CONSEGNA S10/L1

di Giuseppe Lupoi

INDICE

TRACCIA

Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi statica basica.

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:

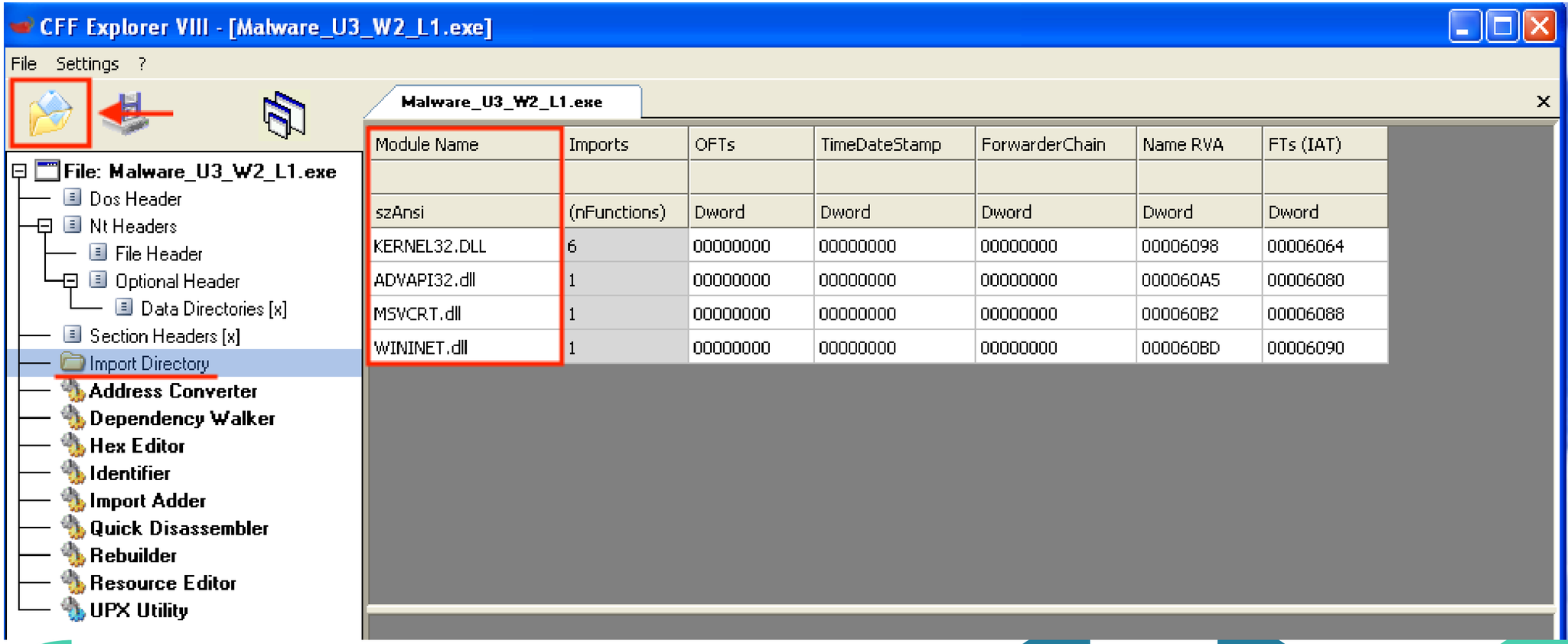
- Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse
- Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

Per procedere con il primo punto della pratica di oggi, una volta avviata la macchina a noi fornita ovvero **Malware Analysis** faremo doppio click sul tool **CFF Explorer** per avviarlo. Clicchiamo dunque sulla cartella in alto a sinistra indicata dal quadrato rosso per scegliere il file malware da analizzare, apriamo dunque **Malware_U3_W2_L1.exe.**

Nella lista delle voci a sinistra dell'immagine spostiamoci su "**Import Directory**" mentre sul rettangolo di destra ci verranno infine mostrate le **librerie utilizzate dal malware in questione**.

Possiamo notare:

- KERNEL32.DLL
- ADVAPI32.dll
- MSVCRT.dll
- WININET.dll

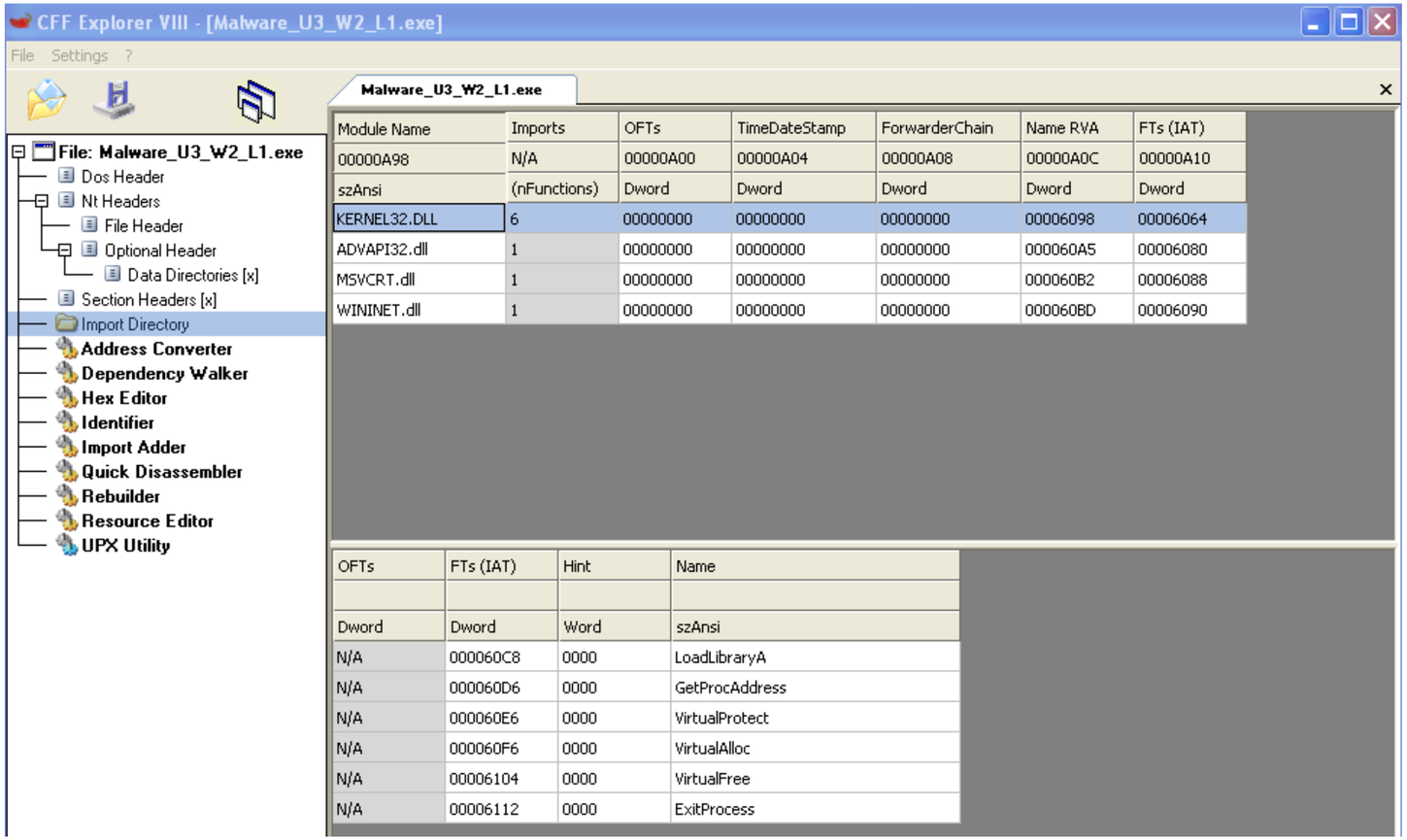


Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088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

Le analizzeremo di seguito una ad una.

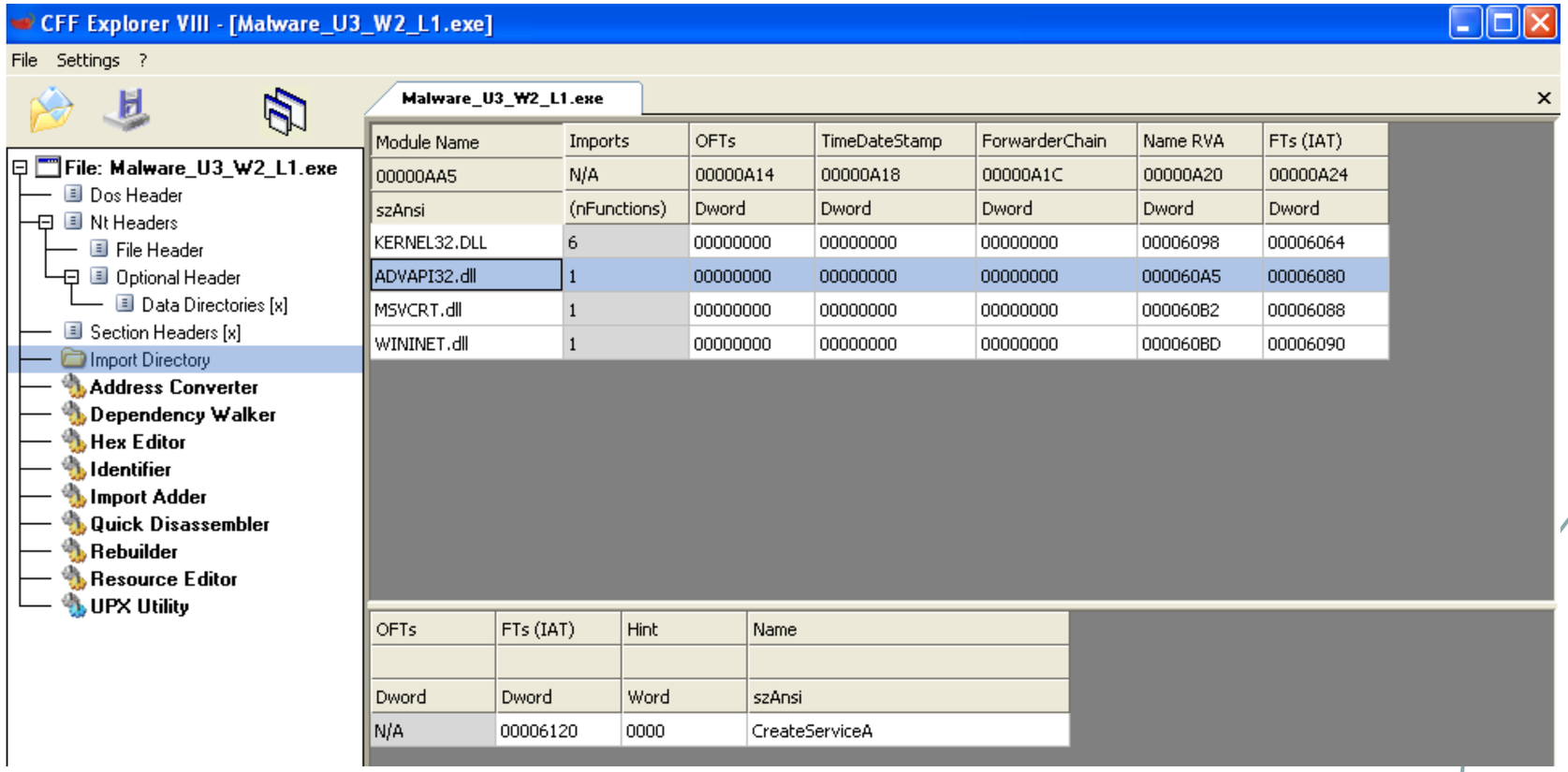
Partiamo dalla prima ovvero **KERNEL32.DLL**.

KERNEL32.DLL è una libreria tipicamente comune da utilizzare in quanto contiene funzioni principali che permettono di interagire con il sistema operativo, ad esempio permette di manipolare file e gestire la memoria.

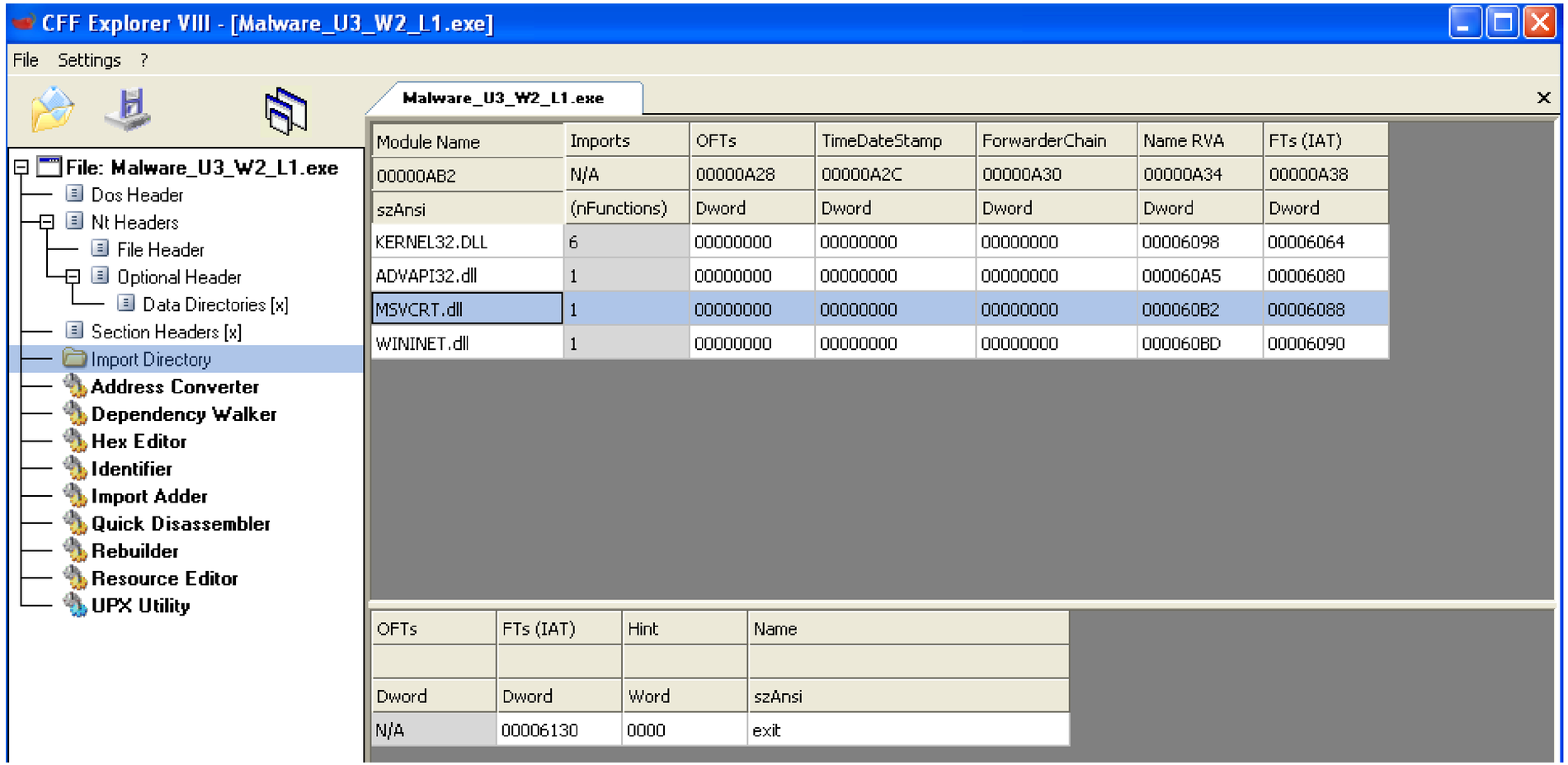


La seconda che analizzeremo sarà **ADVAPI32.dll**.

ADVAPI32.dll è una libreria contenete funzioni che permettono di interagire con i servizi ed i registri del sistema operativo Microsoft.
Il Registro di sistema di Windows viene utilizzato per gestire e modificare le impostazioni relative alle preferenze dell'utente e alla configurazione del sistema.
Il Registro di sistema potrebbe contenere file residui di programmi che non usi più.

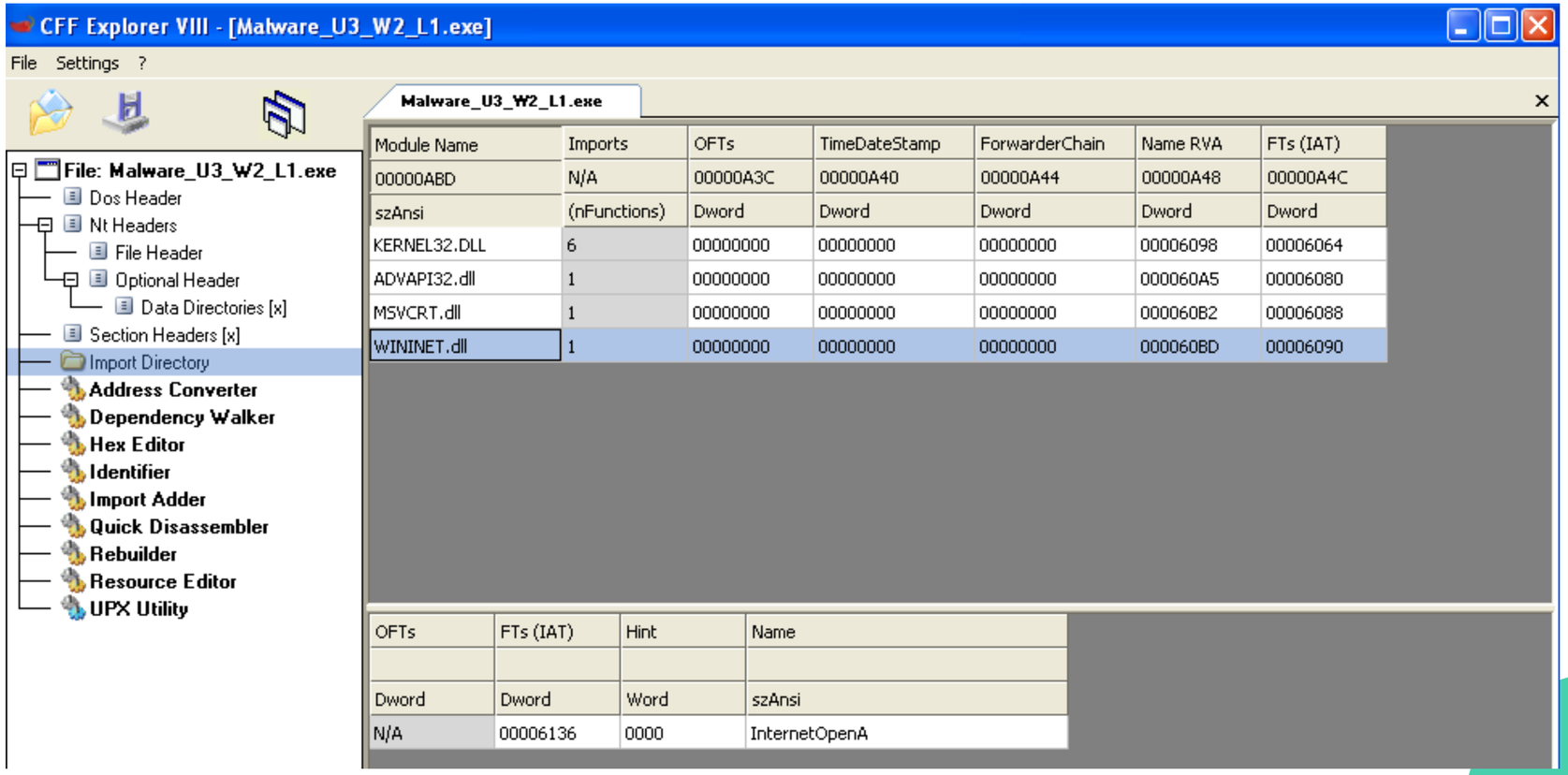


Continuiamo con la libraria **MSVCRT.dll** contenente funzioni per la manipolazione di stringhe, allocazione di memoria oppure può effettuare chiamate per input/output in stile linguaggio C.



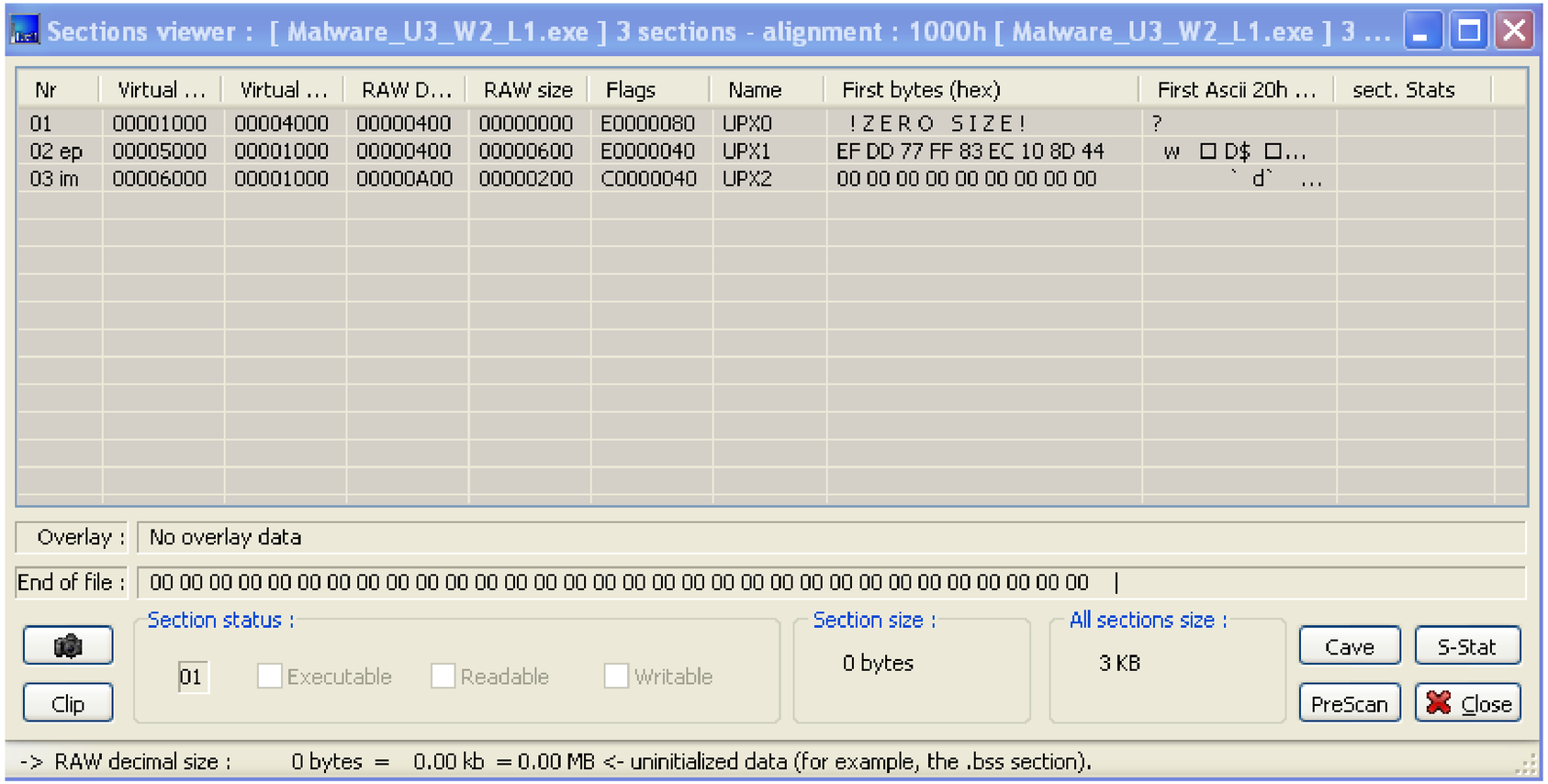
Concludiamo infine con l'ultima libreria **WININET.dll**, una libreria con funzioni che permettono l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Indicherà quindi alla **DLL** Internet di inizializzare le strutture di dati interne e prepararsi per le chiamate future dall'applicazione.
Al termine dell'uso delle funzioni Internet, l'applicazione deve chiamare **InternetCloseHandle** per liberare l'handle e le risorse associate.



Passiamo al secondo punto della traccia, andremo quindi ad analizzare le sezioni da cui il malware è composto.
Dalle scansioni effettuate con i tool **CFF Explorer** ed **ExeInfoPE** troviamo:

- UPX0
- UPX1
- UPX2



Analizzando le sezioni e facendo una ricerca capiamo che:

UPX (Ultimate Packer for eXecutables) è uno strumento di compressione e decompressione per eseguibili, progettato per ridurre le dimensioni dei file eseguibili.
UPX può essere utilizzato legalmente per comprimere e decomprimere file, ma può anche essere utilizzato da malware per nascondere il proprio codice o per rendere più difficile la rilevazione da parte dei software di sicurezza.
Le "sezioni" di un file eseguibile si riferiscono alle diverse parti che compongono il file, come la sezione del codice, la sezione dei dati, ecc. Alcuni malware potrebbero utilizzare tecniche come la compressione UPX per rendere più complesso l'analisi e la rilevazione.

Da ciò possiamo dedurre che il malware ha compresso o decompresso dei file per ridurne il volume.
Deduciamo anche che il processo è stato attuato 3 volte chiamate appunto UPX0, UPX1, UPX2.

CONSIDERAZIONE FINALE

Possiamo quindi provare a dedurre dalle scansioni effettuate in precedenza che il malware in questione stia utilizzando delle librerie e delle funzioni per connettersi ad internet e scaricare altri malware che intaccheranno il sistema operativo e le locazioni della memoria.