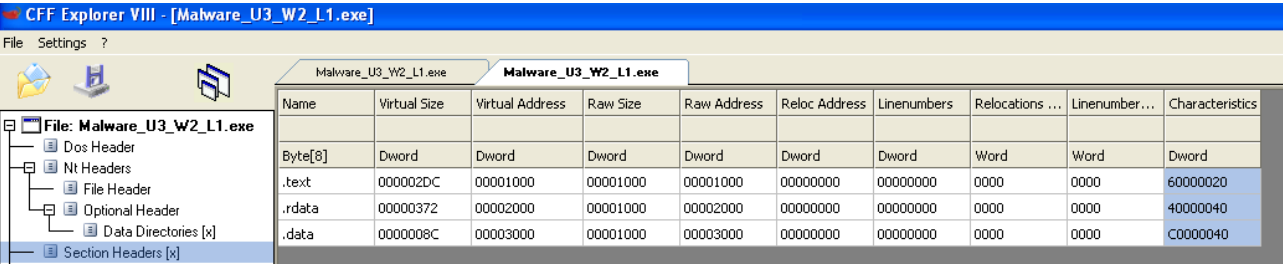
Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com
```

```
Sysinternals - www.sysinternals.com
!This program cannot be run in DOS mode.
Rich
UPX0
UPX1
UPX2
3.04
UPX3
013
h<0
L5
G11
G z
RU5
u+w
.hb
t-p
sHR
lpd
s
a\y
tQE
DmM
t9I
PQ6
<23h
MalService
shG145
http://u
warean
ysisbook.co
ondInt6net Explotr 8FEI
0C
SystemTimeToFile
GetMo
MaH
Cov
*Waitab'r
Process
Openhu$x
ZSB+
ForS
Ing
ObjectU4
(U+tb
CtrlDisp ch
SGM
G_e
Xcpt
mArg
sus
SnnG_
K.Fd
i9H
mKe
P.p
vty
dll37n
oIfp
DEL
dW16
.4t
1B.rd
Q.4
0'0
L~S
u n
G1u
PTj
```

Sono andato a spaccettare l’e eseguibile da terminale con il comando “upx -d” :



A questo punto sono andato ad analizzare nuovamente il programma con CFF Explorer e ho notato che le funzioni invocate dal programma sono aumentate rispetto a prima:



Andando ad effettuare un’analisi con virustotal.com riusciamo ad ottenere maggiori informazioni riguardo all’azione di questo malware, che scopriamo essere un trojan:

Activity Summary

Network Communication ⓘ

DNS Resolutions

+ 106.89.54.20 in-addr.arpa

+ 125.21.88.13 in-addr.arpa

+ 154.210.82.20 in-addr.arpa

+ 183.209.82.20 in-addr.arpa

+ 2.155.190.20 in-addr.arpa

+ 212.161.61.168 in-addr.arpa

+ 234.151.42.104 in-addr.arpa

+ 234.173.86.20 in-addr.arpa

+ 25.140.123.92 in-addr.arpa

+ 254.11.238.8 in-addr.arpa

IP Traffic

104.86.182.50.443 (TCP)

104.96.203.51.443 (TCP)

104.99.239.138.443 (TCP)

13.107.39.203.80 (TCP)

13.107.4.50.80 (TCP)

13.224.247.21.443 (TCP)

131.253.33.203.80 (TCP)

192.168.0.160.137 (UDP)

192.168.0.16.137 (UDP)

192.168.0.1.137 (UDP)

TLS

+ firefox.settings.services.mozilla.com

+ incoming.telemetry.mozilla.org

File system actions ⓘ

Files Dropped

+ %USERPROFILE%\AppData\Local\Microsoft\Windows\WER\ER\statecache.lock

+ C:\ProgramData\Microsoft\Windows\WER\Temp\WER1038.tmp

+ C:\ProgramData\Microsoft\Windows\WER\Temp\WER1038.tmp.txt

+ C:\ProgramData\Microsoft\Windows\WER\Temp\WER104.tmp

+ C:\ProgramData\Microsoft\Windows\WER\Temp\WER104.tmp.csv

+ C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp

+ C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C2.tmp.WERInternalMetadata.xml

+ C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C3.tmp

+ C:\ProgramData\Microsoft\Windows\WER\Temp\WER13C3.tmp.csv

+ C:\ProgramData\Microsoft\Windows\WER\Temp\WER13D4.tmp

Registry actions ⓘ

Registry Keys Set

+ HKEY_CURRENT_USER\Software\Mozilla\Firefox\Default Browser Agent\CurrentDefault

+ HKEY_CURRENT_USER\Software\Mozilla\Firefox\Default Browser Agent\LastPingSentAt

+ HKEY_CURRENT_USER\Software\Mozilla\Firefox\Default Browser Agent\PingCurrentDefault

+ HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\IS-1-5-21-1015118539-3749460369-599379286-1001\{529D8869-582B-4DB2-A56A-3875E5137D81}\From

+ HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\IS-1-5-21-1015118539-3749460369-599379286-1001\{529D8869-582B-4DB2-A56A-3875E5137D81}\Count

+ HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\IS-1-5-21-1015118539-3749460369-599379286-1001\{529D8869-582B-4DB2-A56A-3875E5137D81}\From

+ HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\IS-1-5-21-1015118539-3749460369-599379286-1001\{529D8869-582B-4DB2-A56A-3875E5137D81}\Version

+ HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\IS-1-5-21-1015118539-3749460369-599379286-1001\{8A520402-FAC8-401E-A3A7-77CF9D1A36FC}\Count

+ HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\IS-1-5-21-1015118539-3749460369-599379286-1001\{8A520402-FAC8-401E-A3A7-77CF9D1A36FC}\Count

+ HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\IS-1-5-21-1015118539-3749460369-599379286-1001\{8A520402-FAC8-401E-A3A7-77CF9D1A36FC}\From

Process and service actions ⓘ

Processes Tree

2176 - %windir%\System32\svchost.exe -k WerSvcGroup

2536 - ***.exe

2624 - %SAMPLEPATH%

2692 - %CONHOST% ^-1414162336-142852711499919660223427-18418218118705862841171643310-1687846403

2980 - %WINDIR%\explorer.exe

2992 - wmiadap.exe /F /T /R

3040 - %windir%\system32\wbem\wmiiprvse.exe

↳ 3340 - %SAMPLEPATH%\file.exe

↳ 3672 - C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0x00000000 -ForceV1

4048 - 'C:\Users\user\Desktop\file.exe'

↳ 5832 - 'C:\Program Files (x86)\Mozilla Firefox\pingsender.exe' https://incoming.telemetry.mozilla.org/submit/default-browser-agent/default-browser/1E2DC2A4-42FA-4C6A-8D62-EDB05F6CD5CA 'C:\Users\user\AppData\Roaming\Mozilla\Firefox\Pending Pings\E2DC2A4-42FA-4C6A-8D62-EDB05F6CD5CA'

↳ 6548 - C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0x00000000 -ForceV1

7004 - 'C:\Program Files (x86)\Mozilla Firefox\default-browser-agent.exe' do-task 'E7CF176E110C211B'