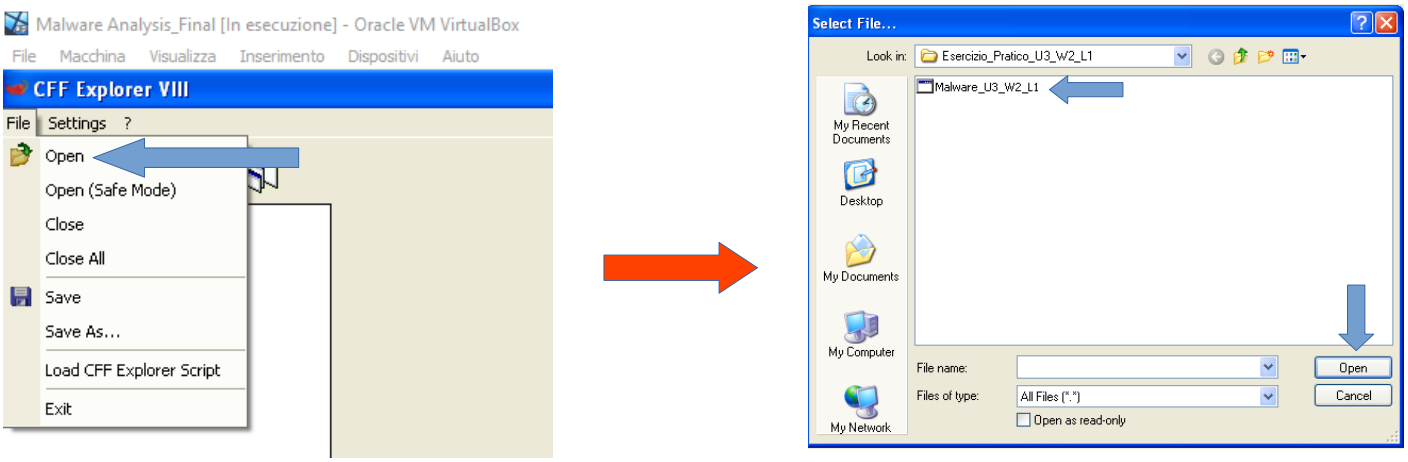
REPORT 09/01/2023 LORENZO SCORBAIOLI

TASK:

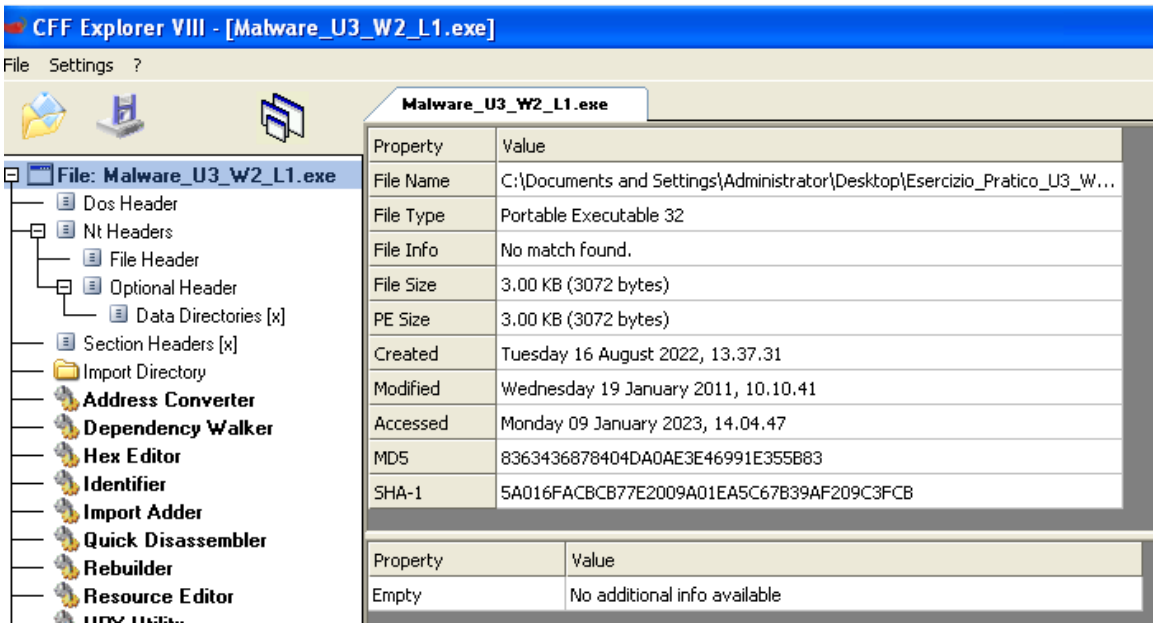
Con riferimento al file eseguibile “Esercizio_Pratico_U2_W2_L1” rispondere ai seguenti quesiti:

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

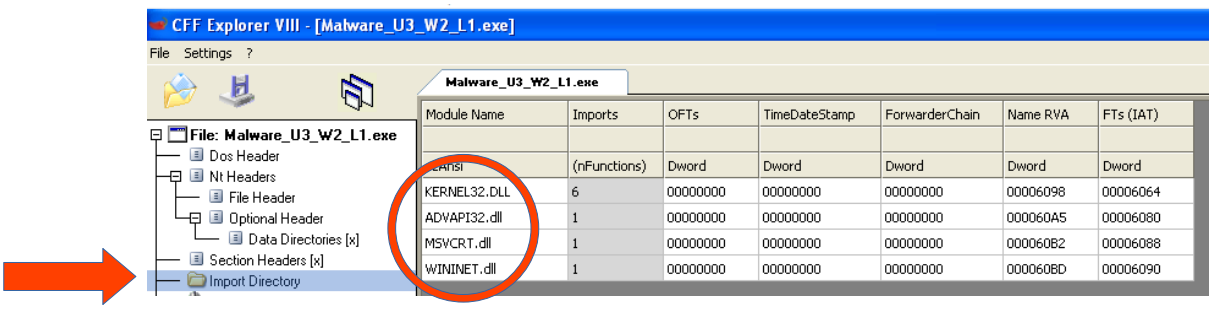
Come prima cosa sono andato ad analizzare il malware tramite il tool CFF Explorer:



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:

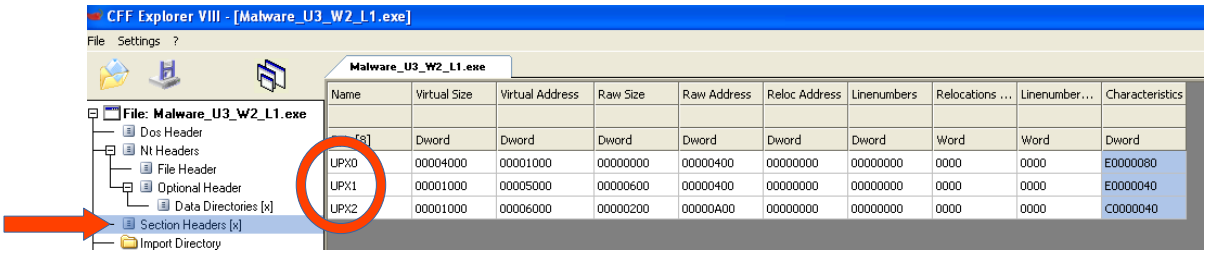
- KERNEL32.dll:
  Kernel32.dll è un modulo del kernel di Windows. È una libreria a collegamento dinamico a 32 bit utilizzata nei sistemi operativi Windows. All'avvio del sistema, kernel32.dll viene caricato in una memoria protetta in modo che non venga danneggiato da altri processi di sistema o utente. 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 Msvcrt.dll 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.

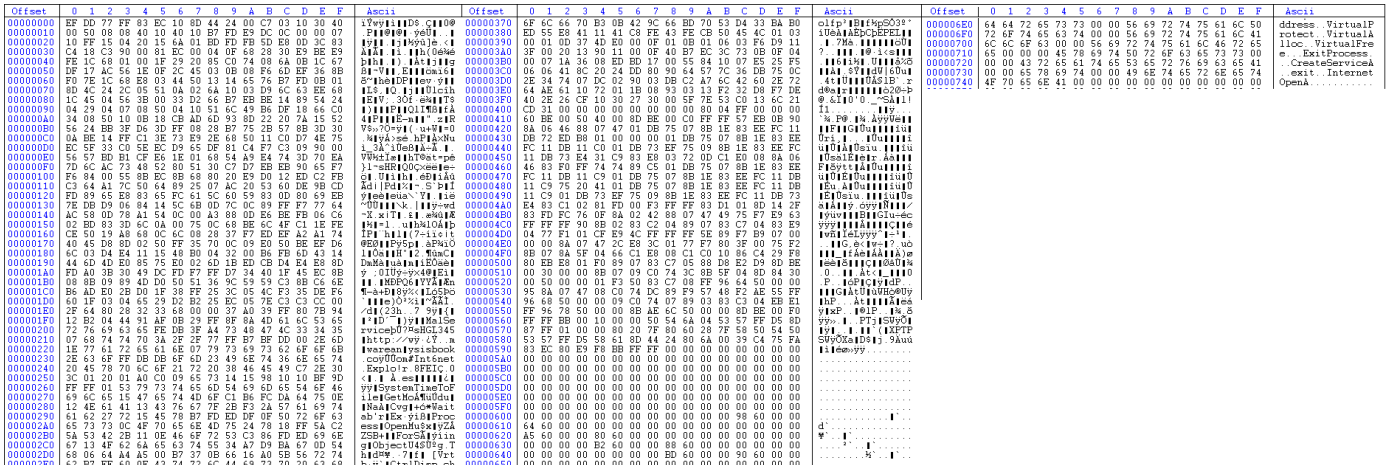
- WININET.dll:
  L'API (Application Programming Interface) di Windows Internet (WinINet) consente all'applicazione di interagire con i protocolli FTP e HTTP per accedere alle risorse Internet.

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

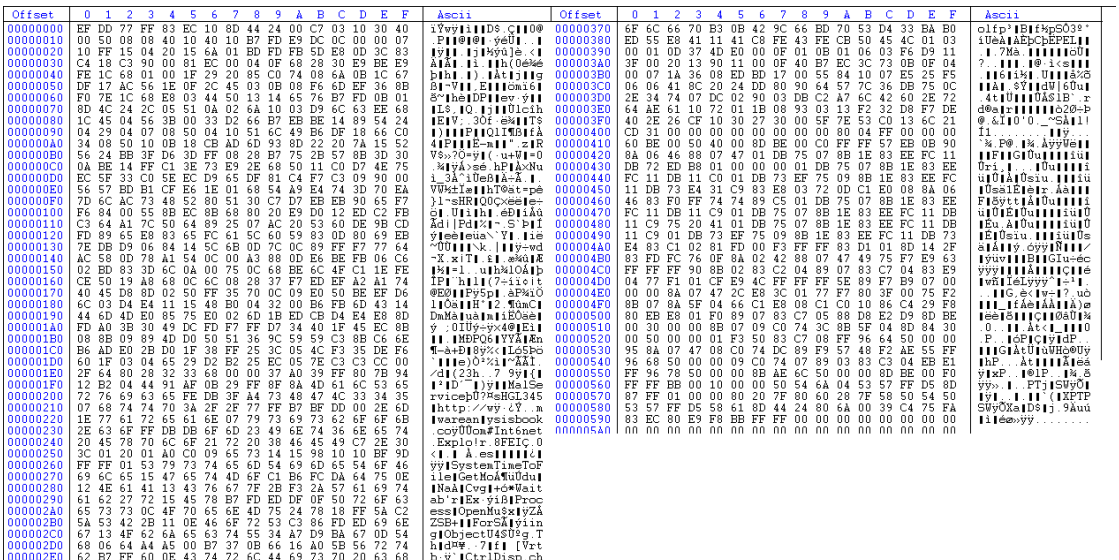


Possiamo vedere come il malware sia composto da 3 sezioni che non sono nominate in chiaro in quanto sono compresse:

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



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



- 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 00 .............`..
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 00 ....²`..ˆ`......
00000640 00 00 00 00 00 00 00 00 BD 60 00 00 90 60 00 00 ........½`..`..
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 00 ....È`..Ö`..æ`..
00000670 F6 60 00 00 04 61 00 00 12 61 00 00 00 00 00 00 ö`...a...a......
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.dl
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..GetProcA
 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...........
```

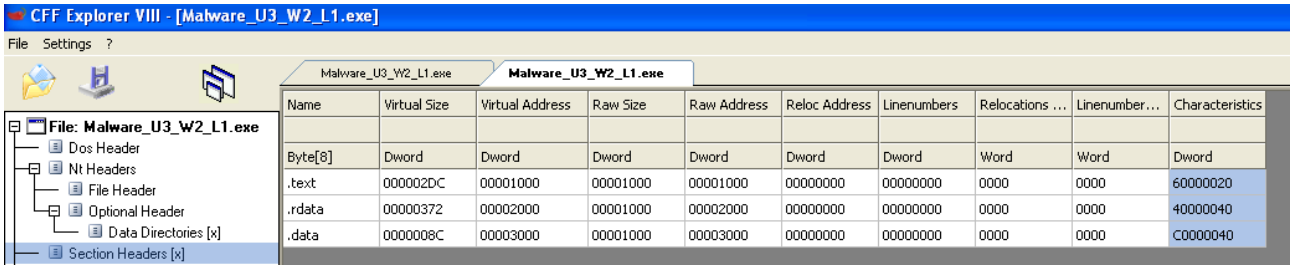
Possiamo vedere quindi dalle librerie e dalle rispettive funzioni che il programma mette in comunicazione la macchina vittima con un indirizzo url specifico tramite il servizio http. Sono andato anche ad utilizzare l’utility strings per avere una visione a schermo più chiara di quanto contenuto nel programma:

```
C:\Documents and Settings\Administrator\Desktop\SysinternalsSuite>strings "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_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
UPX!
A13
hx@
L$,
QlI
" z
RU$
u+W
.hP
t=p
sHR
!Pd
 S`
a\`Y
t@E
DnM
;0I
PQ6
<23h
MalService
sHGL345
http://w
warean
ysisbook.co
om#Int6net Explo!r 8FEI
.0(
SystemTimeToFile
GetMo
NaA
Cvg
=Waitab'r
Process
OpenMu$x
ZSB+
For$
ing
ObjectU4
[Usth
CtrlDisp ch
SCM
8_e
Xcpt
mArg
sus
5nm@_
c_fd
i9H
m<e
9,p
vty
dll37n
olfp
PEL
dW!6
.4t
lB`.rd
@.&
0'0
_^S
u A
Glu
PIj
```

Sono andato a spacchettare l’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:



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

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