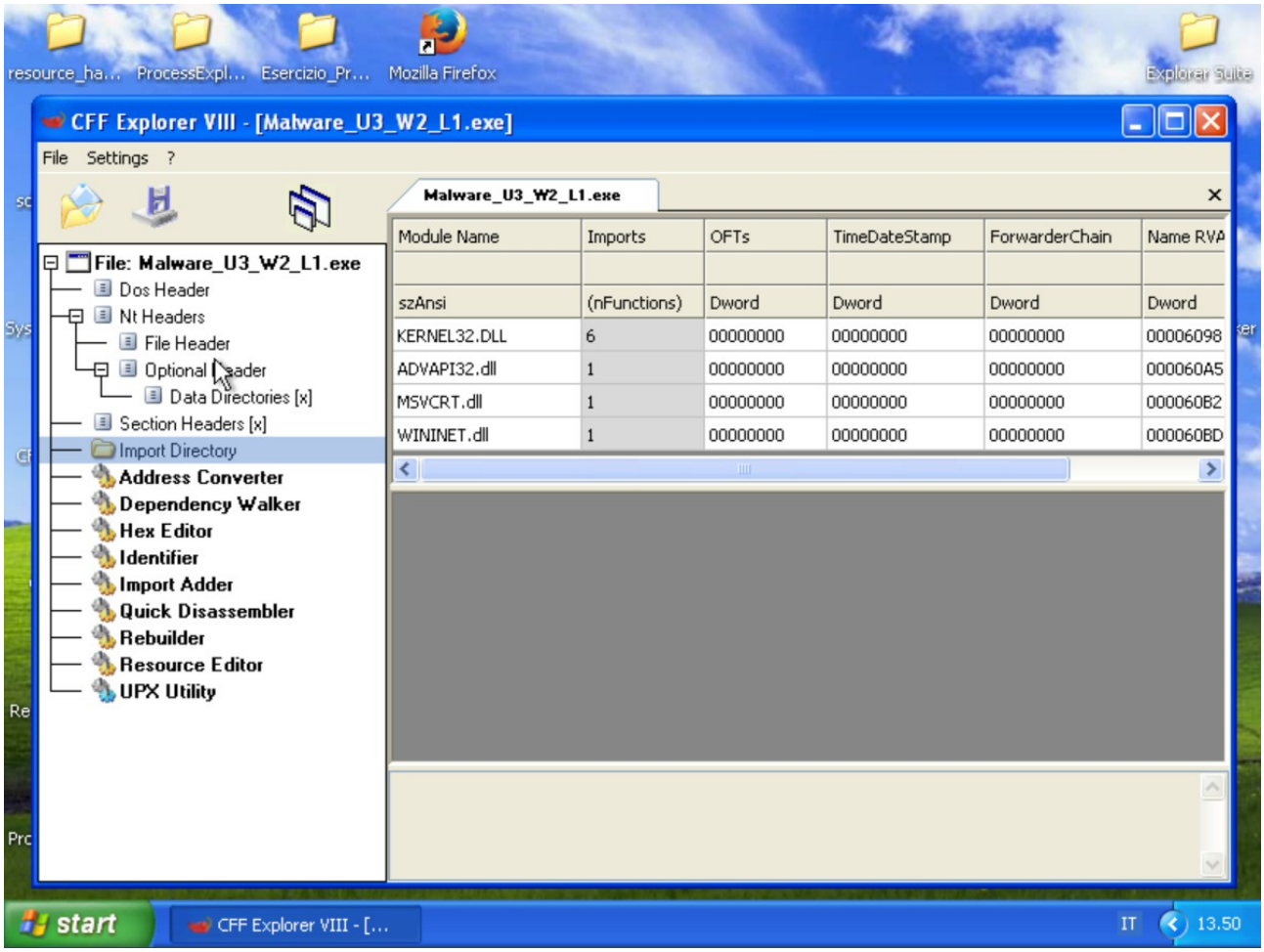
Pratica S10L1

Utilizzando il programma CFF Explorer, andiamo a vedere quali librerie utilizza il malware presente nell'esercizio andando ad effettuare un'analisi statica, ossia senza eseguire il codice del malware. Apriamo quindi il malware con CFF:



Spostandoci sulla import directory possiamo vedere quali librerie, ossia insieme di funzioni, di windows vengono importate prima dell'esecuzione del codice. Tramite queste informazioni possiamo fare delle ipotesi sul funzionamento del programma. Vediamo una per una:

Kernel32.dll

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

Questa è la libreria fondamentale di windows per gestire la memoria, i processi e le funzioni di

sistema. Ha anche accesso all'orario del sistema

Advapi32.dll

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006120	0000	CreateServiceA

Questa libreria invece è utilizzata per la creazione degli utenti, la gestione del registro di sistema e la gestione dei log

msvcrt.dll

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006130	0000	exit

Questa libreria è fondamentale per la gestione dei programmi che vengono compilati tramite Microsoft Visual C++ e poi eseguiti su windows. Contiene funzioni per la gestione dell I/O, dei file e della memoria nelle suddette applicazioni

Wininet.dll

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006136	0000	InternetOpenA

Questa libreria è usata per il controllo delle connessioni internet e dei protocolli di rete

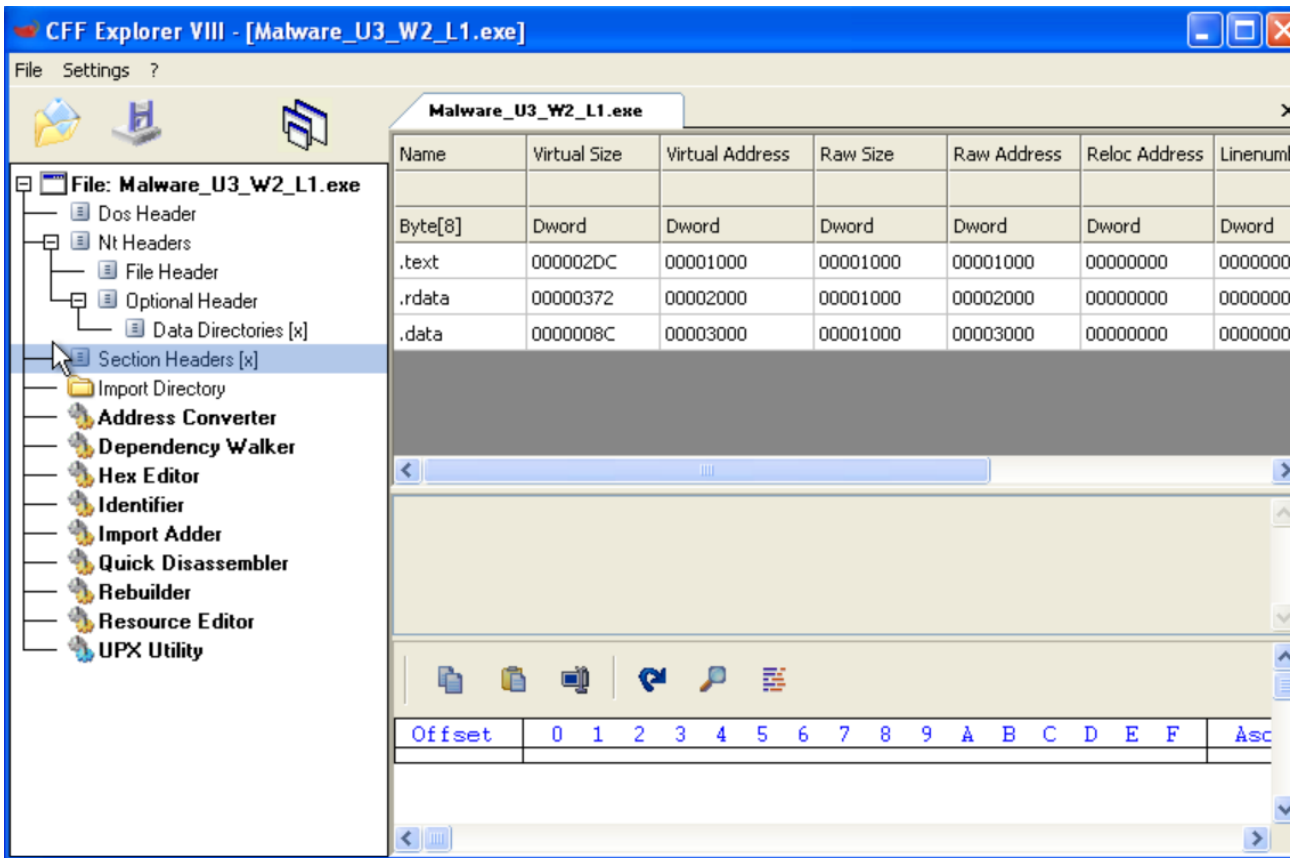
Controllo dell'header

Da un primo tentativo di apertura con CFF non sono riuscito a ricavare il nome delle sezioni. Dopo qualche ricerca ho installato l'utility UPX per windows che mi ha permesso di decomprimere il malware ed andarlo ad analizzare nuovamente:

```
C:\Documents and Settings\Epicode_user\Documenti\Download\upx304w\upx304w>upx -d
 "C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratico_U3_W2_L1\Malw
are_U3_W2_L1.exe"
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2009
UPX 3.04w       Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 27th 2009

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     16384 <-      3072   18.75%    win32/pe     Malware_U3_W2_L1.exe

Unpacked 1 file.
```



Come da immagine sopra vediamo che l'header del malware si compone di tre sezioni:

.text E' la parte di codice che verrà eseguita dalla CPU
.rdata E' la parte che contiene le informazioni sulle librerie importate
.data contiene le variabili globali sul quale il codice andrà ad agire

Possiamo quindi concludere che il malware in questione potrebbe potenzialmente essere molto pericoloso se eseguito, dato che richiama codice dalle librerie più importanti del sistema e potrebbe quindi avere accesso ai file della macchina, gestirne la memoria, avere accesso ai dati sugli utenti e una volta eseguito il codice potrebbe anche andare ad inviare tutte le informazioni raccolte ad un potenziale attaccante, facendo uso delle librerie di rete.