Analisi Malware

Apertura programma per analisi Malware

utilizziamo il programma CFF Explorer e una volta avviato, scegliamo un file eseguibile da caricare per analizzare l'header del PE. Clicchiamo sull'icona a forma di cartella e scegliamo il file che vogliamo caricare.

Una volta scelto il file eseguibile per il quale vogliamo esaminare l'header del formato PE. Per controllare le librerie e le funzioni importate, spostiamoci su «import directory» nel menù a sinistra

Queste sono le librerie presenti nel malware analizzato

Malware_U3_W2_L1.exe

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

Spiegazione Librerie

Kernel32.dll: libreria piuttosto comune che contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.

Advapi32.dll: libreria che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft

MSVCRT.dll: libreria che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output in stile linguaggio C.

Wininet.dll: libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Sezioni Malware

Per controllare le sezioni di un file eseguibile, avviamo CFF Explorer, selezioniamo il file eseguibile per il quale vogliamo controllare le sezioni e spostiamoci nel pannello a sinistra nella sezione «section headers».

In questo caso però il nome delle sezioni è nascosto (tabella name a Sx)

Malware_U3_W2_L1.exe

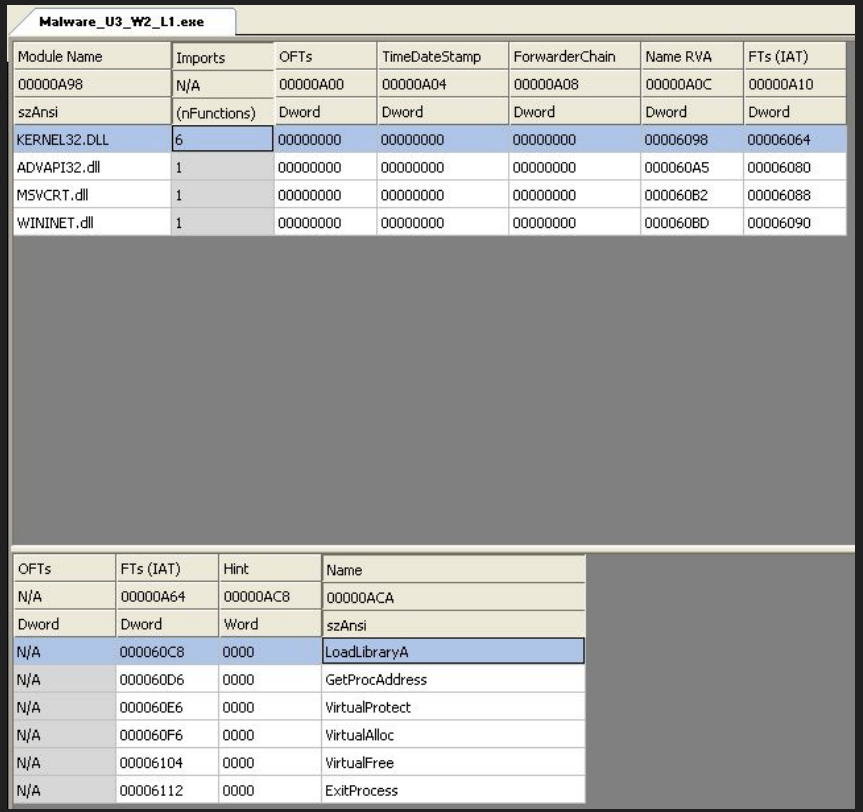
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

Considerazioni Finali

In questo caso abbiamo analizzato un malware che non consente di capire il suo comportamento tramite la sola analisi statica basica.

Sono presenti però delle funzioni (LoadLibrary) che vengono importate a tempo di esecuzione (runtime)

Considerazioni Finali



Malware_U3_W2_L1.exe

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
N/A	00000A64	00000AC8	00000ACA
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