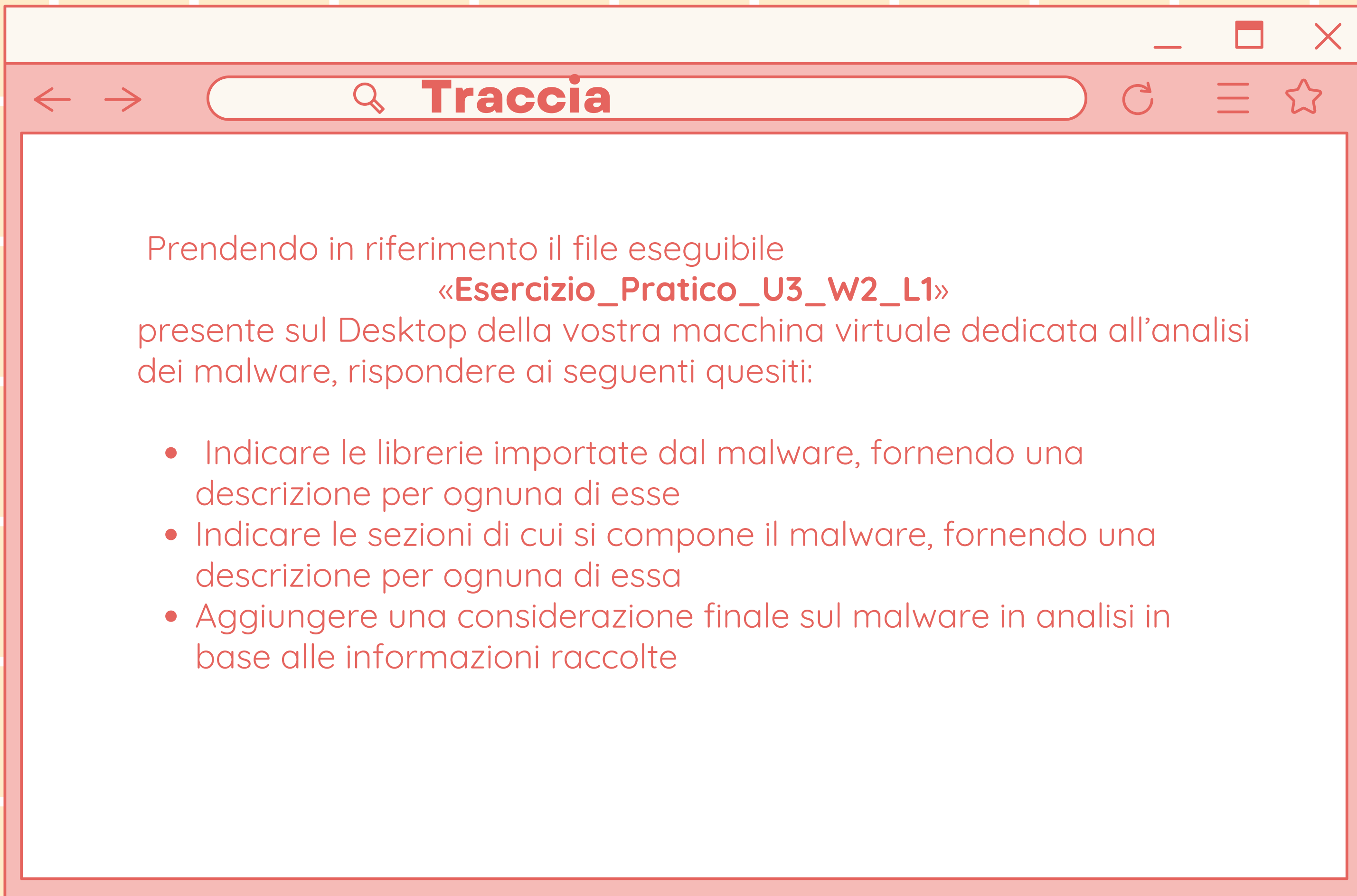


S10 / L1

Analisi statica basica Malware

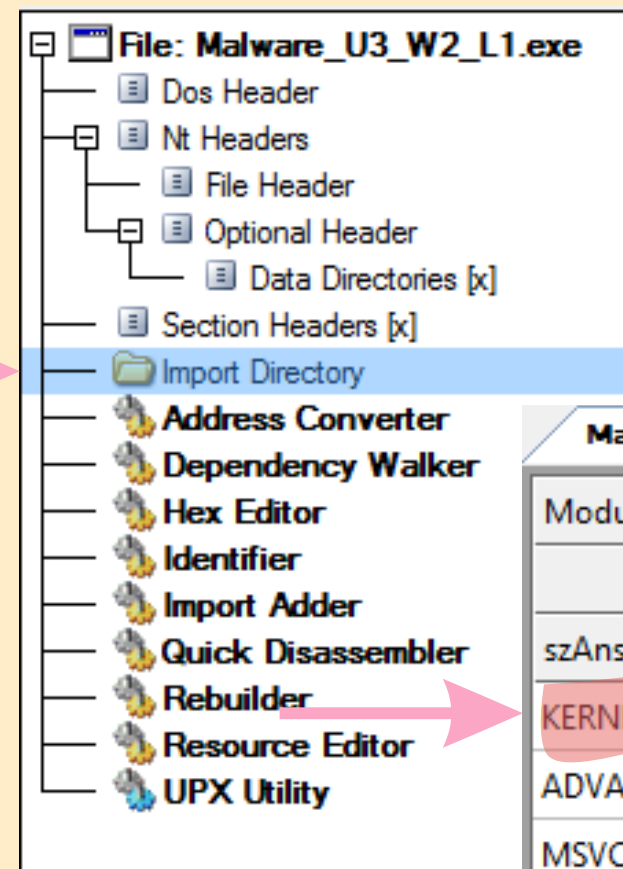
Created by Noemi
de Martino.



Librerie

1. KERNEL32.DLL

- **Descrizione:** Fornisce le API di base del sistema operativo Windows, utilizzate per la gestione della memoria, la gestione dei processi, e altre operazioni di basso livello.
- **Funzioni Importate:** LoadLibraryA, GetProcAddress, VirtualProtect, VirtualAlloc, VirtualFree, ExitProcess

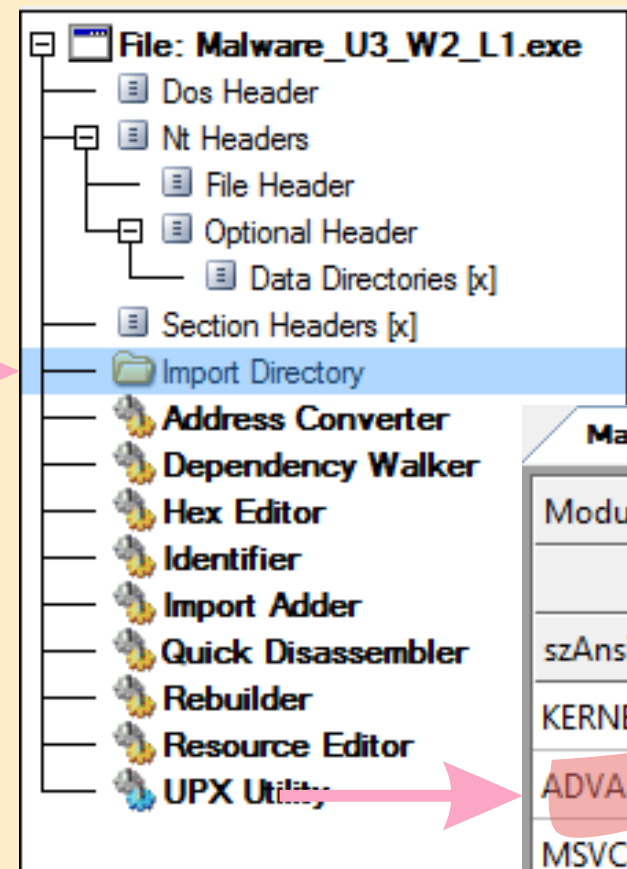


Malware_U3_W2_L1.exe										
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)				
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword				
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064				
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	OFTs	FTs (IAT)	Hint	Name	
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	N/A	00000A64	00000AC8	00000ACA	
WININET.dll	1	00000000	00000000	00000000	000060BD	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	

Librerie

2. ADVAPI32.DLL

- **Descrizione:** Fornisce le API avanzate di Windows per la gestione delle attività di sicurezza e di registro.
- **Funzioni Importati:** CreateServiceA



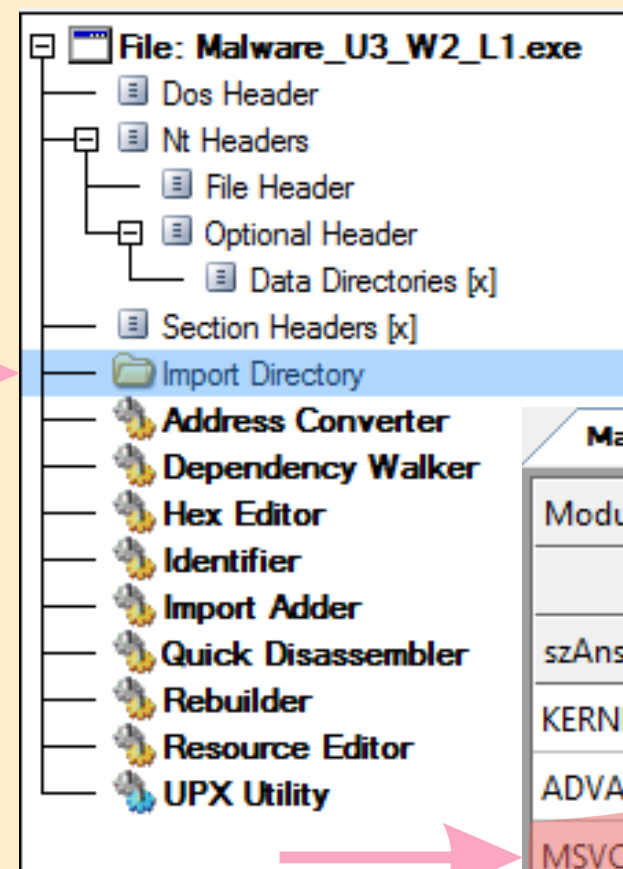
Malware_U3_W2_L1.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006080
WININET.dll	1	00000000	00000000	00000000	000060BD	00006080

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

Librerie

3. MSVCRT.DLL

- **Descrizione:** Fornisce le routine standard del runtime C di Microsoft, incluse le funzioni per la gestione della memoria, la manipolazione delle stringhe, le operazioni di I/O e altre funzioni di runtime.
- **Funzioni Importati:** exit



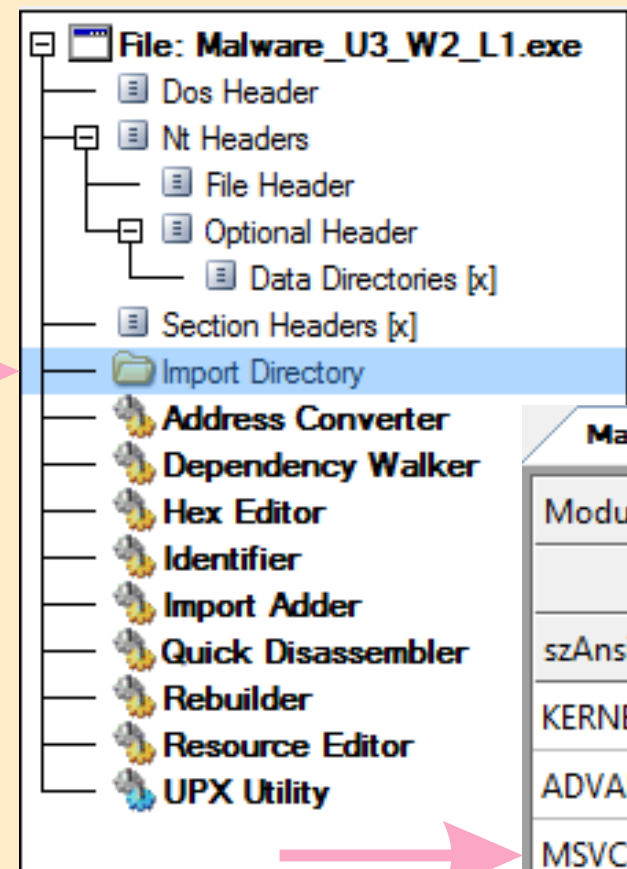
Malware_U3_W2_L1.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000			

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

Librerie

4. WININET.DLL

- **Descrizione:** Fornisce funzioni che implementano i protocolli Internet come FTP, HTTP, e HTTPS. Queste API vengono spesso utilizzate per il download e l'upload di file attraverso Internet.
- **Funzioni Importati:** InternetOpenA

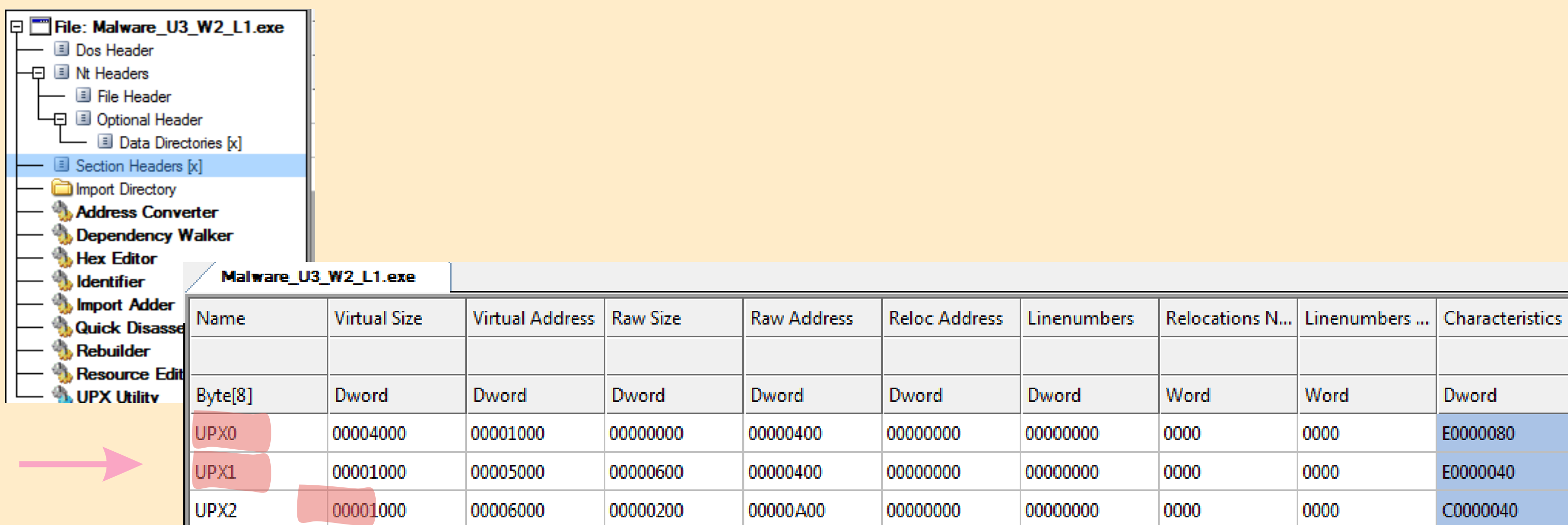


Malware_U3_W2_L1.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

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

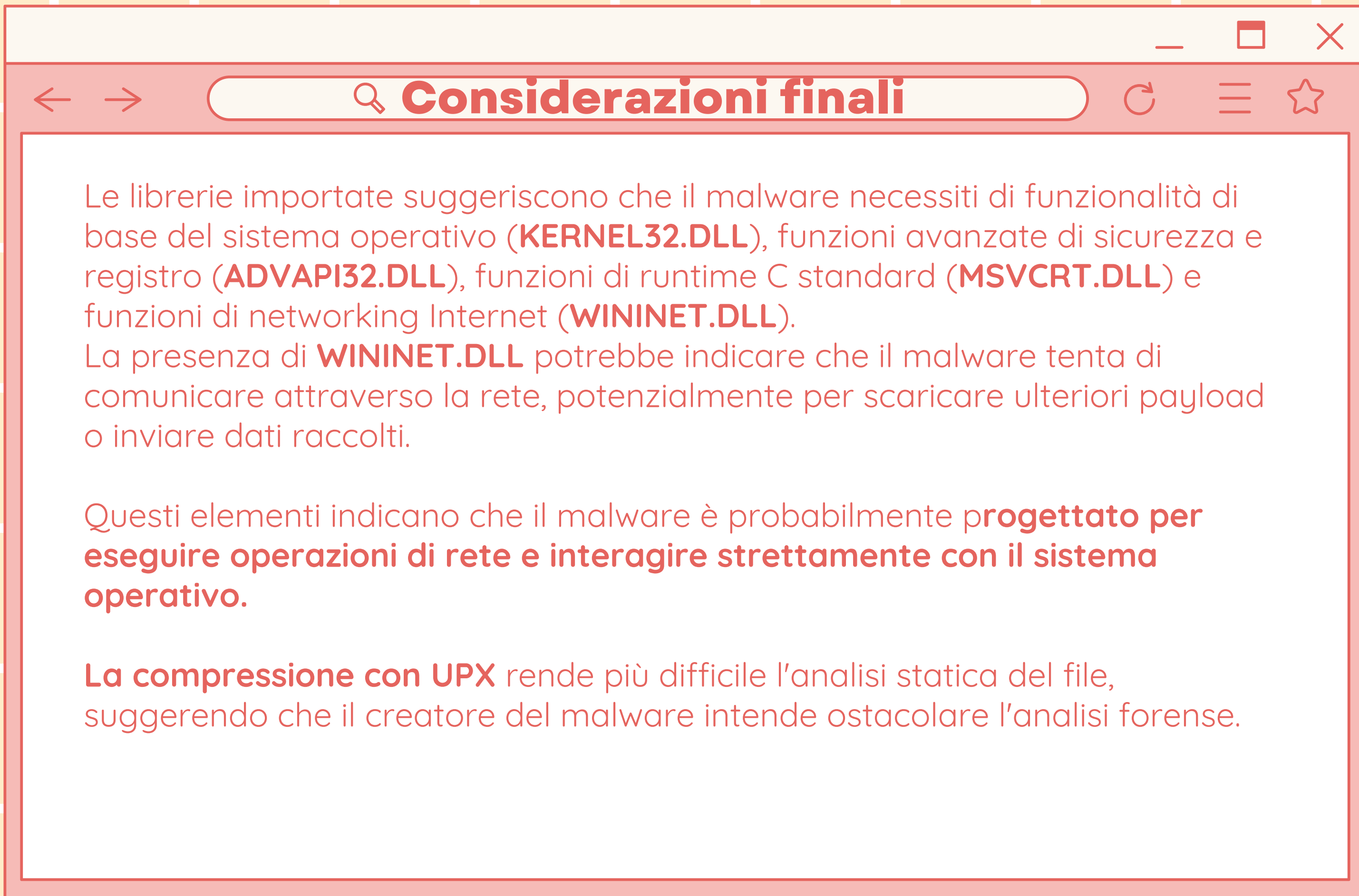
Sezioni

Andando nel menu “**Section header**” si può notare che il malware è composto da **3 sezioni**, che in questo caso però, non ci danno nessuna informazione utile, perché sono state evidentemente rinominate dal creatore del malware e quindi risulta difficile capire che tipo di sezioni siano.



The screenshot shows a malware analysis tool interface. On the left, a tree view under 'File: Malware_U3_W2_L1.exe' has 'Section Headers [x]' selected, indicated by a pink arrow. Below this, a table titled 'Malware_U3_W2_L1.exe' displays the details of the sections. The table has columns: Name, Virtual Size, Virtual Address, Raw Size, Raw Address, Reloc Address, Linenumbers, Relocations N..., Linenumbers ..., and Characteristics. Three sections are listed: UPX0, UPX1, and UPX2, each with a red highlight on its name. A pink arrow points from the 'Section Headers [x]' entry to the table.

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
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

Le librerie importate suggeriscono che il malware necessiti di funzionalità di base del sistema operativo (**KERNEL32.DLL**), funzioni avanzate di sicurezza e registro (**ADVAPI32.DLL**), funzioni di runtime C standard (**MSVCRT.DLL**) e funzioni di networking Internet (**WININET.DLL**).

La presenza di **WININET.DLL** potrebbe indicare che il malware tenta di comunicare attraverso la rete, potenzialmente per scaricare ulteriori payload o inviare dati raccolti.

Questi elementi indicano che il malware è probabilmente **progettato per eseguire operazioni di rete e interagire strettamente con il sistema operativo**.

La compressione con UPX rende più difficile l'analisi statica del file, suggerendo che il creatore del malware intende ostacolare l'analisi forense.