INTRO E ANALISI STATICA BASICA

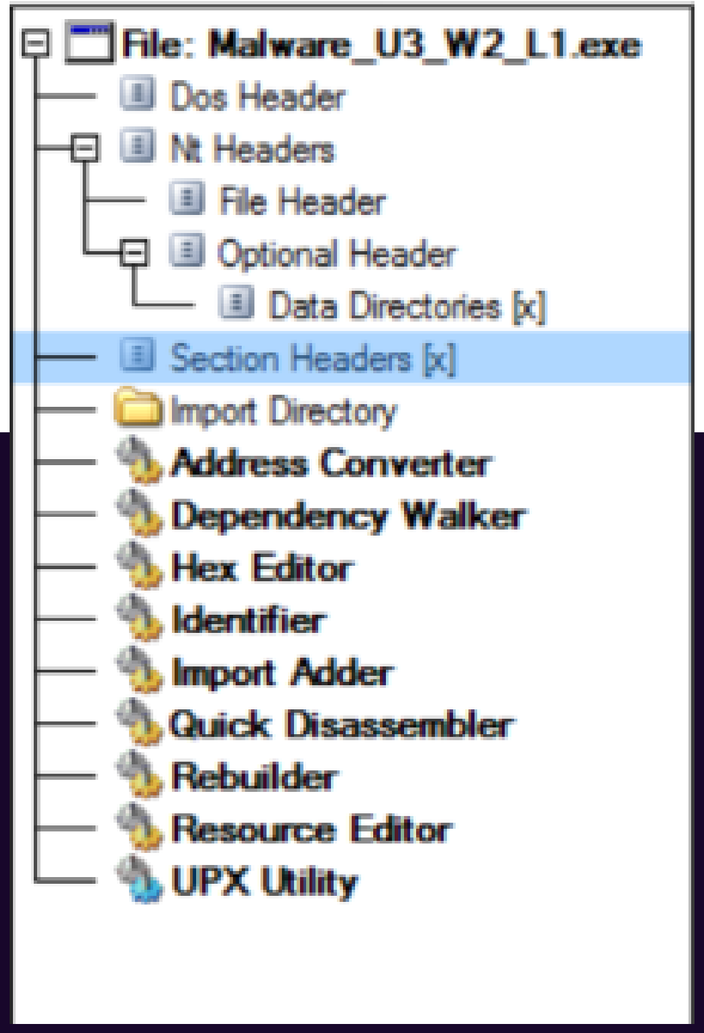
INTRO E ANALISI STATICA BASICA

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

SCANSIONE



Grazie all'impiego di un'analisi dinamica attraverso l'utilizzo dello strumento CFF Explorer, si procede all'analisi approfondita del file contenente un malware all'interno di un ambiente protetto. In questo specifico contesto, l'ambiente in questione è la macchina con sistema operativo Windows 7. Questo processo consente di esaminare il comportamento dinamico del malware, fornendo una comprensione dettagliata delle sue azioni all'interno del sistema operativo.

LIBRERIE

- 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
- WSock32.dll e Ws2_32.dll: contengono le funzioni di network, come le socket, le funzioni connect, bind. Ogni malwareche utilizza funzionalità di rete caricherà certamente una di queste librerie.

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	9	00000000	00000000	00000000	0000216C	00002010
ADVAPI32.dll	3	00000000	00000000	00000000	00002179	00002000
MSVCRT.dll	13	00000000	00000000	00000000	00002186	00002038
WININET.dll	2	00000000	00000000	00000000	00002191	00002070

MALWARE

Un "malware trojan" (o trojan) è un tipo di software dannoso progettato per sembrare legittimo o utile, ma che in realtà esegue attività dannose senza il consenso dell'utente. Il termine "trojan" deriva dal mito del cavallo di Troia, dove i Greci fecero entrare un enorme cavallo di legno nella città di Troia, nascondendovi segretamente dei soldati al suo interno.
Similmente, un trojan può sembrare inoffensivo o persino vantaggioso, ma una volta che viene eseguito sul sistema dell'utente, può svolgere varie attività dannose, come:

1. Furto di informazioni: Il trojan può raccogliere informazioni personali come password, dati bancari e altre informazioni sensibili.
2. Installazione di altri malware: Il trojan può scaricare e installare ulteriori malware sul sistema.
3. Creazione di una backdoor: Può aprire una "porta posteriore" nel sistema, consentendo a un attaccante di accedere e controllare il computer in modo remoto.
4. Attacchi di tipo ransomware: Alcuni trojan sono progettati per cifrare i file dell'utente e chiedere un riscatto per ripristinare l'accesso.