

# Esercizio 1 Settimana 10

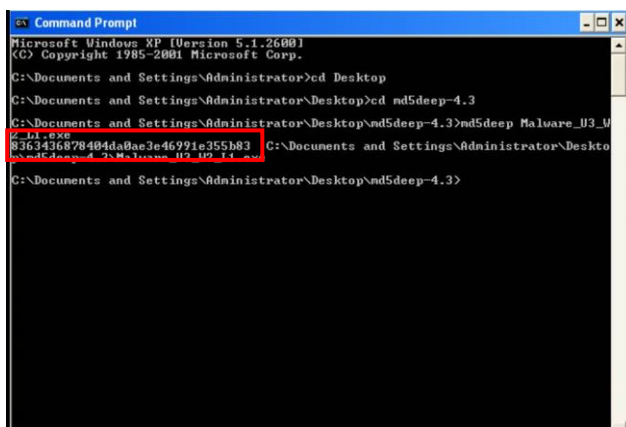
## Analisi Statica

Nella teoria abbiamo visto come andare ad analizzare e studiare un Malware per poterne predire il comportamento e, in seguito, rimuoverlo. Per fare ciò abbiamo a disposizione una vasta gamma di tools e risorse online: noi andremo ad utilizzare VirusTotal e CFF Explorer.

L'approccio da utilizzare sarà un'analisi basica statica per analizzare un Malware ad hoc senza bisogno di eseguirlo, agendo quindi in ambiente sicuro.

### VIRUS TOTAL

Iniziamo con l'utilizzare il tool web VirusTotal per avere informazioni dettagliate sul programma. Vista la possibilità di caricare direttamente il codice Hash del programma malevolo, usiamo 'md5deep' sulla nostra macchina virtuale per poter creare il codice che ci serve, per poi andarlo ad inserire sul sito.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>cd Desktop
C:\Documents and Settings\Administrator\Desktop>cd md5deep-4.3
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>md5deep Malware_U3_W2_11.exe
8363436878404da0ae3e46991e355b83  C:\Documents and Settings\Administrator\Desktop\md5deep-4.3\Malware_U3_W2_11.exe
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>
```

c876a332fd7d8fda331cb8ee07ab75f32752834d4b2b54eaa3626742a48ff6a

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
UPX0	4096	16384	0	0	d41d8cd9f800b204e9800998ecf8427e	-1
UPX1	20480	4096	1536	7.07	ad0f236c2b347f031486c8cc4803a908	5848.3
UPX2	24576	4096	512	2.8	f998d25f473e96cc89cf43af302bee9	53922

Imports

— ADVAPI32.dll

CreateServiceA

— KERNEL32.DLL

ExitProcess

GetProcAddress

LoadLibraryA

VirtualAlloc

VirtualFree

VirtualProtect

— MSVCRT.dll

exit

— WINNET.dll

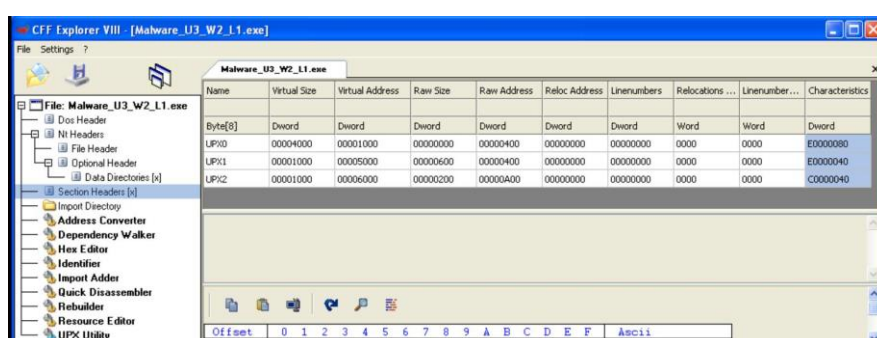
InternetOpenA

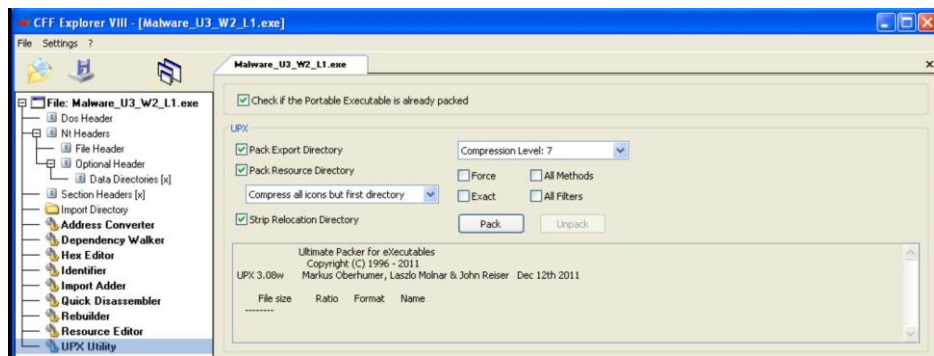
Da qui abbiamo accesso ad una grande varietà di informazioni tra cui anche la tipologia di Malware, sezioni, librerie incorporate etc.

Il problema giunge nella parte delle sezioni poiché quest'ultime non sono in chiaro, ma "oscurate" dal software "packer UPX" per nascondere la presenza e rendere il Malware difficilmente riconoscibile.

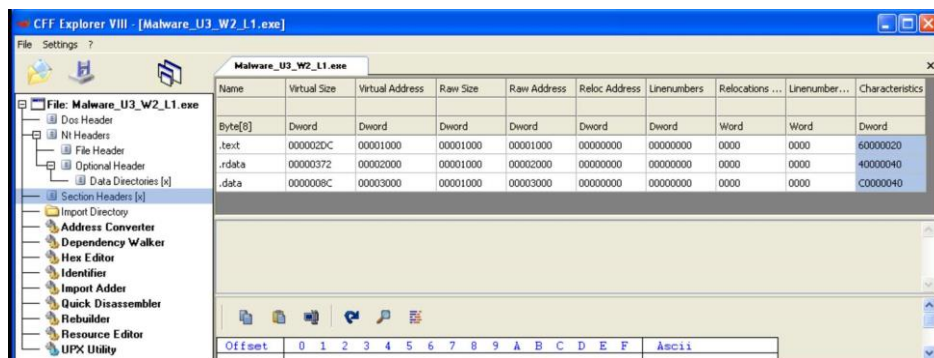
### CFF Explorer

A questo punto utilizziamo il tool CFF Explorer. Il programma comprende un UPX Utility che va a spaccettare le estensioni UPX e ci fornisce in chiaro le sezioni di cui abbiamo bisogno:





Unpack UPX



Sezioni in chiaro

Le sezioni hanno un preciso scopo e conoscere quelle trovate è un grosso aiuto nell'analisi:

- **.text:** contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto;
- **.rdata:** include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer;
- **.data:** contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

Le librerie, invece, contengono un insieme di funzioni e quando un programma ha bisogno di una funzione «chiama» una libreria al cui interno è definita la funzione necessaria. Nel nostro Malware troviamo:

- **Kernel32.dll:** contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria;
- **Advapi32.dll:** contiene le funzioni per interagire con i servizi ed i registri del sistema operativo;
- **Wininet.dll:** contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP;
- **MSVCRT.dll:** contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C.

## CONSIDERAZIONI FINALI

Grazie a VirusTotal possiamo considerare il programma analizzato come malevolo grazie alle descrizioni date: con molta probabilità si può definire come un Trojan/Downloader che andrà a scaricare un secondo file dannoso per il nostro sistema. Da qui possiamo anche vedere lo storico del programma e con quanti nomi è stato segnalato.

Da CFF Explorer possiamo capire quali librerie il programma andrà ad inglobare ed attaccare con precisione sul sistema operativo.