

**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:**

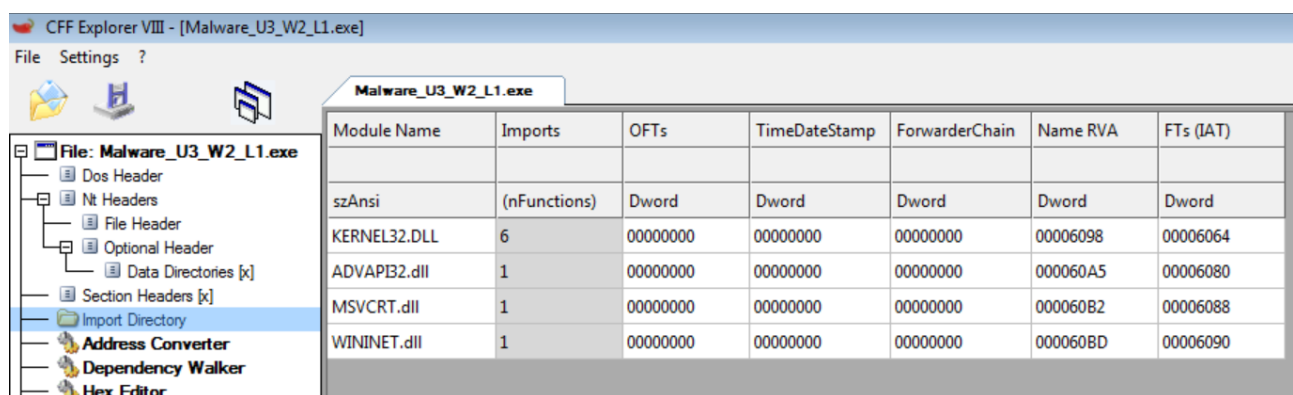
**a. Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse:**

Il sistema operativo Windows utilizza principalmente il formato **PE (Portable Executable)** per i file eseguibili. Questo formato include informazioni essenziali per il sistema operativo al fine di gestire il codice del file, come le librerie. Le **librerie**, o moduli, contengono un insieme di funzioni. Quando un programma necessita di una funzione, richiama una libreria in cui è definita tale funzione. Questo processo è noto come importazione di una libreria.

Le librerie e le funzioni possono essere importate in tre modi diversi dagli eseguibili:

- **Importazione statica:** in questo caso, l'eseguibile incorpora completamente il contenuto della libreria nel proprio codice. Ad esempio, se un programma denominato "SOMMA" utilizza una libreria, copierà l'intero contenuto della libreria, inclusa la definizione di funzioni come la sottrazione, la divisione e il modulo, anche se non sono utilizzate. Questo approccio aumenta la dimensione del file e complica l'analisi statica avanzata, poiché è difficile distinguere il codice della libreria dal codice dell'eseguibile.
- **Importazione a tempo di esecuzione (runtime):** in questo caso, l'eseguibile richiama la libreria solo quando ha bisogno di una specifica funzione. Questo comportamento è comunemente utilizzato dai malware per ridurre la loro rilevabilità e invasività. Per chiamare la libreria solo quando necessario, vengono utilizzate funzioni fornite dal sistema operativo come "LoadLibrary" e "GetProcAddress".
- **Importazione dinamica:** questo è il metodo più interessante per gli analisti di sicurezza ed è anche il più diffuso. Le librerie importate dinamicamente vengono caricate dal sistema operativo quando l'eseguibile viene avviato. Le funzioni all'interno della libreria vengono chiamate ed eseguite solo quando necessario.

Le librerie importate dal malware «Esercizio\_Pratico\_U3\_W2\_L1» sono le seguenti:

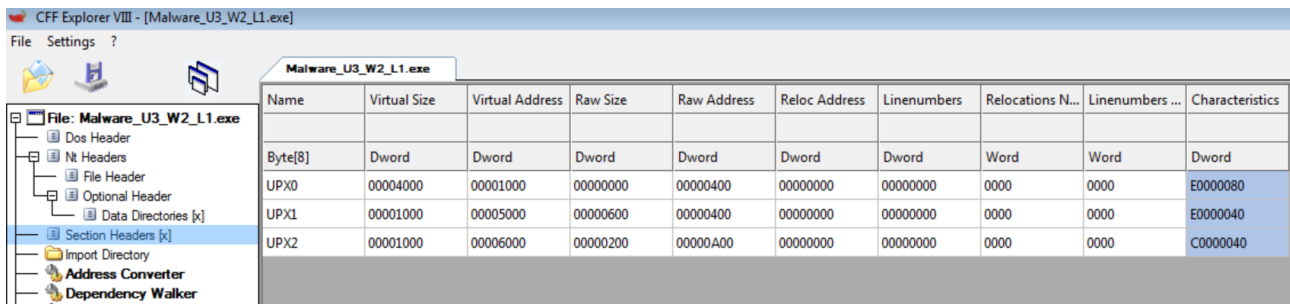


Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll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

- **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.

**b. Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di esse:**

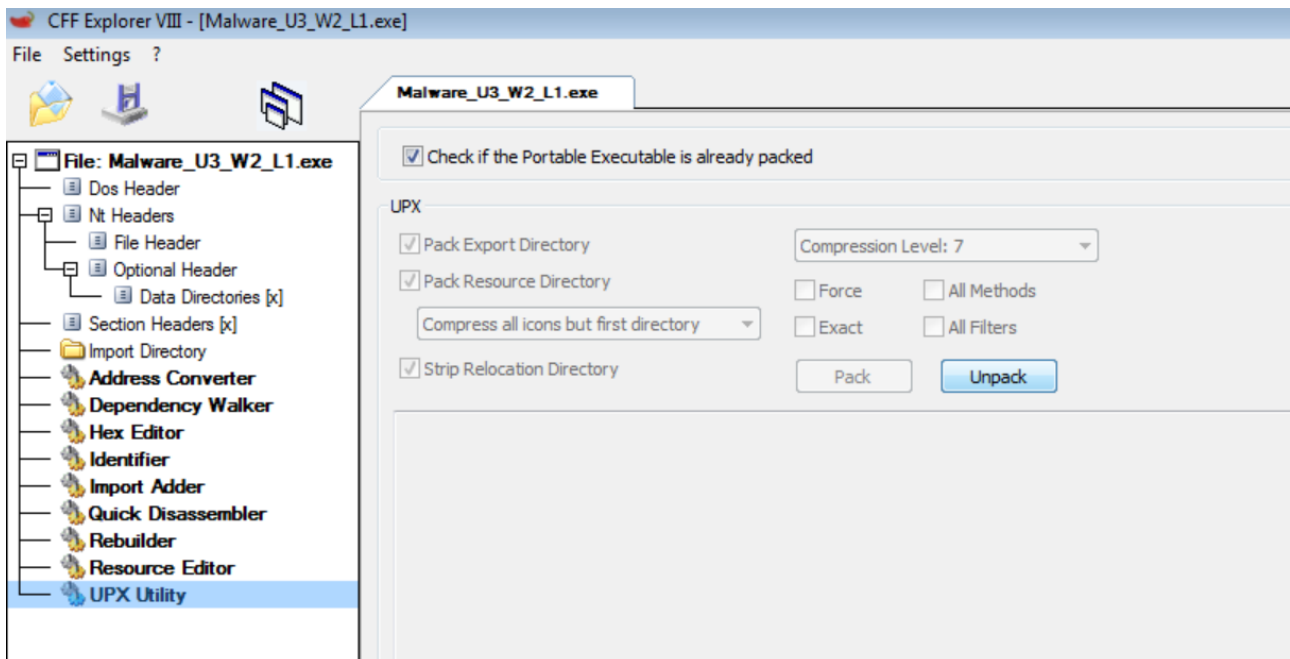


Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

Le sezioni di cui si compone il malware, inizialmente non erano visibili, in quanto erano compresse con UPX.

**UPX** è un programma utilizzato per comprimere eseguibili, incluso il codice malevolo, al fine di ridurre le dimensioni del file e rendere più difficile la sua individuazione e analisi da parte degli antivirus e degli analisti della sicurezza informatica. Ad esempio la sezione UPX0 indica che il file è stato compresso con UPX e potrebbe essere un segnale che il file potrebbe contenere del codice dannoso.

Allora sono andato su UPX Utility e ho cliccato "Unpack":



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
.text	000002DC	00001000	00001000	00001000	00000000	00000000	0000	0000	60000020
.rdata	00000372	00002000	00001000	00002000	00000000	00000000	0000	0000	40000040
.data	0000008C	00003000	00001000	00003000	00000000	00000000	0000	0000	C0000040

Ritornando su “Section Headers”, noto come ora le Sezioni sono visibili in chiaro.

- **.text**: contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto.
- **.rdata**: include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer.
- **.data**: contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma. Una variabile si dice globale quando non è definita all'interno di un contesto di una funzione, ma bensì è globalmente dichiarata ed è di conseguenza accessibile da qualsiasi funzione all'interno dell'eseguibile.

### c. Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte:

Le librerie importate indicano che il malware ha accesso a funzionalità cruciali del sistema operativo, come la manipolazione dei file, la gestione della memoria, l'interazione con i servizi di sistema e i registri, nonché la comunicazione attraverso protocolli di rete come HTTP, FTP e NTP. Questo suggerisce che il malware potrebbe essere in grado di eseguire varie azioni dannose, come il download di ulteriori componenti dannosi, l'filtrazione di dati sensibili o la creazione di backdoor nel sistema.

Le sezioni del malware indicano una struttura tipica di un eseguibile, con una sezione .text contenente le istruzioni eseguibili, una sezione .rdata contenente informazioni sulle librerie importate ed esportate, e una sezione .data contenente dati e variabili globali. Questa struttura suggerisce che il malware è stato progettato con una certa complessità e che è in grado di operare in modo sofisticato.

Considerando l'accesso alle funzionalità del sistema operativo e la struttura complessa del malware, è probabile che questo rappresenti una minaccia significativa per la sicurezza del sistema. Potrebbe essere in grado di causare danni importanti, come la compromissione dei dati, il danneggiamento del sistema operativo o l'installazione di altri malware.