

Cyber Security & Ethical Hacking

ANALISI STATICA BASICA

Alejandro Cristino
S10-L3

TRACCIA

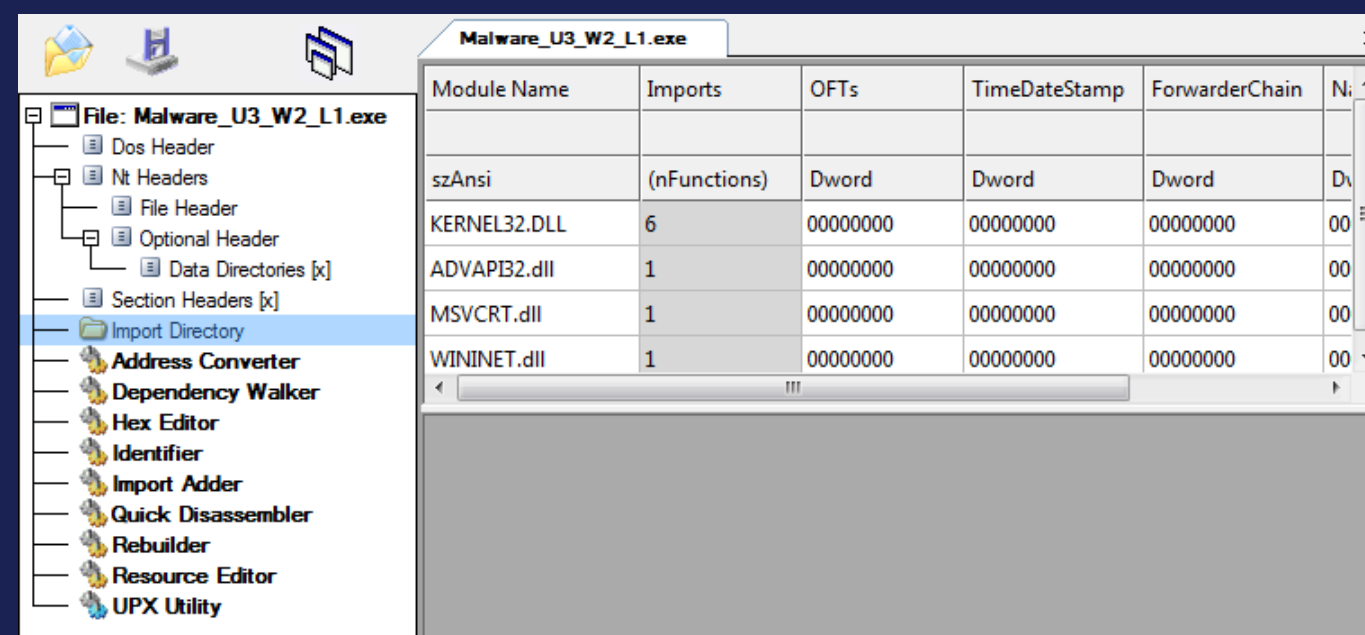
Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1» presente sul Desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- 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

LIBRERIE DEL MALWARE

Utilizzando CFF Explorer, dalla sezione "Import Directory" risulta che il malware U3_W2_L1 importa quattro librerie:

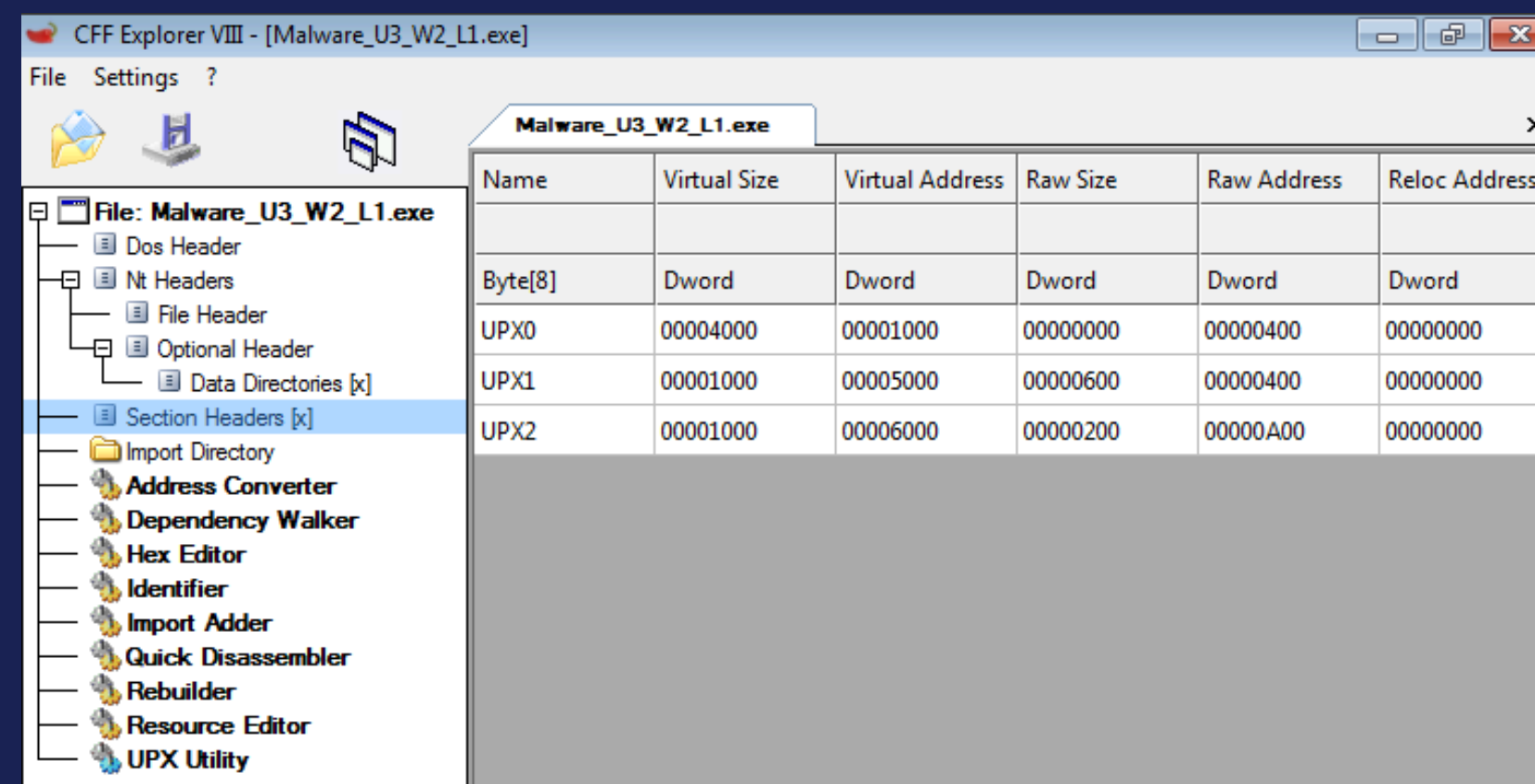
1. Kernel32.dll: Fornisce le funzioni essenziali per il funzionamento del sistema operativo.
2. Advapi32.dll: Include funzioni per l'interazione con il registro di sistema e la gestione dei servizi di Windows.
3. MSVCRT.dll: Una libreria C che offre funzionalità per la gestione delle stringhe e l'allocazione della memoria.
4. Wininet.dll: Contiene funzioni per implementare servizi di rete come FTP, NTP e HTTP.



SEZIONI DEL MALWARE

Per esaminare le diverse sezioni di cui è composto il malware, ci spostiamo nella sezione "Section Headers [x]" del programma. Qui osserviamo che il malware U3_W2_L1 contiene tre sezioni distinte.

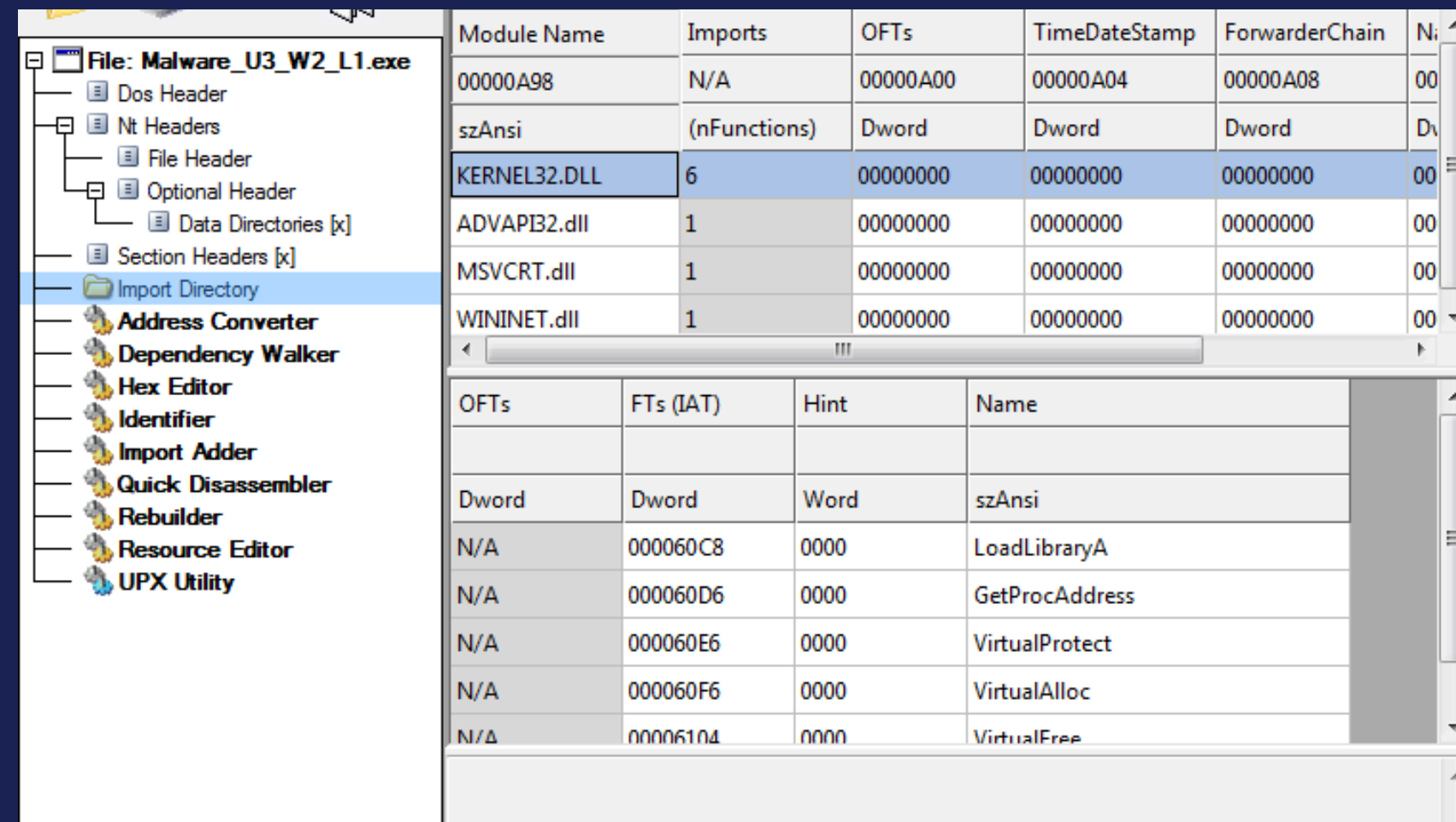
Sembra che il malware abbia offuscato i veri nomi delle sezioni utilizzando le etichette UPX0, UPX1, e UPX2. Questa tecnica è tipicamente impiegata per impedire l'identificazione delle sezioni originali, spesso tramite l'uso di un packer come UPX (Ultimate Packer for eXecutables). Di conseguenza, non è possibile determinare con precisione la funzione di ciascuna sezione senza ulteriori analisi o processi di deoffuscamento.



CONSIDERAZIONI FINALI

Il malware analizzato risulta essere particolarmente avanzato, rendendo difficile il recupero di informazioni dettagliate sul suo comportamento tramite l'analisi statica di base.

Questo è evidenziato dalla presenza delle funzioni importate "LoadLibrary" e "GetProcAddress", che suggeriscono l'uso di tecniche di caricamento dinamico delle librerie durante l'esecuzione (runtime). Tali tecniche mascherano efficacemente le informazioni sulle librerie utilizzate, nascondendo le dipendenze reali fino al momento dell'esecuzione, e rendendo così più complessa l'analisi e la rilevazione del malware.



Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Ni
00000A98	N/A	00000A00	00000A04	00000A08	00
szAnsi	(nFunctions)	Dword	Dword	Dword	Dv
KERNEL32.DLL	6	00000000	00000000	00000000	00
ADVAPI32.dll	1	00000000	00000000	00000000	00
MSVCRT.dll	1	00000000	00000000	00000000	00
WININET.dll	1	00000000	00000000	00000000	00

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	000060C8	0000	LoadLibraryA
N/A	000060D6	0000	GetProcAddress
N/A	000060E6	0000	VirtualProtect
N/A	000060F6	0000	VirtualAlloc
N/A	00006104	0000	VirtualFree