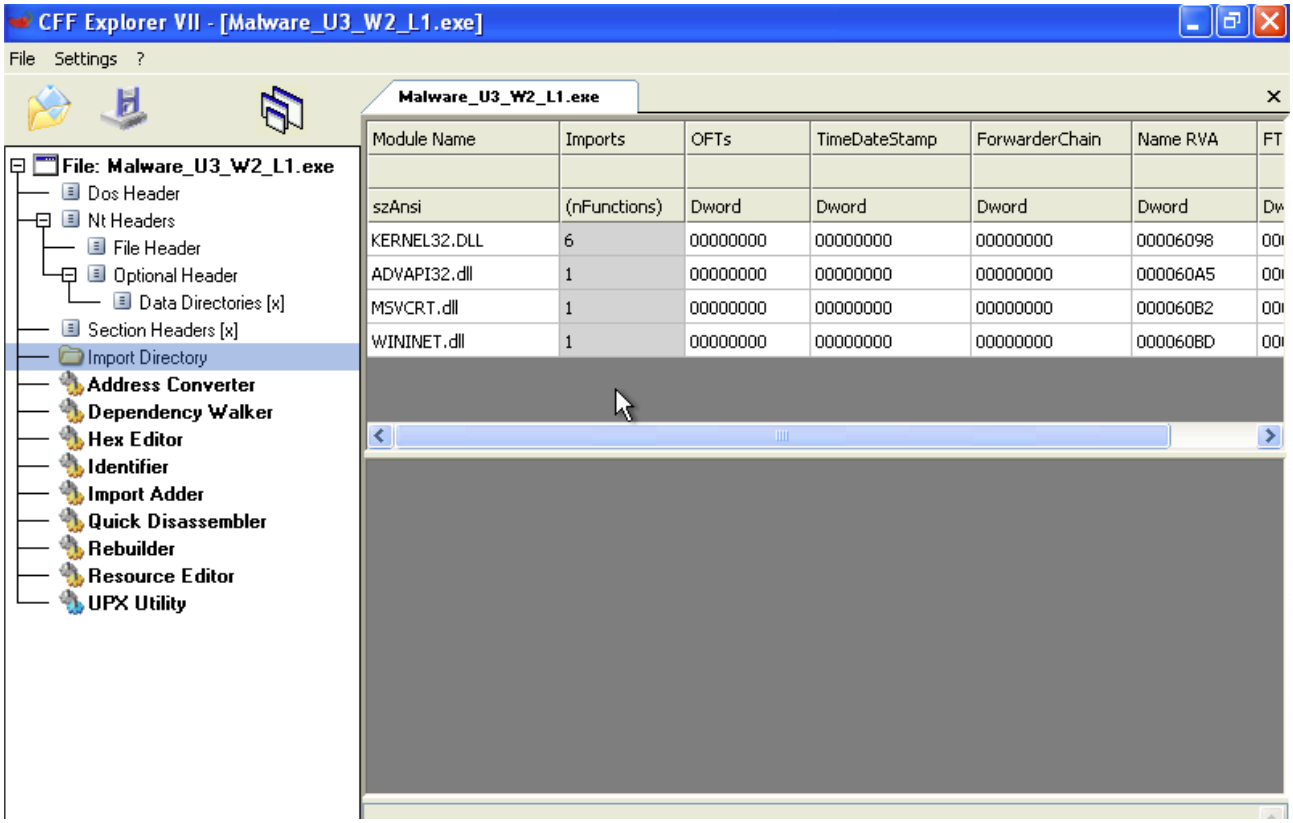
Esercizio G1

Analisi del malware

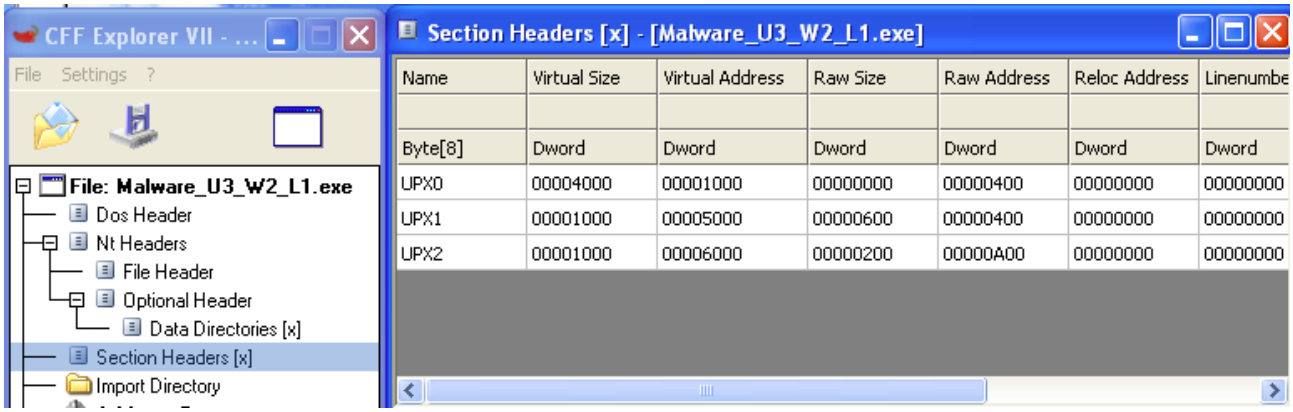
Un malware (Malicius software) serve per descrivere un programma o codice malevolo/dannoso per un sistema.



Kerlnel.32.dill: Contiene le funzioni principali del sistema operativo.
Advapi.32.dll: Contiene le funzioni per interagire con i servizi ed i registri del OS Microsoft.
Msvcrt.dll: Contiene funzioni per manipolare stringhe e allocazione di memoria.
Wininet.dll: Contiene le funzioni per l'implementazione di alcuni protocolli di rete(HTTP, FTP, NTP).

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

Le sezioni



UPX è uno dei packer più conosciuti. I packer sono dei software che vengono utilizzati dalle software house per proteggere il proprio codice da azioni di #**reverseEngineering**. Gli sviluppatori di #**Malware** li utilizzano invece per complicare le operazioni di malware analisi. Un software compresso con UPX è facilmente identificabile, le sessioni del file vengono rinominate in UPX0 UPX1.

Source: https://www.cybersecurityup.it

Considerazione

Potrebbe essere una backdoor, perché un modulo crea un servizio, un'altro crea una connessione ad internet e un'altro una uscita.