

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

L'esercizio di oggi riguardava l'analisi di un malware, nello specifico tramite la tecnica dell'analisi statica, cioè senza eseguirlo.

Tramite l'utilizzo del tool CFF Explorer abbiamo individuato le librerie importate, come visibili nell'immagine seguente.

Malware_U3_W2_L1.exe					
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5
MSVCRT.dll	1	00000000	00000000	00000000	000060B2
WININET.dll	1	00000000	00000000	00000000	000060BD

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

Entrando nel dettaglio queste librerie servono:

- **KERNEL32:** è una componente fondamentale del sistema operativo e viene utilizzata per l'esecuzione di operazioni di basso livello come la creazione di processi, manipolazione di file e directory, accesso a risorse del sistema. Al suo interno vi sono funzioni come "LoadLibraryA" e "GetProcAddress" che serviranno a chiamare le librerie all'occorrenza, questa casistica è denominata importazione a tempo di esecuzione delle librerie;
- **ADVAPI31:** contiene le funzioni per interagire con i servizi e registri del sistema operativo;
- **MSVCRT:** contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate input/output, come nel linguaggio C;
- **WININET:** contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Successivamente abbiamo individuato le sezioni di cui si compone il malware:

Malware_U3_W2_L1.exe							X
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	R
00000228	00000230	00000234	00000238	0000023C	00000240	00000244	0
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	V
.text	000002DC	00001000	00001000	00001000	00000000	00000000	0
.rdata	00000372	00002000	00001000	00002000	00000000	00000000	0
.data	0000008C	00003000	00001000	00003000	00000000	00000000	0

- **.text:** contiene istruzioni che la CPU eseguirà una volta che il software sarà avviato;
- **.rdata:** contiene le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile;
- **.data:** contiene di solito i dati e le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

Il malware è un trojan downloader che potrebbe essere utilizzato per scaricare sulla vittima una Backdoor.