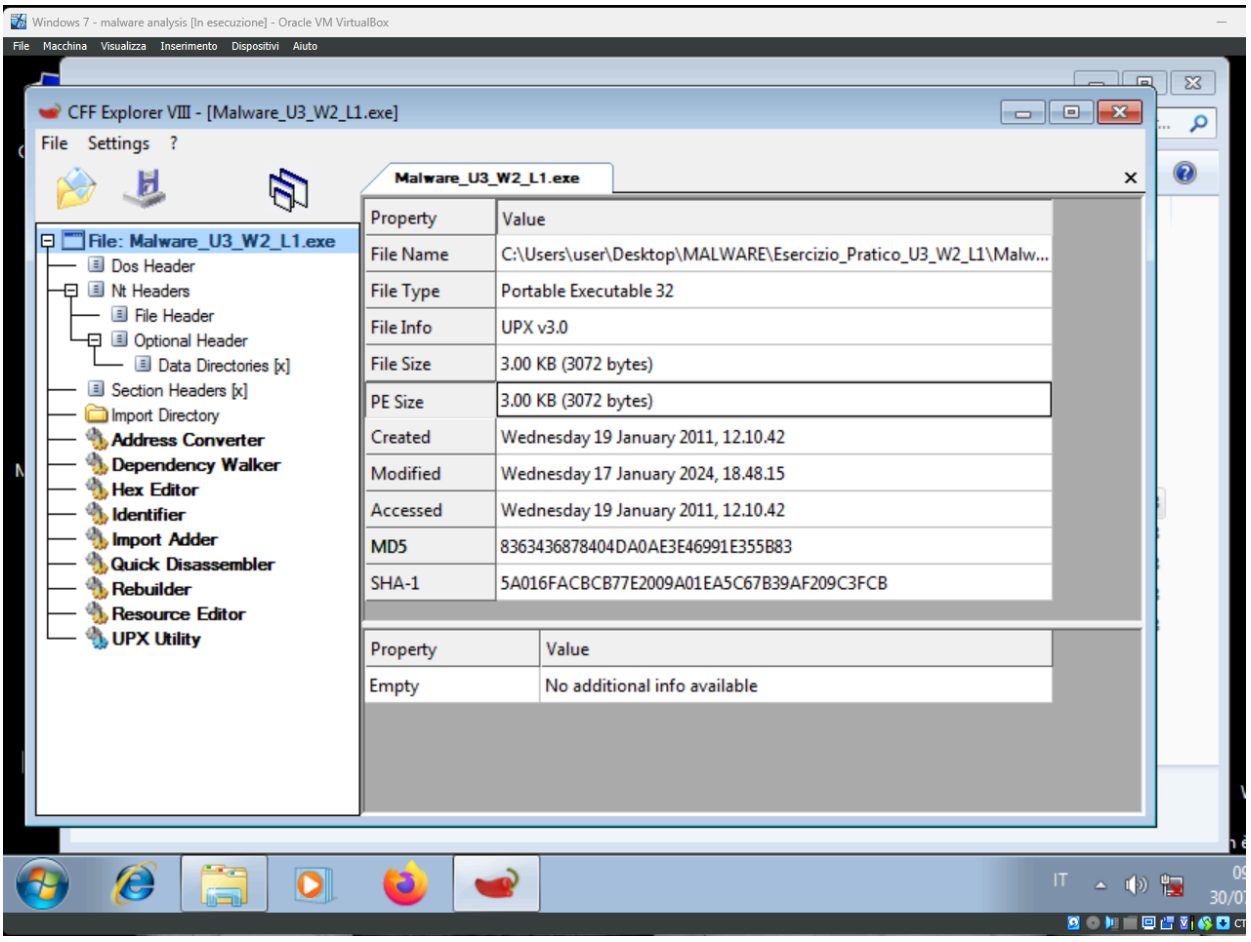
Analisi statica basica - Malizia Marco | Datashields

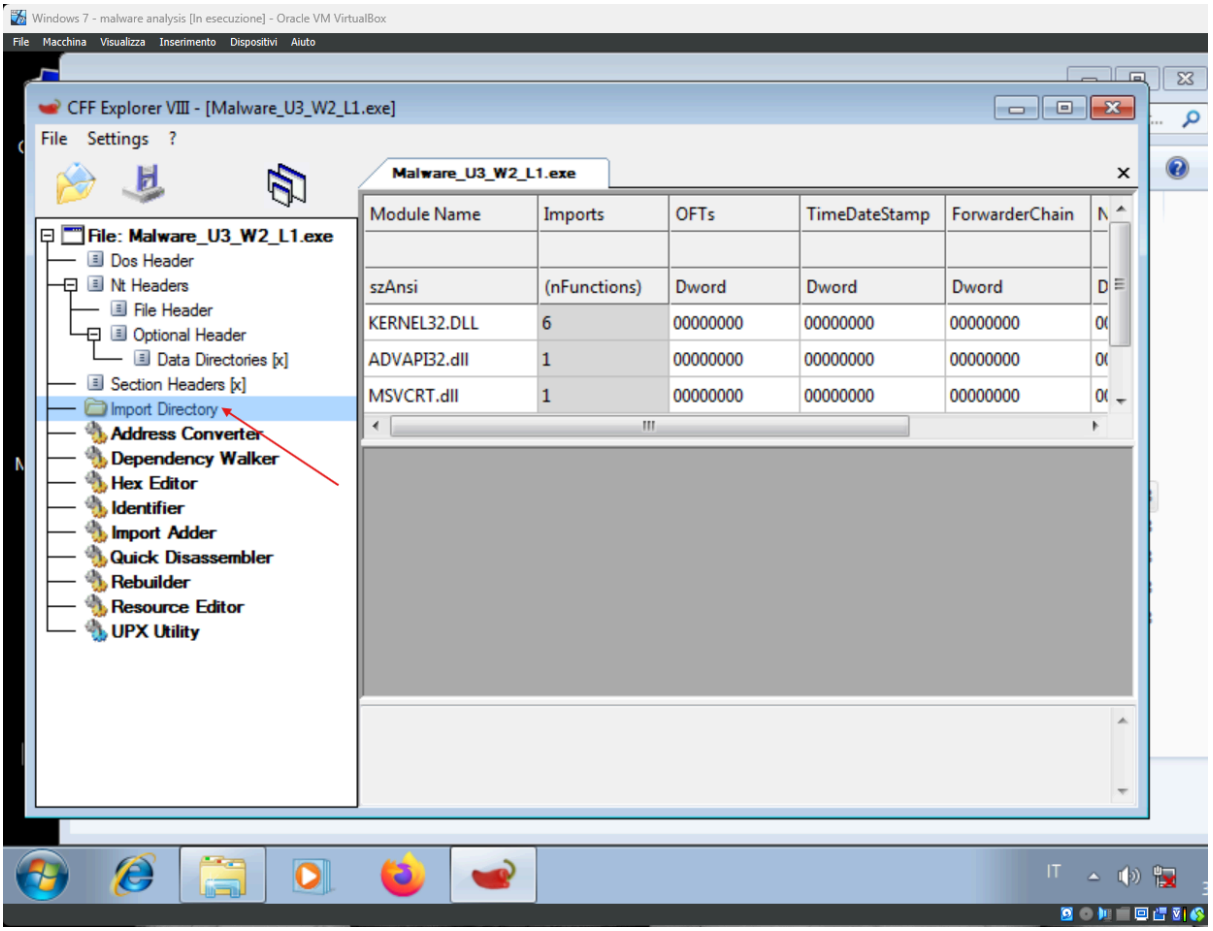
Traccia:
Esercizio Analisi statica Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1» presente sul Desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:
• Indicare le librerie importate dal malware, fornendo una 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

Svolgimento:

1. Avviamo in sicurezza la macchina di Windows Malware Analysis disattivando ogni possibile collegamento o scheda di rete.
2. Una volta avviata possiamo eseguire il programma **CFF Explorer** per proseguire con le analisi del Malware oggetto di lavoro.
3. Avviato il programma possiamo importare il file oggetto.



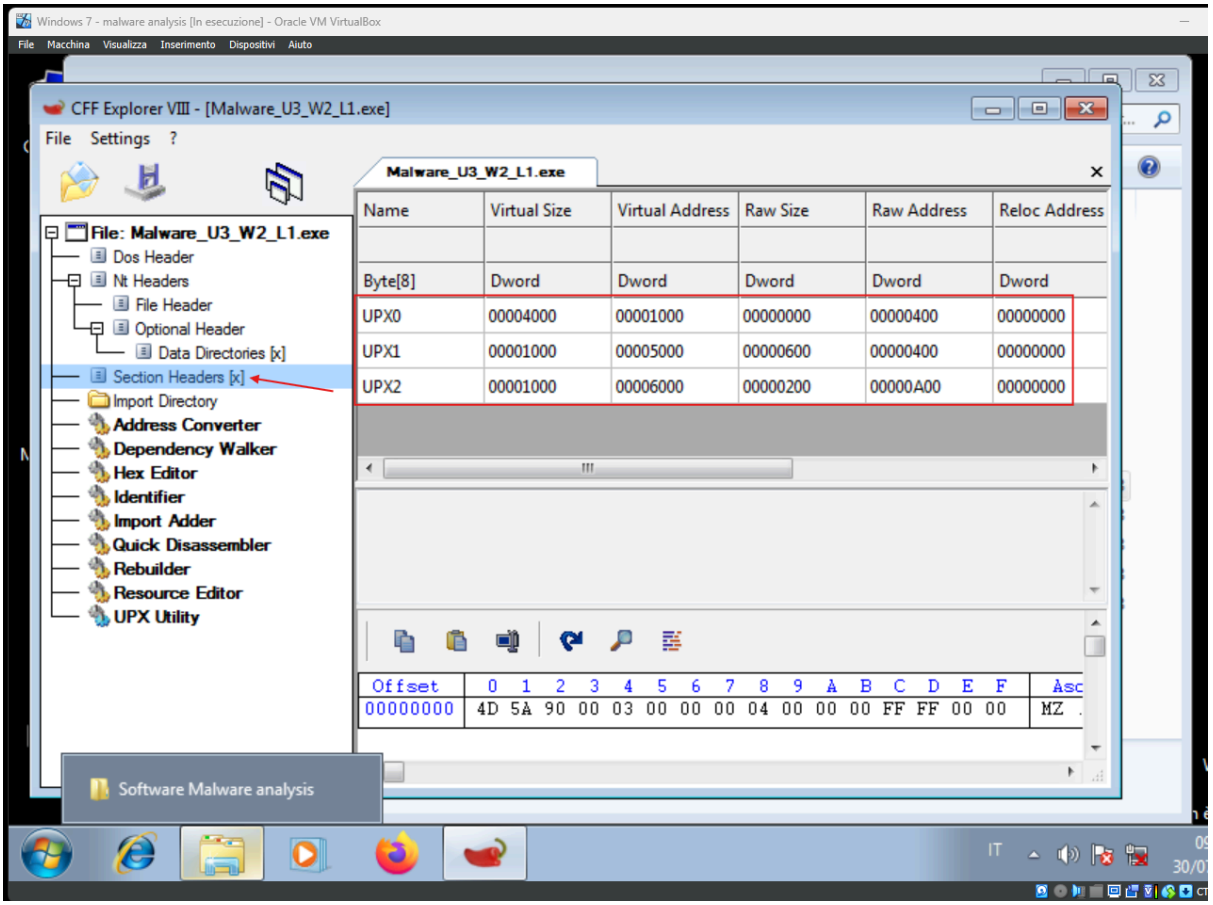
4. Successivamente, navigando nel menù a tendina del file, possiamo spostarci su “Import Directory” ed analizzare le librerie utilizzate dal file malevolo.



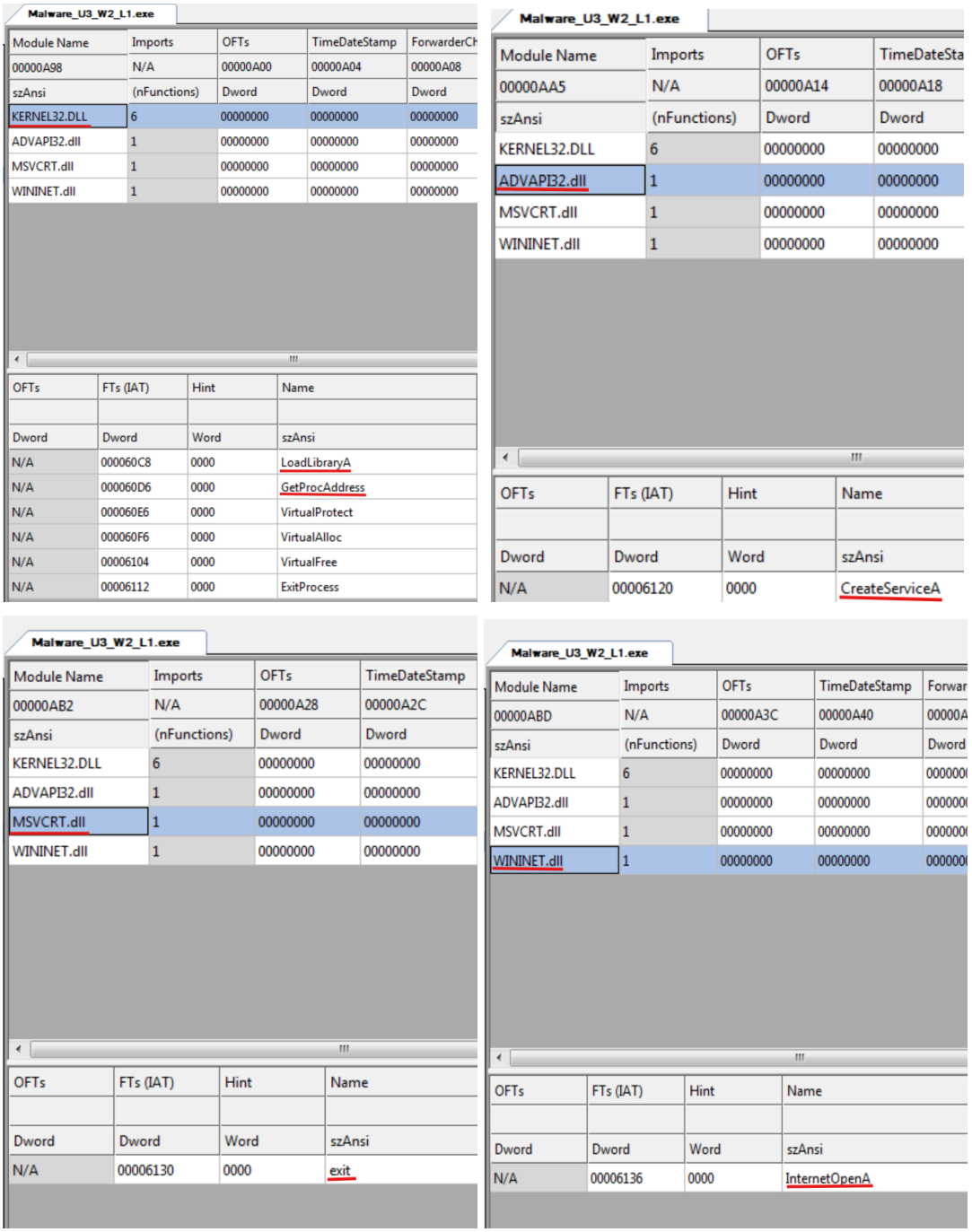
Il file contiene 4 librerie essenziali per il funzionamento delle applicazioni su Windows.

- KERNEL32.DLL: Gestisce la memoria, i processi e le operazioni I/O di Windows.
- ADVAPI32.dll: Fornisce funzioni di sicurezza, gestione del registro e registrazione degli eventi.
- MSVCRT.dll: Implementa le funzioni standard del linguaggio C per Visual C++.
- WININET.dll: Supporta operazioni di rete con protocolli Internet come HTTP e FTP.

5. Spostandoci sulla directory “Section Headers” possiamo analizzare le sezioni che compongono l’eseguibile malevolo, analisi che porta poche informazioni a riguardo poichè non abbiamo informazioni estrapolabili.



6. Tornando in “Import Directory” possiamo analizzare meglio le librerie andando a visionare le funzioni importate da ognuna di esse.



Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderCh
00000A98	N/A	00000A00	00000A04	00000A08
szAnsi	(nFunctions)	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000
ADVAPI32.dll	1	00000000	00000000	00000000
MSVCRT.dll	1	00000000	00000000	00000000
WININET.dll	1	00000000	00000000	00000000

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

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateSta
00000AA5	N/A	00000A14	00000A18
szAnsi	(nFunctions)	Dword	Dword
KERNEL32.DLL	6	00000000	00000000
ADVAPI32.dll	1	00000000	00000000
MSVCRT.dll	1	00000000	00000000
WININET.dll	1	00000000	00000000

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006120	0000	CreateServiceA

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp
00000AB2	N/A	00000A28	00000A2C
szAnsi	(nFunctions)	Dword	Dword
KERNEL32.DLL	6	00000000	00000000
ADVAPI32.dll	1	00000000	00000000
MSVCRT.dll	1	00000000	00000000
WININET.dll	1	00000000	00000000

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006130	0000	exit

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	Forwar
00000ABD	N/A	00000A3C	00000A40	00000A
szAnsi	(nFunctions)	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	0000000
ADVAPI32.dll	1	00000000	00000000	0000000
MSVCRT.dll	1	00000000	00000000	0000000
WININET.dll	1	00000000	00000000	0000000

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006136	0000	InternetOpenA

Dopo aver effettuato ricerche in rete riguardo le funzioni di queste librerie possiamo valutare il file malevolo come un file che importa le librerie in questione e le esegue mantenendole nascoste all’utente, tra le tante le funzioni della libreria “KERNEL32.dll” come “LoadLibrary” e “GetProcAddress” hanno destato più sospetto.