

# S10-L1

## Esercizio



V A N   Z W A M   A R J E N



1

2

3

4

5

# Traccia

## S10-L1

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 importate



1

2

3

4

5

## 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

## MSVCRT.DLL

Contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C

## WININET.DLL

Contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP

CFF Explorer VIII - [Malware\_U3\_W2\_L1.exe]

File Settings ?

Malware\_U3\_W2\_L1.exe

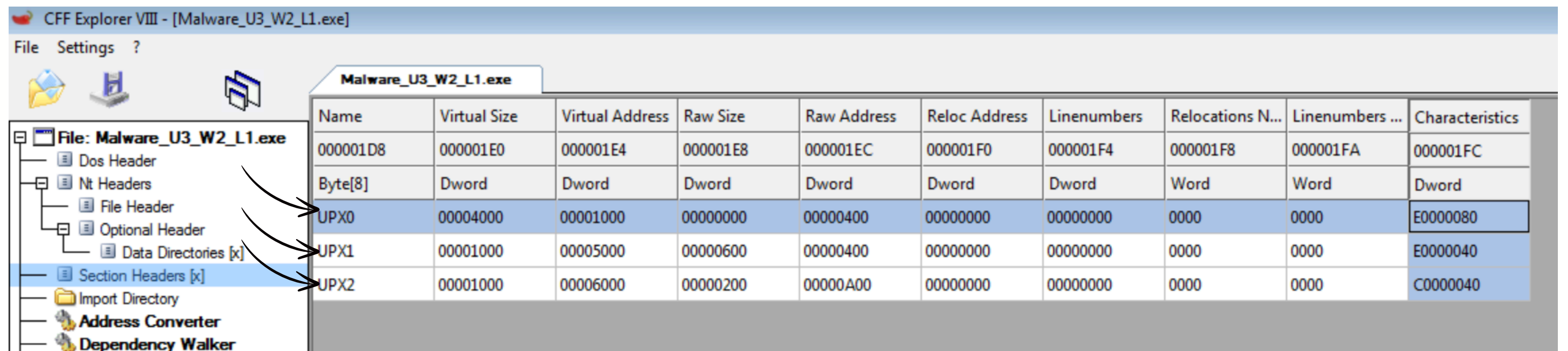
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

File: Malware\_U3\_W2\_L1.exe

- Dos Header
- Nt Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor

# Sezioni

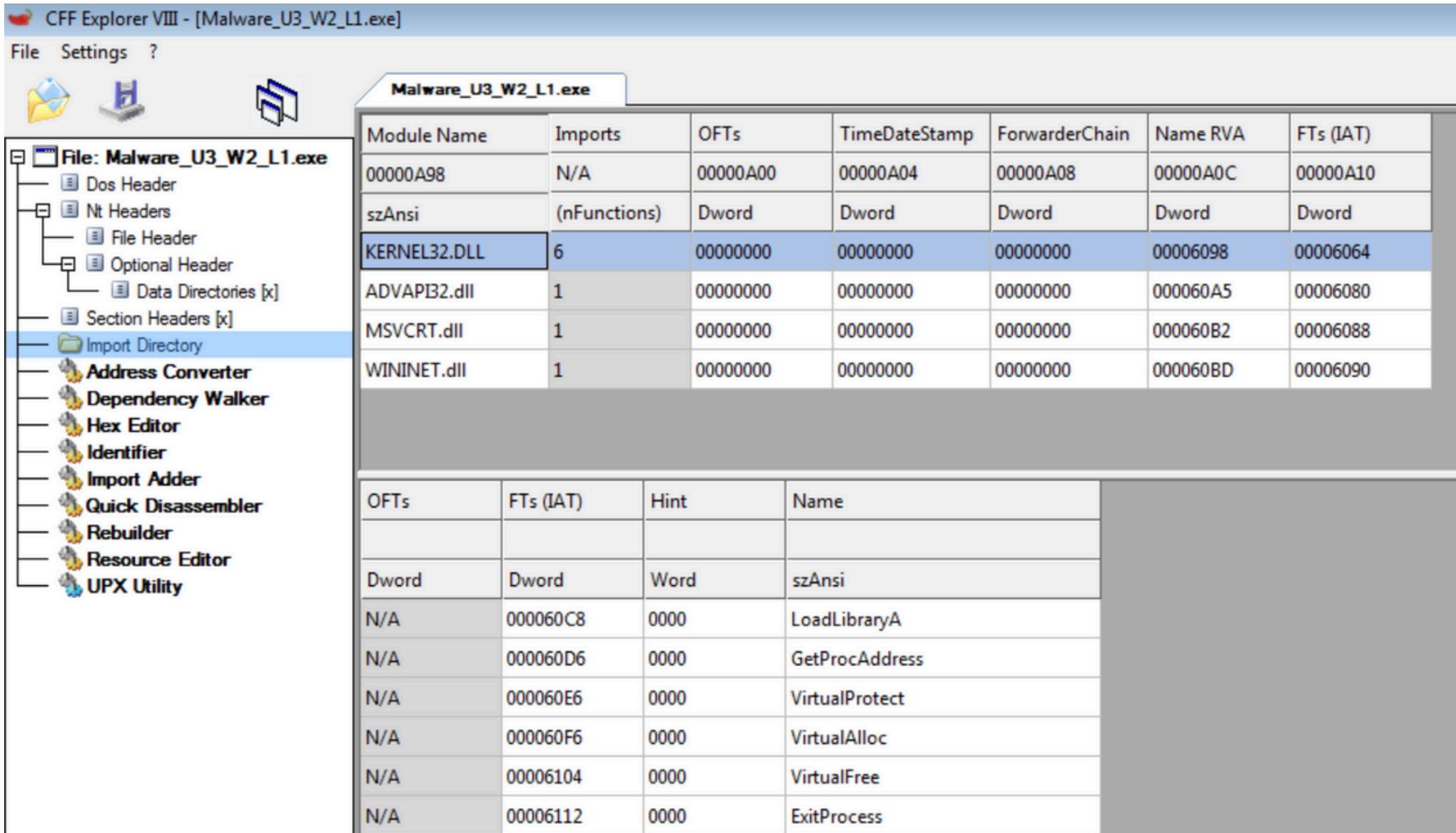
Tramite “Section Headers” possiamo controllare le sezioni utilizzate dal malware, però in questo caso il nome non è visibile, potrebbe essere un camuffamento.



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
000001D8	000001E0	000001E4	000001E8	000001EC	000001F0	000001F4	000001F8	000001FA	000001FC
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

# Considerazioni finali

Si tratta di un malware altamente sofisticato che presenta alcune caratteristiche che rendono difficile analizzarne il comportamento attraverso **un'analisi statica di base**. Questa difficoltà è evidenziata dal fatto che il **malware** utilizza le funzioni **"LoadLibrary"** e **"GetProcAddress"** per importare librerie durante l'esecuzione, **nascondendo così le informazioni sulle librerie importate inizialmente**. L'uso di **"LoadLibrary"** e **"GetProcAddress"** suggerisce che il malware carica **dinamicamente** librerie esterne durante l'esecuzione, piuttosto che dipendere da librerie statiche già presenti nel sistema.



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

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
N/A	00006112	0000	ExitProcess

**Questo approccio rende più complesso** identificare le librerie coinvolte e comprendere appieno le **funzionalità** del malware. Inoltre, l'analisi statica di base, che si basa sull'esame del codice sorgente o del file eseguibile senza effettuare l'esecuzione effettiva, **non fornisce molte informazioni sul comportamento del malware a causa della sua natura avanzata**. Questo significa che si possono avere difficoltà nel determinare le azioni esatte che il malware intraprende o le risorse di sistema che sfrutta.

In sintesi, il malware in questione è progettato in modo da rendere complicata l'analisi statica di base, grazie all'importazione dinamica di librerie a tempo di esecuzione. Questo rende necessario un approccio più avanzato per comprendere appieno le sue funzionalità e il suo comportamento.



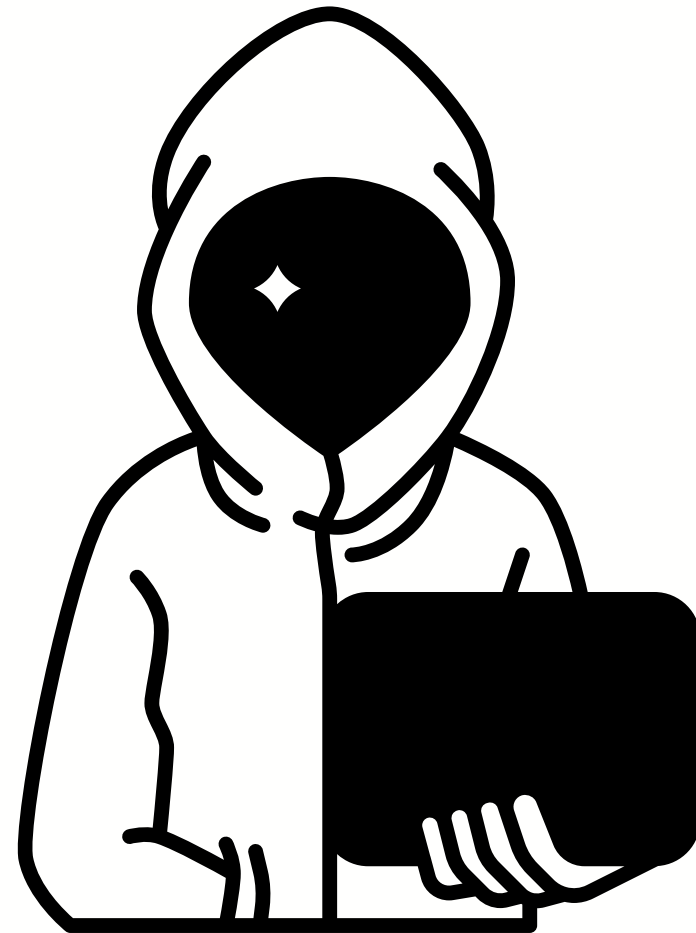
1

2

3

4

5



# ***Grazie***

**Esercizio a cura di**  
Van Zwam Arjen

