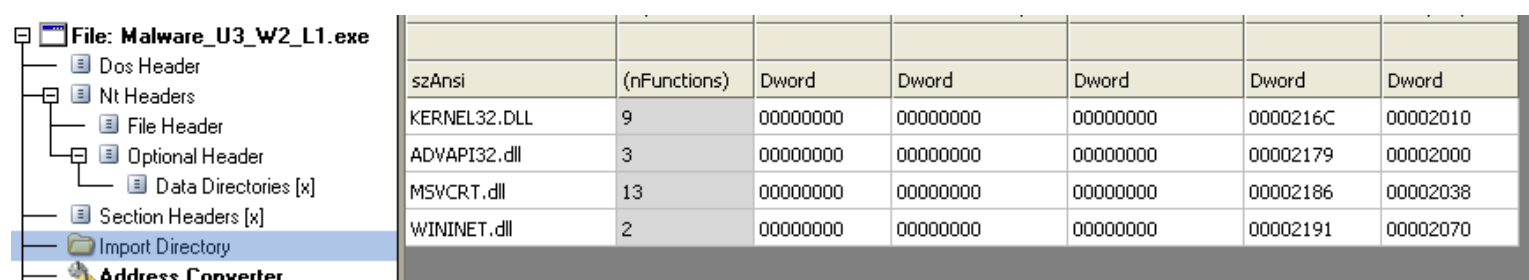


S10/L1

Nell'esercizio di oggi andremo ad eseguire un'analisi statica basica su un malware.

Come tool utilizzeremo CFF Explorer

Come possiamo vedere in figura il malware importa quattro librerie:



szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	9	00000000	00000000	00000000	0000216C	00002010
ADVAPI32.dll	3	00000000	00000000	00000000	00002179	00002000
MSVCRT.dll	13	00000000	00000000	00000000	00002186	00002038
WININET.dll	2	00000000	00000000	00000000	00002191	00002070

Spieghiamo cosa fanno queste librerie:

- **Kernel32.dll**

Libreria che contiene le funzioni principali per interagire col sistema operativo, come per esempio la manipolazione di file e la gestione della memoria.

- **Advapi32.dll**

Libreria che contiene le funzioni per interagire con i registri e i servizi del sistema operativo Microsoft.

- **MSVCRT.dll**

Libreria che contiene le funzioni per la manipolazione di stringhe, allocazione memoria e altro.

- **Wininet.dll**

Libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP e NTP.

Per vedere le sezioni di cui si compone il malware dobbiamo prima spaccettare le sezioni UPX e potremo vedere il seguente risultato:

	Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Relative Address	Relative Offset	Relative Offset	Relative Offset
	Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word
	.text	000002DC	00001000	00001000	00001000	00000000	00000000	0000	0000
	.rdata	00000372	00002000	00001000	00002000	00000000	00000000	0000	0000
	.data	0000008C	00003000	00001000	00003000	00000000	00000000	0000	0000

.text

contiene le istruzioni che la CPU eseguirà una volta che il software sarà avviato.

.rdata

include le info circa le librerie e le funzioni importate ed esportate dall'eseguibile.

.data

contiene i dati/variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

Per poter ottenere maggiori informazioni su che cosa fa il programma possiamo analizzare l'hash del malware con il sito VirusTotal.

	Property	Value
	File Name	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W...
	File Type	Portable Executable 32
	File Info	No match found.
	File Size	3.00 KB (3072 bytes)
	PE Size	16.00 KB (16384 bytes)
	Created	Tuesday 16 August 2022, 13.37.31
	Modified	Wednesday 19 January 2011, 10.10.41
	Accessed	Monday 27 November 2023, 14.12.56
	MD5	AE4CA70697DF5506BC610172CFC288E7
	SHA-1	31E8A82E497058FF14049CF283B337EC51504819
	Property	Value
	Empty	No additional info available

Se andiamo a cercare il seguente hash possiamo vedere che il malware che stiamo andando ad analizzare è un Trojan.