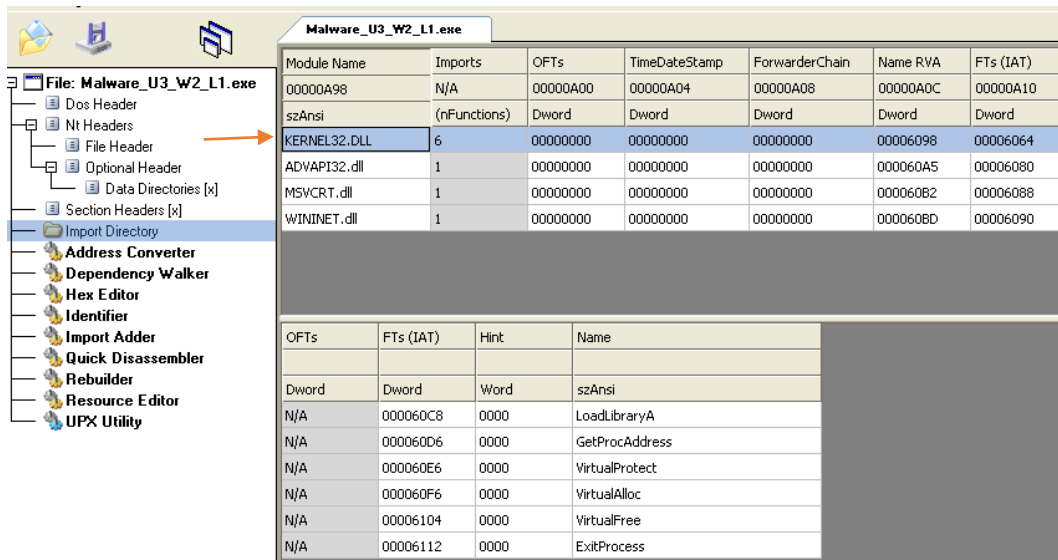


Esercizio Pratico U3 W2 L1

Programma usato CFF Explorer.

1. Librerie importate dal malware:

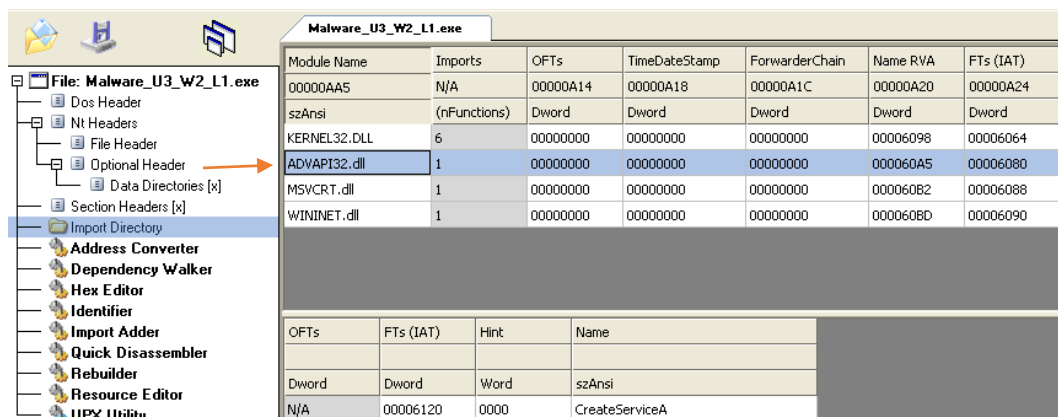
- **Kernerl32.dll**: contiene funzioni principali per interagire con il sistema operativo, inclusa la manipolazione dei file e la gestione della memoria. Un malware potrebbe utilizzare queste funzioni per accedere, modificare o eliminare file sul sistema, caricare o scaricare altri componenti del malware in memoria e sfruttare vulnerabilità nel sistema operativo.



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
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	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

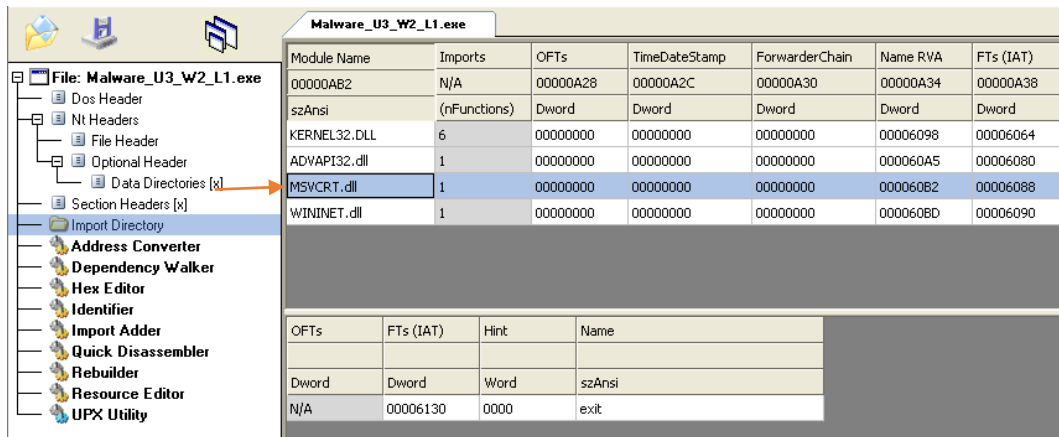
- **Advapi32.dll**: contiene funzioni per interagire con i servizi e i registri del sistema operativo Microsoft. Un malware potrebbe utilizzare queste funzioni per creare, modificare o eliminare servizi sul sistema, accedere o modificare le chiavi di registro, eseguire azioni di persistenza per sopravvivere ai riavvii del sistema e svolgere altre attività dannose.



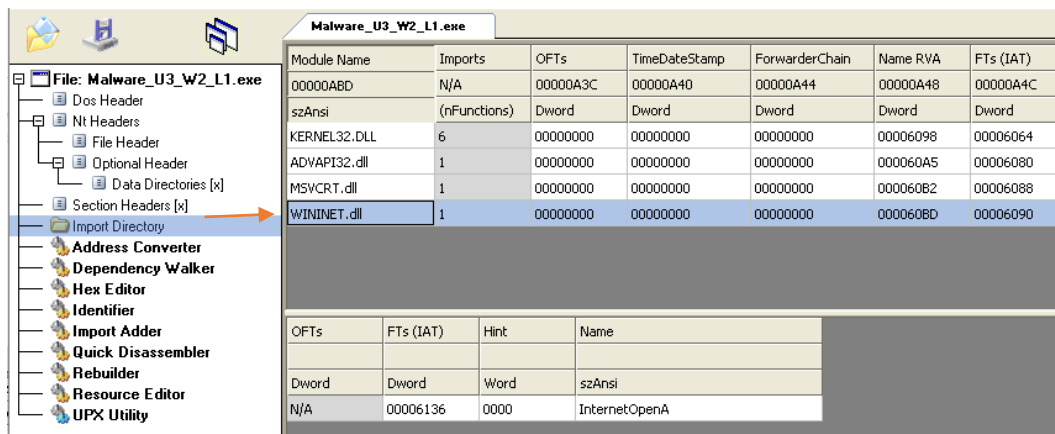
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000AA5	N/A	00000A14	00000A18	00000A1C	00000A20	00000A24
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
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	00006120	0000	CreateServiceA

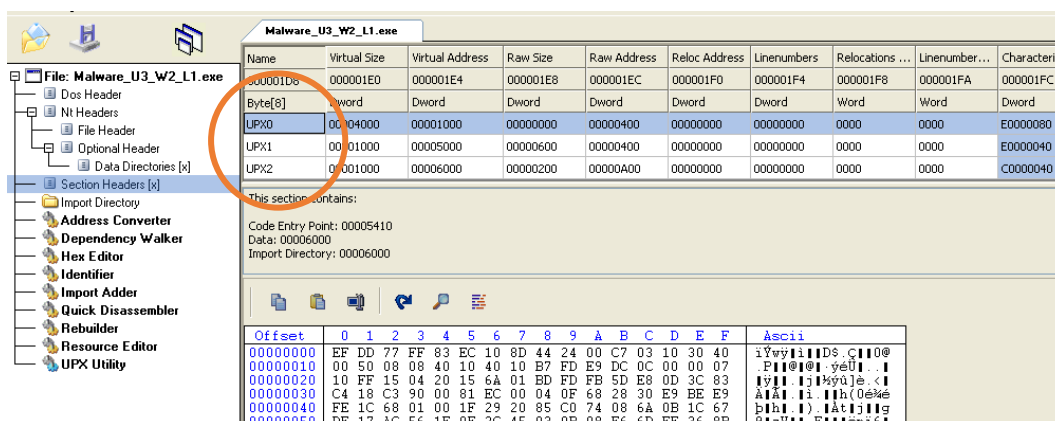
- **MSVCRT.dll**: contiene funzioni per la manipolazione delle stringhe, l'allocazione della memoria e altre operazioni di input/output, simili a quelle presenti nel linguaggio C. Un malware potrebbe utilizzare queste funzioni per eseguire operazioni di manipolazione dei dati, crittografia, decrittografia o per comunicare con server di comando e controllo.

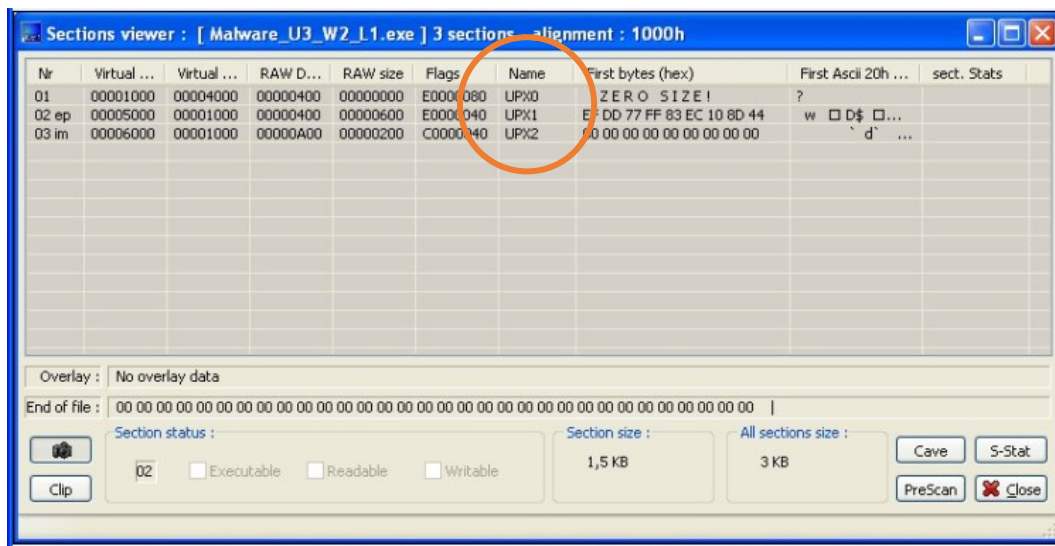


- **Wininet.dll**: contiene funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP e NTP. Un malware potrebbe utilizzare queste funzioni per comunicare con server remoti, ad esempio per scaricare altri componenti del malware, inviare dati rubati o ricevere istruzioni dal server di comando e controllo.



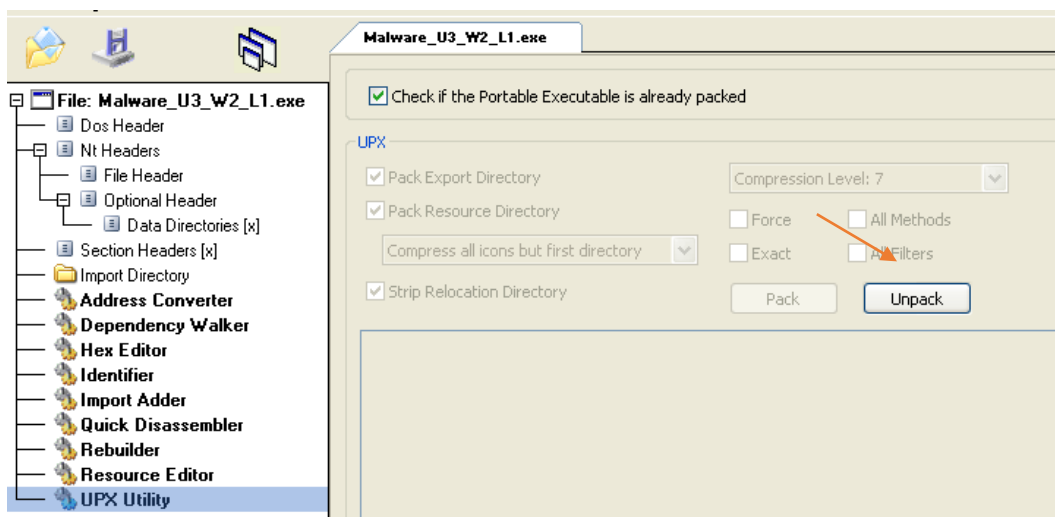
- In questo caso invece di avere il tipo di file visibile, .data .text .rdata .src, abbiamo **UPX0 UPX1 UPX2** che sono usati da UPX per memorizzare i dati compressi, le informazioni di decompressione e altre risorse necessarie per ripristinare il file originale, durante l'esecuzione del file in analisi UPX decodifica queste sezioni e restituisce il funzionamento normale dell'applicazione. Anche usando ExeinfoPE abbiamo le stesse sezioni.





Usando UPX Utility andiamo a fare **Unpack**, quindi adesso abbiamo:

- **.text**: Questa sezione contiene le istruzioni del programma che la CPU eseguirà una volta che il software sarà avviato. Contiene il codice eseguibile, ovvero le istruzioni che definiscono il comportamento del programma. È l'unica sezione che viene effettivamente eseguita dalla CPU.
- **.rdata**: Questa sezione, abbreviazione di "read-only data" (dati di sola lettura), contiene informazioni costanti o dati di sola lettura che il programma utilizza durante l'esecuzione. Ad esempio, può includere stringhe di testo, tabelle di costanti o altre informazioni che non devono essere modificate durante l'esecuzione del programma.
- **.data**: Questa sezione contiene dati e variabili globali del programma eseguibile che devono essere accessibili da qualsiasi parte del programma. Questi dati possono essere modificati durante l'esecuzione del programma. Ad esempio, potrebbe includere variabili globali, strutture dati o altri dati inizializzati dal programma.



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteris
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

3. Con solo queste informazioni disponibili osserviamo che il malware è progettato per svolgere un'ampia gamma di attività dannose, tra cui manipolazione dei file, modifica delle impostazioni del sistema, comunicazione remota e possibilmente anche l'esecuzione di azioni di persistenza per mantenere una presenza prolungata sul sistema infetto. Alcune delle funzionalità suggerite dalle librerie importate potrebbero essere indicative di un tipo di malware polivalente e avanzato, un malware di tipo backdoor o Trojan, in grado di infiltrarsi nel sistema, creare una presenza persistente e consentire l'accesso remoto al sistema compromesso.