

## 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

## Librerie importate dal malware:

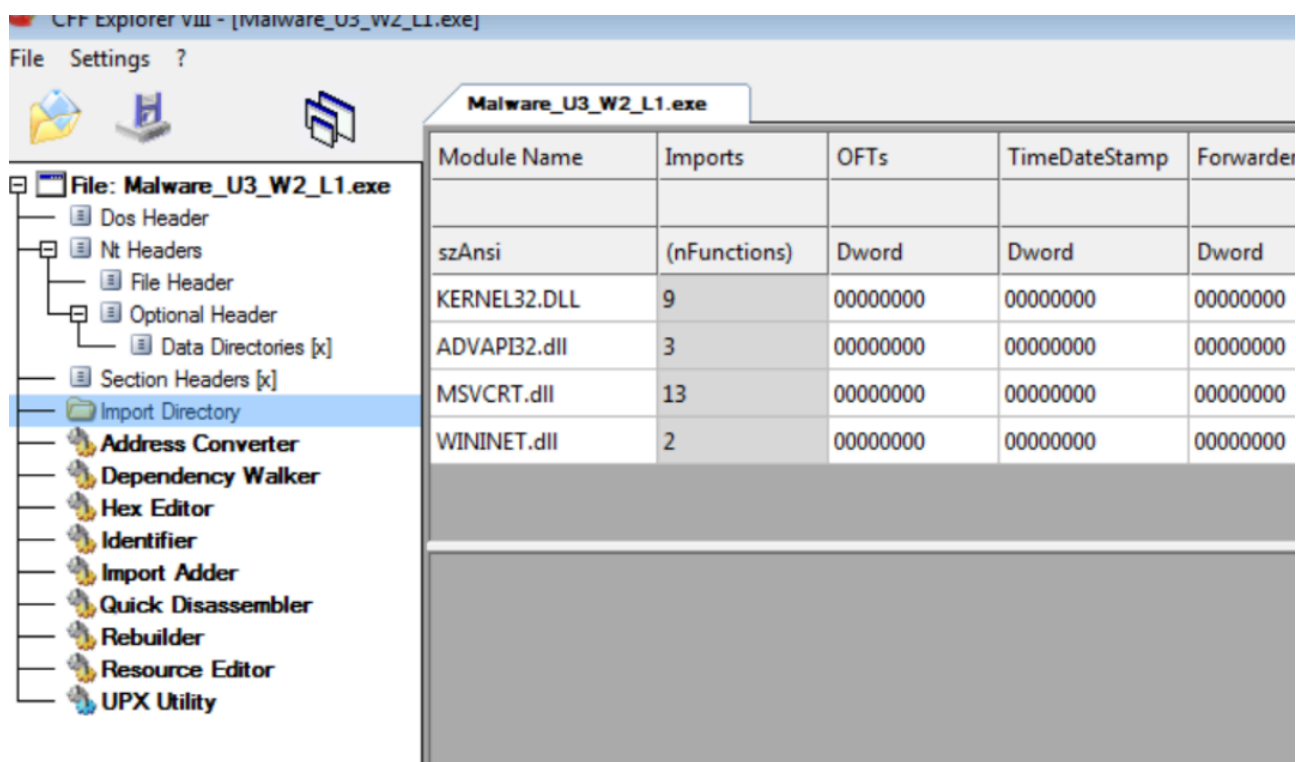
**Kernel32.dll:** La libreria "kernel32.dll" è una parte fondamentale del sistema operativo Microsoft Windows. Essa contiene molte funzioni di base del kernel del sistema operativo, come la gestione della memoria, la gestione dei processi e delle thread, le operazioni di input/output, la gestione degli errori e altre funzioni essenziali per il funzionamento del sistema.

**Advapi32.dll:** La libreria "advapi32.dll" è un'altra libreria di sistema essenziale nei sistemi operativi Microsoft Windows. Questa DLL fornisce funzioni avanzate per la gestione della sicurezza, la gestione dei servizi, la gestione degli account utente, la crittografia e altre operazioni relative alla sicurezza e all'amministrazione del sistema.

**Msvcrt.dll:** La libreria "msvcrt.dll" (Microsoft C Runtime Library) è una libreria dinamica di runtime fornita da Microsoft. Essa contiene funzioni di supporto e servizi utilizzati dai programmi scritti in linguaggio di programmazione C che sono stati compilati con il compilatore Microsoft Visual C++.

La libreria svolge un ruolo cruciale nell'esecuzione di programmi C su sistemi Windows.

**Wininet.dll:** La libreria "wininet.dll" (Windows Internet API) è una libreria di sistema di Microsoft Windows che fornisce un'interfaccia di programmazione per l'accesso a risorse Internet. Questa DLL contiene funzioni che consentono alle applicazioni Windows di eseguire operazioni di rete, come la gestione delle connessioni Internet, il recupero di risorse da server Web, l'invio di richieste HTTP, la gestione dei cookie, e altro ancora.



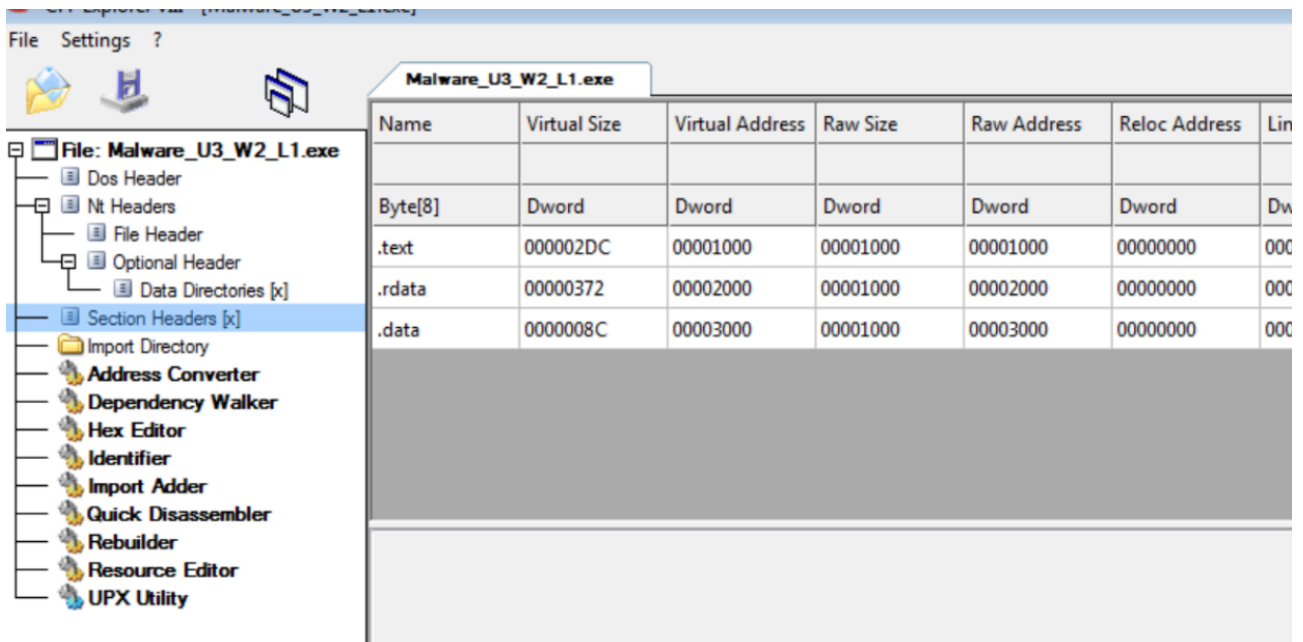
Module Name	Imports	OFTs	TimeStamp	Forwarder
szAnsi	(nFunctions)	Dword	Dword	Dword
KERNEL32.DLL	9	00000000	00000000	00000000
ADVAPI32.dll	3	00000000	00000000	00000000
MSVCRT.dll	13	00000000	00000000	00000000
WININET.dll	2	00000000	00000000	00000000

## Sezioni di cui si compone il malware:

**.text:** contiene il codice eseguibile e si tratta in genere dell'unica sezione che contiene codice

**.rdata:** contiene informazioni sull'import e l'export e può contenere anche altri dati read only;

**.data:** contiene i dati globali, cioè quelli che possono essere acceduti da ogni punto del programma



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Lin
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dw
.text	000002DC	00001000	00001000	00001000	00000000	000
.rdata	00000372	00002000	00001000	00002000	00000000	000
.data	0000008C	00003000	00001000	00003000	00000000	000

## Considerazioni finali sul malware

Tramite l'analisi su off possiamo dedurre che questo malware opera a livello del sistema operativo tramite la libreria kernel32.dll dalla quale può lanciare altri malware o comandi malevoli, può inoltre fungere da spyware controllando le altre librerie windows che richiama come da analisi iniziale. Grazie al controllo effettuato sul sito virustotal.com evinciamo che si tratta di un trojan.