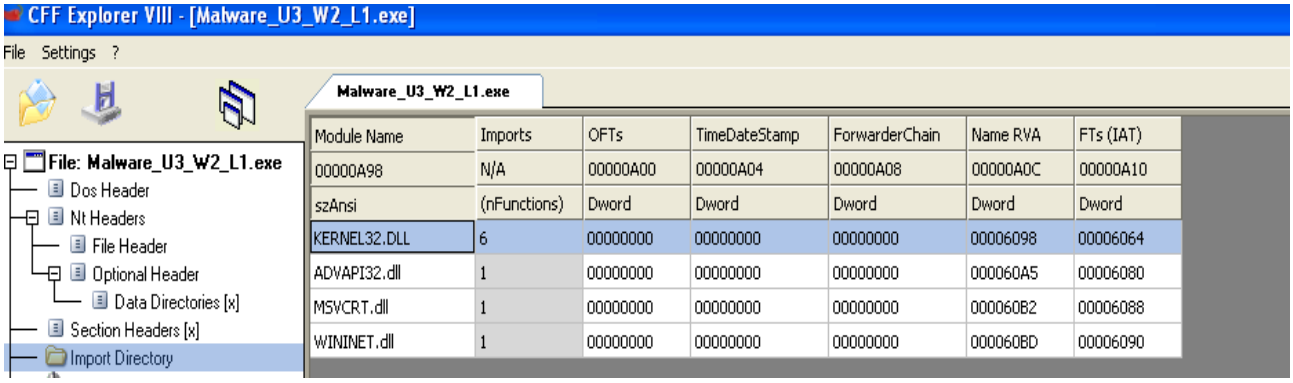
ANALISI DI UN MALWARE

Dentro import directory aprendo il malware con cff possiamo trovare le librerie importate
KERNEL32.DLL: Kernel32. dll è considerato un tipo di file DLL (Dynamic Link Library). I file DLL, come kernel32. dll, sono essenzialmente una "guida" che conserva le informazioni e le istruzioni per i file eseguibili (EXE) da eseguire.
ADVAPI32.DLL: Advapi32. dll è una libreria dinamica contenente numerose funzioni che vanno dall'avvio, pausa ed interruzione dei servizi del sistema operativo alla disconnessione dell'utente ed operazioni sul registro. Probabilmente qualche programma sta interferendo col sofwtare che si vuole installare.
MSVCRT.DLL: msvcrt.dll è un modulo che contiene le funzioni di libreria C Standard quale il printf, memcpy e cos. è una parte della libreria Runtime di Microsoft C.
Processi non di sistema come msvcrt.dll provengono da software installati nel sistema. Poiché la maggior parte delle applicazioni memorizza i dati sul disco rigido e nel registro di sistema, è probabile che il computer abbia subito frammentazione e accumuli di voci non valide che possono aver influito sulle prestazioni del PC.
WININET.DLL:wininet.dll è un modulo che contiene le funzioni Internet-relative usate dalle applicazioni di Windows. Nota: wininet.dll è un processo che il Trojan di Troj/Zlob-AO prova a travestire in se come nell'ambito di vero nome trattato di %systemroot% \ mscornet.exe. Questo processo è un rischio per la sicurezza e dovrebbe essere rimosso dal vostro sistema.
wininet.dll è un processo di sistema necessario perché il PC funzioni correttamente. Non lo si deve rimuovere.

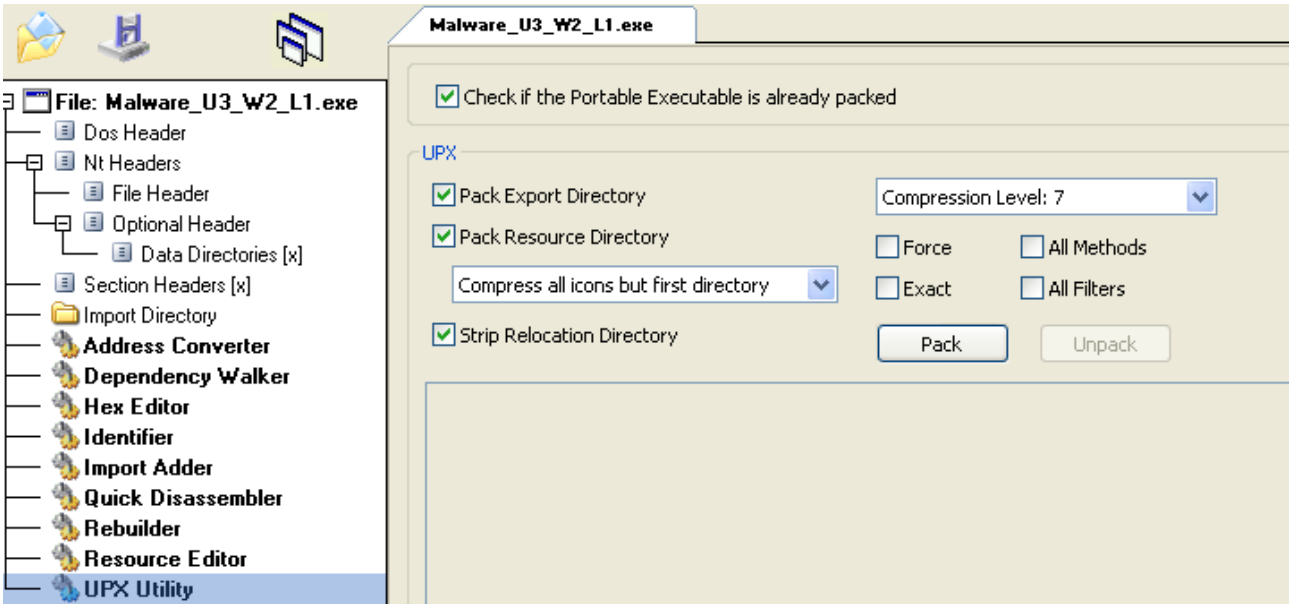


ANALISI DI UN MALWARE

Andiamo a trovare le sezioni del malware dentro ‘selection headers’ e troviamo che le sezioni sono compresse con upx

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
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

Andiamo su upx utility e clicchiamo su unpack



Torniamo nella cartella di prima e le nostre sezioni sono decompresse
.text: la sezioni text contiene le istruzioni che la cpu eseguirà una volta che il software sarà avviato.
.rdata: la sezione rdata include generalmente le informazioni circa le librerie e le funzione importate ed esportate dall’eseguibile, informazione che possiamo ricavare con cff explorer.
.data: la sezione data contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

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