

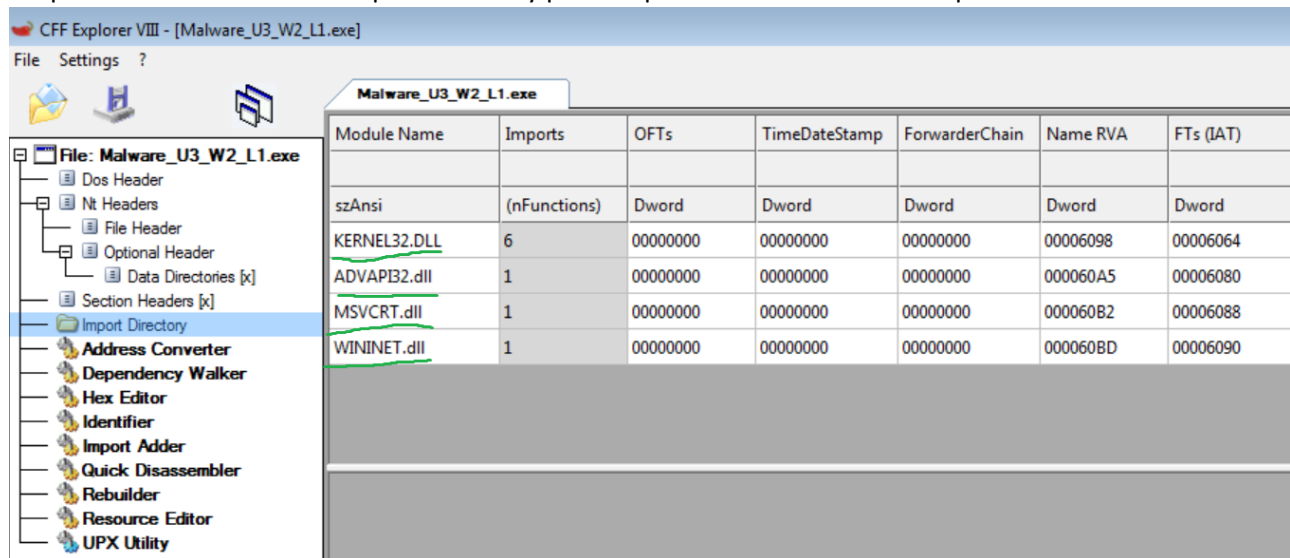
Nell'esercizio di oggi ci viene chiesto di analizzare un malware; in particolare:

- 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

LIBRERIE IMPORATE DAL MALWARE

Apriamo, dunque, "CFF explorer", particolarmente adatto per analizzare nel dettaglio la struttura interna dei file PE. Apriamo il malware e cominciamo ad analizzarlo. La maggior parte dei malware esegue **Dinamicamente** le librerie all'interno del suo codice (ovvero le librerie non vengono importate all'interno del codice ma vengono richiamate solo quando il file è in esecuzione); in questo modo sarà più facile, per i malware, aggirare controlli come antivirus.

Ci spostiamo nella sezione "import Directory per comprendere se il malware importa librerie remote.



CFF Explorer V8.1.1 - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

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

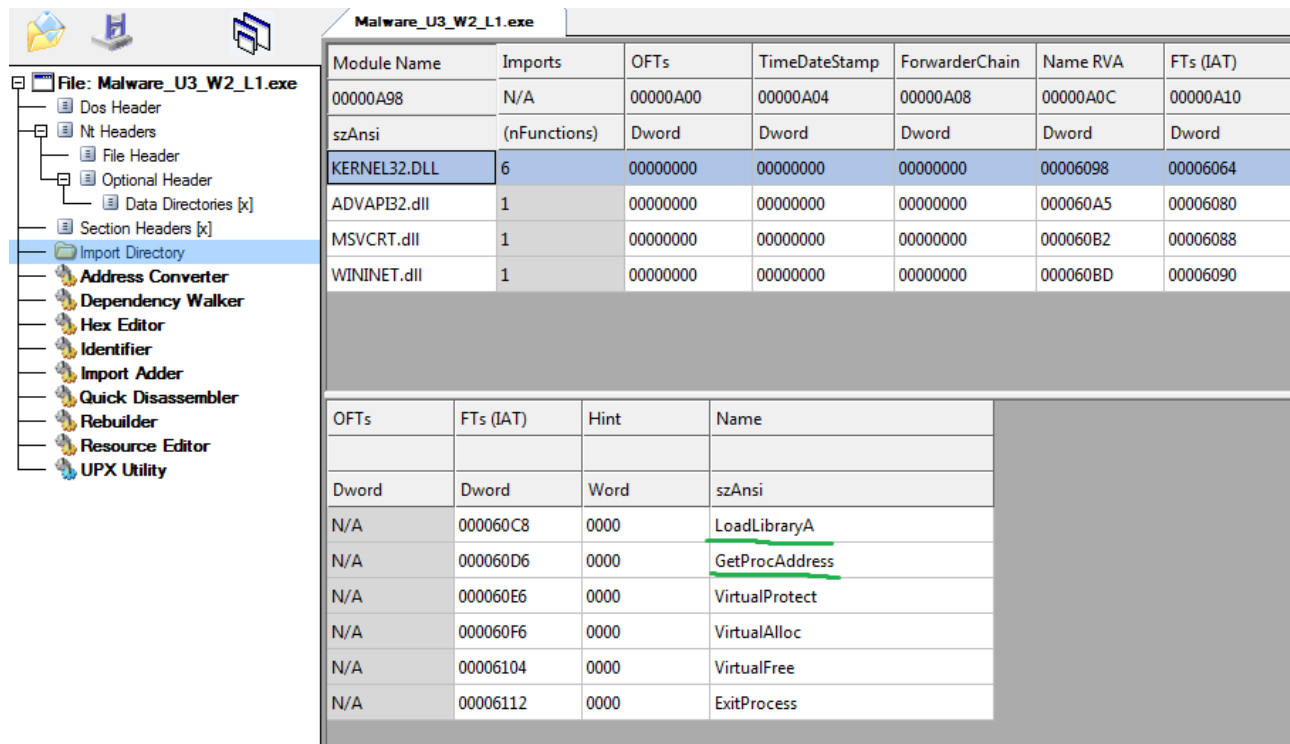
File: Malware_U3_W2_L1.exe

- Dos Header
- Nt Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

In effetti ci sono 4 librerie sospette; queste, in particolare hanno lo scopo di:

- Kernel32.dll**: interagisce con il sistema operativo e gestisce (anche impropriamente) la memoria e le risorse del sistema operativo.
- Advapi32.dll**: contiene informazioni per manipolare il sistema operativo
- MSVCRT.dll**: Contiene informazioni sulla manipolazione di stringhe e allocazione di memoria
- Wininet.dll**: permette alle applicazioni di interagire con protocolli come HTTP, HTTPS ed FTP.

Inoltre, analizzando le librerie, ci accorgiamo che in esse sono presenti le funzioni **“LoadLibrary”** e **“GetProcAddress”**.



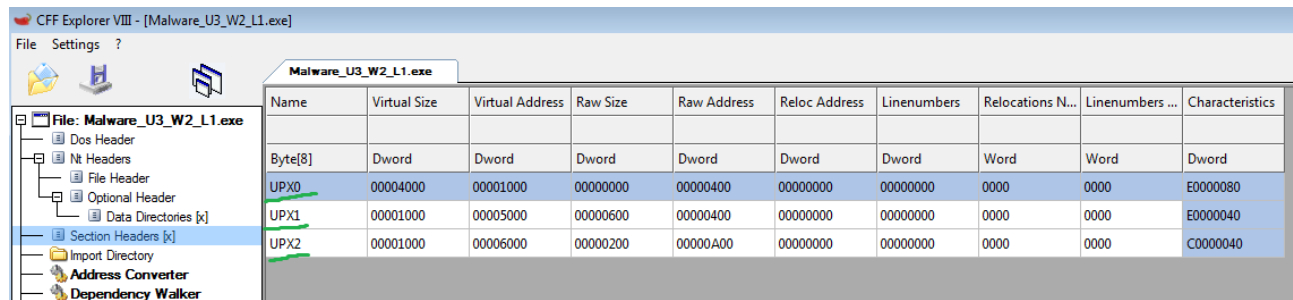
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
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

La presenza di questi file dovrebbe quantomeno allertarci, poiché si tratta proprio delle funzioni utilizzate per richiamare librerie da remoto (cioè dinamicamente) ed aggirare software anti-malware.

SEZIONI DEL MALWARE

Nella sezione “Section Headers” analizziamo da quali parti è composto il malware.



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

Il malware sembra essere composto da 3 sezioni: **UPX0**, **UPX1**, **UPX2**. Generalmente, si passa ad analizzare le sezioni del malware per rilevare file di comportamento del programma; in particolare:

- “.text”: contiene informazioni sulla parte di memoria che verrà usata durante l’esecuzione del programma
- “.rdata”: contiene informazioni sulle librerie importate ed esportate del malware
- “.data”: contiene informazioni sulle variabili globali del sistema
- “.rsrc”: include informazioni sui file non eseguibili(come foto e video) utilizzati dal malware

Sfortunatamente, però non ci vengono restituite ulteriori informazioni poiché il programma riesce a camuffare le sezioni di cui si compone.

CONCLUSIONI

Per concludere, possiamo dire di trovarci di fronte ad un malware che proprio a causa del suo livello di sofisticatezza ci impedisce di comprendere appieno come funziona solo tramite un’analisi statica basica; bisognerà, pertanto, passare ad effettuare ulteriori analisi.