

Librerie importate dal Malware

The screenshot shows the CFF Explorer VIII interface. The title bar reads "CFF Explorer VIII - [Malware_U3_W2_L1.exe]". The menu bar includes "File", "Settings", and "?". The left pane displays a tree view of the file structure for "File: Malware_U3_W2_L1.exe", with nodes for Dos Header, Nt Headers, File Header, Optional Header, Data Directories [x], Section Headers [x], Import Directory, and Address Converter. The right pane is titled "Malware_U3_W2_L1.exe" and contains a table with the following data:

Module Name	Imports	OFTs
szAnsi	(nFunctions)	Dword
KERNEL32.DLL	6	00000000
ADVAPI32.dll	1	00000000
MSVCRT.dll	1	00000000
WININET.dll	1	00000000

Possiamo notare come il malware analizzato importi 6 funzioni di kernel32.dll, quindi possiamo immaginare che manipoli i file e le cartelle, poi vediamo la advapi32, quindi interagisce con i registri di windows, poi la msvcrt che sappiamo serve per chiamate i/o e allocazione memoria, in ultimo la wininet, quindi sappiamo che probabilmente fa richieste su internet o invia dati.

Analisi sezioni

The screenshot shows the CFF Explorer VIII interface. The title bar reads "CFF Explorer VIII - [Malware_U3_W2_L1.exe]". The menu bar includes "File", "Settings", and "?". The left pane displays a tree view of the file structure for "File: Malware_U3_W2_L1.exe", with nodes for Dos Header, Nt Headers, File Header, Optional Header, Data Directories [x], Section Headers [x], and Import Directory. The right pane is titled "Malware_U3_W2_L1.exe" and contains a table with the following data:

Name	Virtual Size	Virtual Address
Byte[8]	Dword	Dword
UPX0	00004000	00001000
UPX1	00001000	00005000
UPX2	00001000	00006000

Sono funzioni di compressione, proviamo quindi a usare l'utilità interna di CFF per decomprimere

The screenshot shows the UPX settings dialog box. It has several sections: "Check if the Portable Executable is already packed" (unchecked), "UPX" (with "Pack Export Directory" checked, "Compression Level: 7" dropdown set to 7, "Force", "Exact", and "All Methods" checkboxes unchecked, and "Strip Relocation Directory" checked), "Ultimate Packer for eXecutables Copyright (C) 1996 - 2011 Markus Oberhumer, Laszlo Molnar & John Reiser Dec 12th 2011", "File size Ratio Format Name -----upx: C:\DOCUMENTI\ADMINISTRATOR\LOCALS\Temp\upx4.tmp: NotPackedException: not packed by UPX", and "Unpacked 0 files."

In questo modo possiamo vedere in chiaro alcune stringhe nel Hex editor

The screenshot shows a hex editor window with the title "ASCII". On the left, there is a vertical scroll bar. The main area displays several ASCII strings:

```
.....KERN  
EL32.DLL.ADVAPI3  
2.dll.MSWCRT.dll  
.WININET.dll...  
SystemTimeToFile  
Time..GetModuleF  
ileNameA..Create  
WaitableTimerA..  
ExitProcess...Op  
enMutexA..SetWai  
tableTimer..Wait  
ForSingleObject.  
..CreateMutexA..  
CreateThread..Cr  
eateServiceA..St  
artServiceCtrlDi  
spatcherA..Open  
SCManagerA.._exi  
t..._XcptFilter.  
..exit..__p_in  
itenv...__getmai  
nargs..._initter  
m...__setusermat  
herr..._adjust_fd  
iv...__p_commode  
..__p_fmode..__  
set_app_type.._e  
xcept_handler3..  
_controlfp..Inte  
rnetOpenUrlA..In  
ternetOpenA....  
.....
```

Qui possiamo notare invece una serie di stringhe, probabilmente i nomi delle funzioni richiamate

The screenshot shows a hex editor window with the title "ASCII". On the left, there is a vertical scroll bar. The main area displays several ASCII strings:

```
.....MalService..Mals  
ervice..HGL345..  
http://www.malwa  
reanalysisbook.c  
om..Internet.Exp  
lorer.8.0...|....  
.....
```



Qui per esempio vediamo un link in chiaro

The screenshot shows the CFF Explorer VIII interface with the title "CFF Explorer VIII - [Malware_U3_W2_L1.exe]". The menu bar includes "File", "Settings", and "?". The toolbar has icons for file operations. The left pane shows a tree view of the file structure:

- File: Malware_U3_W2_L1.exe
 - Dos Header
 - Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
 - Section Headers [x]

The right pane displays the "Malware_U3_W2_L1.exe" section headers table:

Name	Virtual Size	Virtual Addr
Byte[8]	Dword	Dword
.text	000002DC	00001000
.rdata	00000372	00002000
.data	0000008C	00003000

Inoltre possiamo notare che ora i nomi delle funzioni sono cambiati

Considerazioni

Con una ricerca su google troviamo un github che spiega il funzionamento di questo malware
<https://github.com/SafeEval/practical-malware-analysis/blob/master/exercises/lab-07-1.md>

5) Purpose of the program?

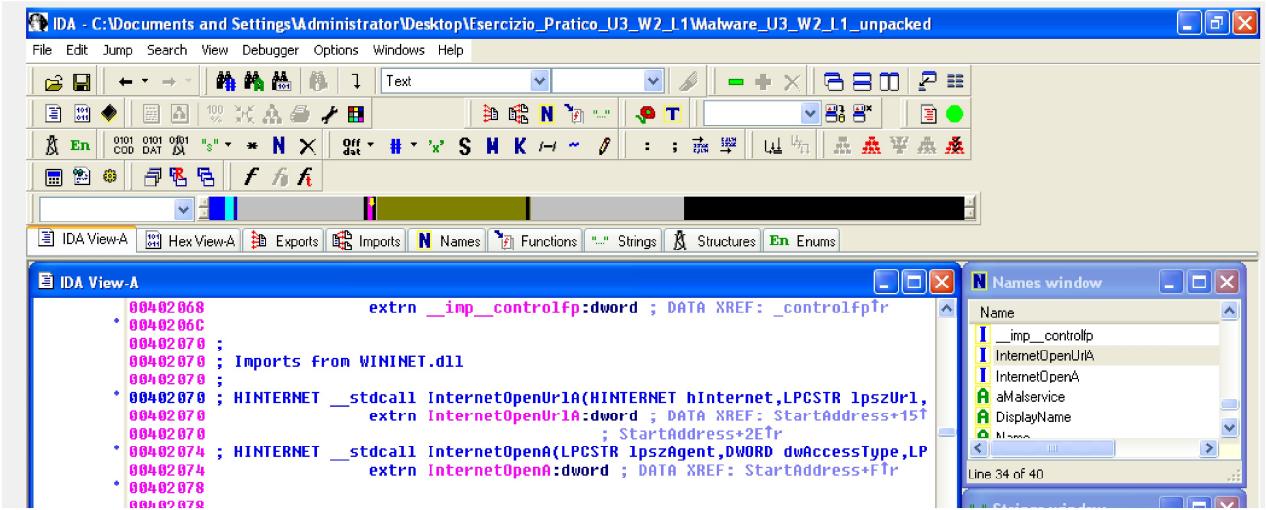
Installs a DDoS service with 20 threads attacks <http://www.malwareanalysisbook.com> in the year 2100.

Connects to <http://www.malwareanalysisbook.com> in infinite loop. Leaves a mutex open to let other instances know it's running.

Program starts a service dispatcher, allowing `malservice` to execute in this process. Calls `ServiceMain`.

Questo è quello che fa il malware.

Grazie a IDA possiamo vedere meglio le funzioni



Per esempio internet url open conferma quello che avevamo trovato prima.