

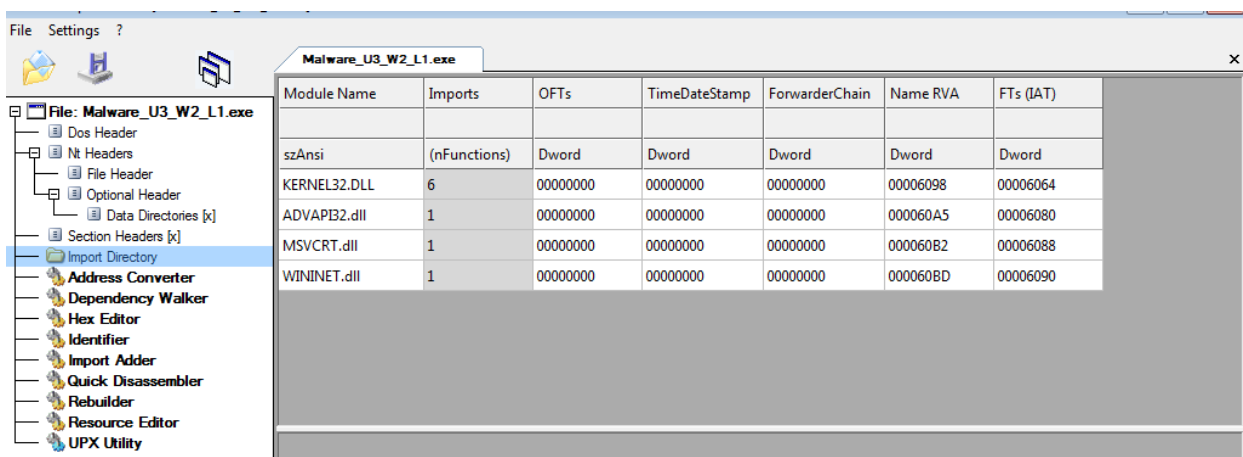
ESERCITAZIONE S10 L1

Analisi statica basica

1. LIBRERIE IMPORTATE
2. SEZIONI MALWARE
3. CONSIDERAZIONI FINALI

1. LIBRERIE IMPORTATE

Attraverso l'utilizzo del programma *CFF EXPLORER* possiamo effettuare una prima analisi del malware.



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

Andando nella sezione *Import Directory*, possiamo analizzare le directory utilizzare dal malware, così da poter dedurre alcune funzioni.

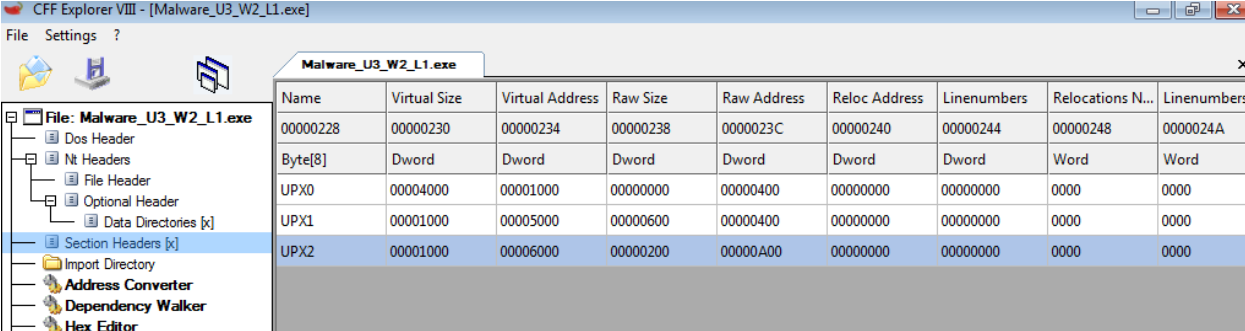
- **Kernel32.dll** è una libreria di sistema essenziale in ambienti Windows che fornisce funzioni fondamentali per la gestione della memoria, dei file, degli errori e dei processi. È cruciale per il corretto funzionamento dei programmi su piattaforma Windows.
- **Advapi32.dll** è una libreria che fornisce funzioni avanzate per la gestione della sicurezza, la manipolazione dei servizi di sistema, la registrazione degli eventi e altre operazioni critiche. Essa è

fondamentale per il corretto funzionamento di diversi programmi su un sistema Windows.

- **Msvcrt.dll** è una libreria associata al compilatore Microsoft Visual C++. Fornisce funzioni di **runtime** per programmi scritti in linguaggio C/C++, comprendendo operazioni di gestione della memoria, manipolazione delle stringhe e altre funzioni di supporto. La sua presenza è cruciale per garantire la corretta esecuzione di applicazioni che dipendono da questa libreria di runtime.
- **Wininet.dll** è una libreria di sistema su piattaforme Windows dedicata alla gestione delle operazioni di rete e della connettività Internet. Essa fornisce funzionalità cruciali per applicazioni come browser web e altri programmi che richiedono l'accesso a risorse online.

2. SEZIONE MALWARE

Sempre dalla sezione di sinistra di *FCC EXPLORER*, spostandoci in *Section Headers*, possiamo visualizzare le sezioni di cui si compone il *Malware*.



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers
00000228	00000230	00000234	00000238	0000023C	00000240	00000244	00000248	0000024A
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000

Si possono notare 3 sezioni:

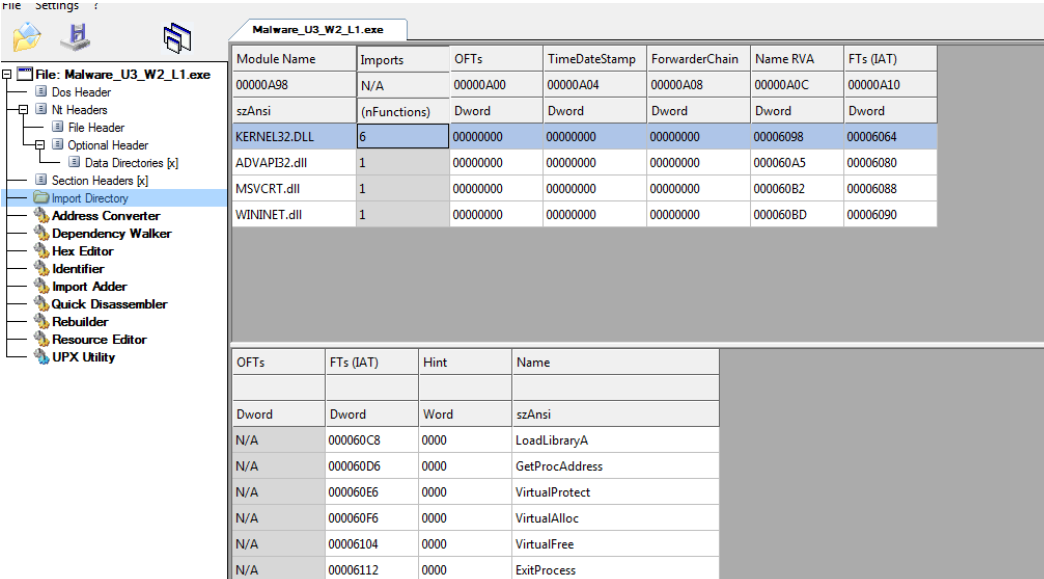
- UPX0
- UPX1
- UPX2

Sembra che il malware abbia nascosto il nome originale delle sezioni, quindi non siamo in grado di identificare le sezioni.

3. CONSIDERAZIONI FINALI

Si tratta sicuramente di un malware abbastanza avanzato, in quanto cerca di nascondere più informazioni possibili sul suo comportamento.

Tuttavia, analizzando nello specifico le librerie, troviamo *Load Library* e *Get Process Address*, che suggeriscono un caricamento in **runtime** delle librerie, nascondendo quindi quelle che va ad utilizzare.



The screenshot shows the Immunity Debugger interface. The left pane displays the file structure for 'Malware_U3_W2_L1.exe', with 'Import Directory' selected. The main pane shows a table of imported modules and functions.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000A98	N/A	0000A00	0000A04	0000A08	0000A0C	0000A10
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