

# **ANALISI STATICÀ BASICA**

**REPORT: MORGAN PETRELLI**

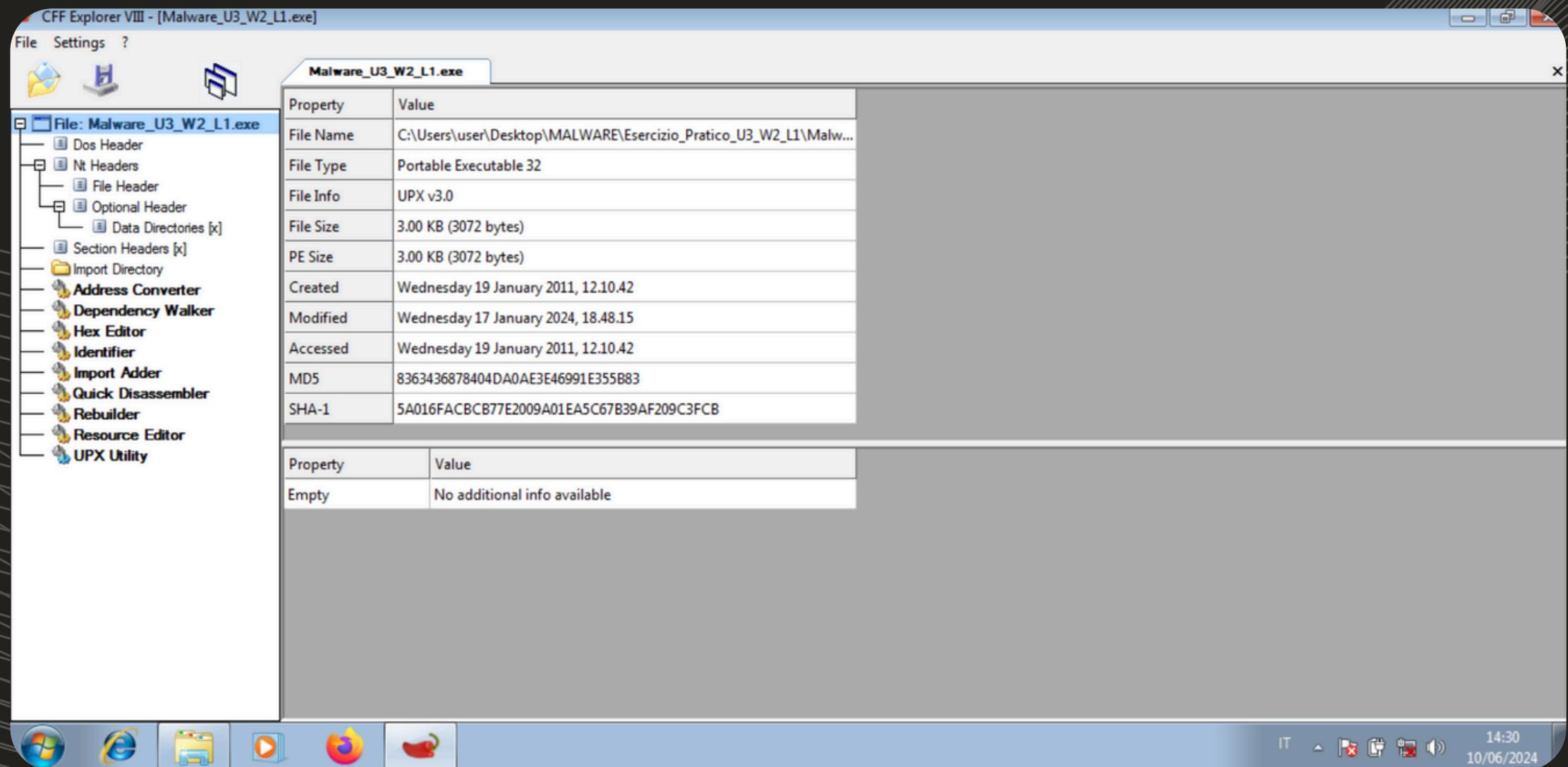


# TRACCIA

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

inizio importando il file eseguibile «Esercizio\_Pratico\_U3\_W2\_L1» su CFF Explorer uno strumento utile in vari aspetti della cybersecurity, in particolare per analisi dei malware, reverse engineering e valutazione delle vulnerabilità.



# LIBRERIE IMPORTATE

mi sposto su import Directory per vedere che librerie importa il file.

**kernel32.dll:** è una delle principali librerie di sistema di Windows contiene numerose funzioni a basso livello utilizzate per la gestione del sistema operativo e per l'interazione con l'hardware. Queste funzioni sono fondamentali per il funzionamento delle applicazioni e del sistema operativo stesso.

**Advapi32.dll:** libreria di sistema fondamentale per il sistema operativo Windows che fornisce funzioni avanzate per la gestione della sicurezza, del registro di sistema, dei servizi di sistema e degli eventi.

**MSVCRT.dll:** è una componente critica per l'esecuzione di applicazioni sviluppate con Microsoft Visual C++. Fornisce un'ampia gamma di funzioni come operazioni su stringhe, gestione della memoria, manipolazione di file e input/output, gestione degli errori e operazioni matematiche.

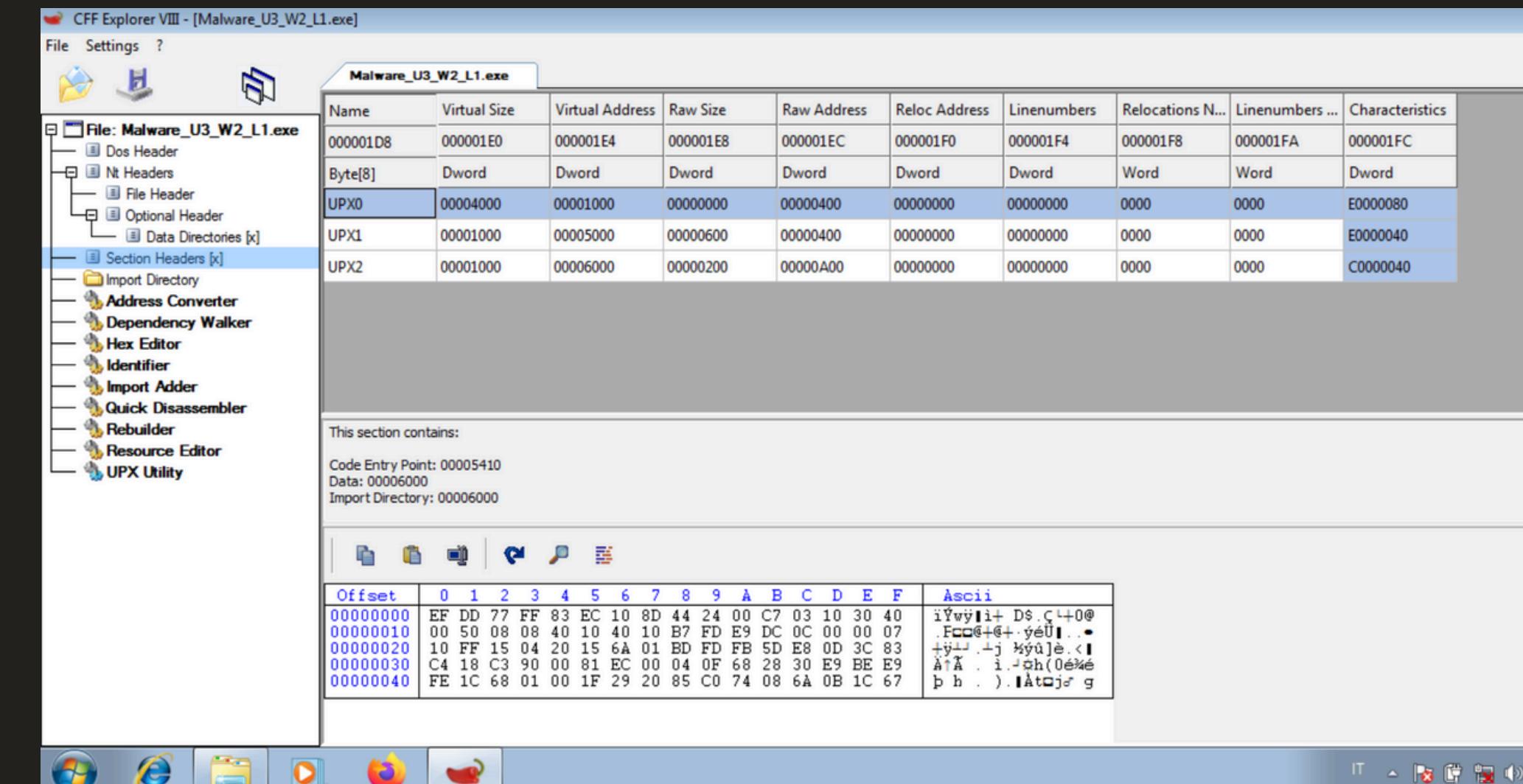
**Wininet.dll:** è una libreria di sistema di Windows che fornisce funzioni per l'accesso a Internet e ai servizi di rete. Viene utilizzata da applicazioni che necessitano di comunicare attraverso protocolli Internet come HTTP e FTP.

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

# SEZIONI

per visualizzare le sezioni di cui è composto il malware mi sono spostato sulla sezione "section header".

il malware è formato da 3 sezioni ma non è possibile visualizzare il vero nome delle sezioni è nascosto e non mi è quindi possibile capire da che sezioni è composto.



# CONSIDERAZIONI FINALI

si tratta di un malware avanzato che non consente di recuperare molte informazioni da un analisi statica basica. Questo perchè alcuni malware utilizzano il caricamento delle librerie durante l'esecuzione (runtime import) nascondendo di fatto all'analisi statica le funzioni e le librerie importate come le funzioni «LoadLibrary e GetProcAddress» che vengono utilizzate per caricare funzioni addizionali durante l'esecuzione.

Module Name	Imports	OFTs	TimeStamp	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	00006098	00006064	
ADVAPI32.dll	1	00000000	00000000	000060A5	00006080	
MSVCRT.dll	1	00000000	00000000	000060B2	00006088	
WININET.dll	1	00000000	00000000	000060BD	00006090	

OFTs	FTs (IAT)	Hint	Name
N/A	00000A64	00000AC8	00000ACA
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