PRATICA S10-L1

ANALISI STATICA BASICA

GIULIA FIACCHI

TRACCIA

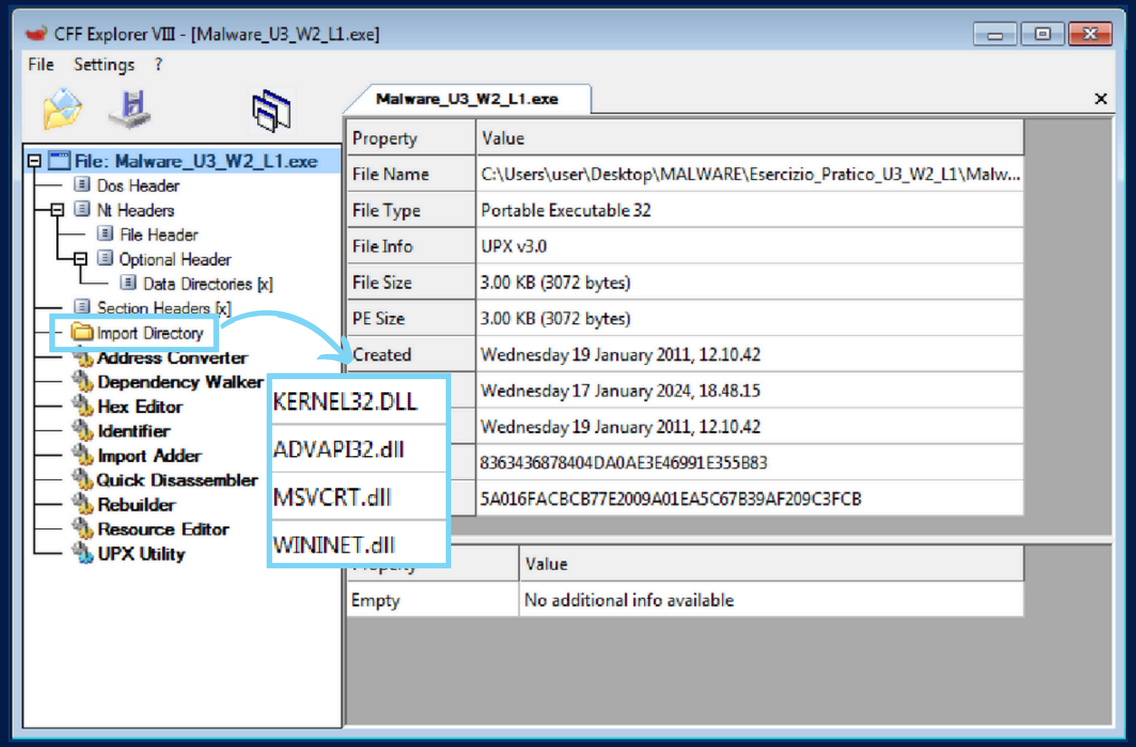
Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1» presente sul Desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse
- Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

PARTE 1

librerie importate

Come prima cosa avviamo la nostra macchina “Window 7 - malware analysis”, poi clicchiamo sulla cartella che si trova nel Desktop con il nome di “**Software Malware Analysis**” e da qui apriamo il software di nostro interesse che è **CFF Explorer.**
Una volta aperto è possibile da qui caricare un file per la seguente scansione, quindi clicchiamo sulla cartellina in alto a destra e cerchiamo il file di nostro interesse; che troviamo nella cartella “**MALWARE**” con il nome di **«Esercizio_Pratico_U3_W2_L1».**



Cliccando nella sezione “Import directory” possiamo trovare le librerie importate dal malware:

- **KERNEL32.DLL:** funzioni di gestione di memoria, input/output, e operazioni di file. È essenziale per molte operazioni di base del sistema operativo.
- **ADVAPI32.dll:** funzioni per l'accesso avanzato alle API di Windows, come la gestione del registro di sistema e i servizi.
- **MSVCRT.dll:** funzioni standard della libreria C/C++, come la gestione delle stringhe, l'input/output, la gestione della memoria e altre operazioni per l’esecuzione di C/C++
- **WININET.dll:** set di API che permettono alle applicazioni di interagire con i protocolli di Internet, come HTTP e FTP. È utilizzata principalmente per operazioni di rete e per l'accesso a Internet

PARTE 2

sezioni

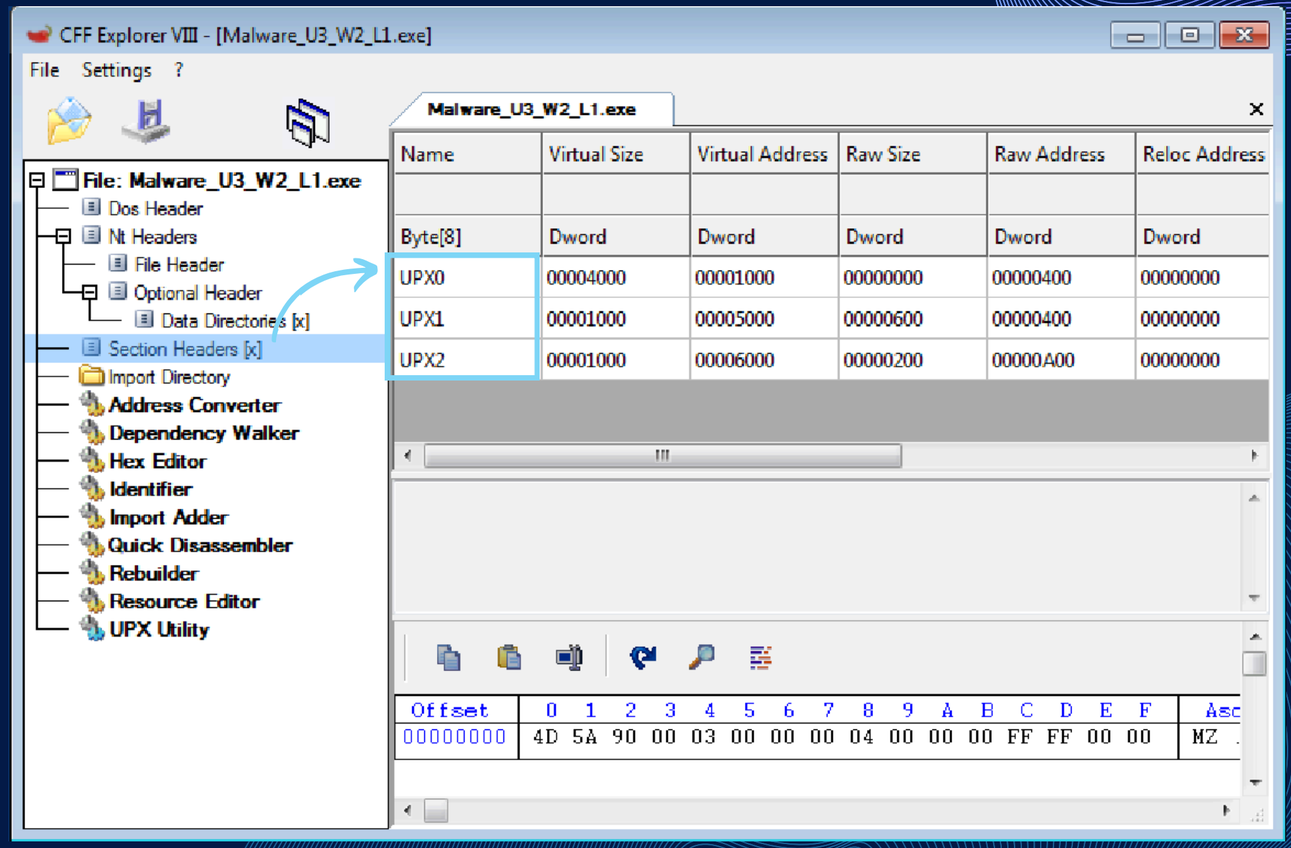
Ora ci spostiamo nella sezione “Section Headers [x]” e qui possiamo trovare le sezioni (blocchi di dati distinti che contengono vari tipi di informazioni necessarie per l'esecuzione del programma).

Sono state trovate 3 tipologie diverse ma, tutte hanno in comune che sono compressori di eseguibili;

- **UPX0:** contiene i dati non compressi che possono includere il codice di decompressione e altre informazioni necessarie per avviare il processo di decompressione

- **UPX1:** sezione principale che contiene i dati compressi del file originale

- **UPX2:** può contenere dati aggiuntivi compressi o risorse che non rientravano nelle altre sezioni (non sempre presente)



PARTE 3

considerazione finale

L'uso di UPX per comprimere il malware e l'uso di advapi32.dll per manipolare il registro di sistema o i servizi di Windows indicano strategie per evadere la rilevazione e mantenere la persistenza nel sistema. L'utilizzo di wininet.dll implica che il malware ha capacità di comunicazione di rete usato per dare comandi o esfiltrare dati. Le chiamate al kernel indicano che che il malware può manipolare il sistema operativo a basso livello.

L'uso combinato di queste librerie e la compressione con UPX indicano un livello di complessità e sofisticazione nel design del malware.

Tutti questi fattori indicano dunque che gli attaccanti utilizzano tecniche sofisticate e che sono esperti del campo, per questo per analizzare al meglio il malware sono necessari strumenti avanzati e metodologie di analisi approfondite per comprendere completamente il comportamento e l'esecuzione del malware.