

Marzo 2024

CYBER SECURITY SPECIALIST

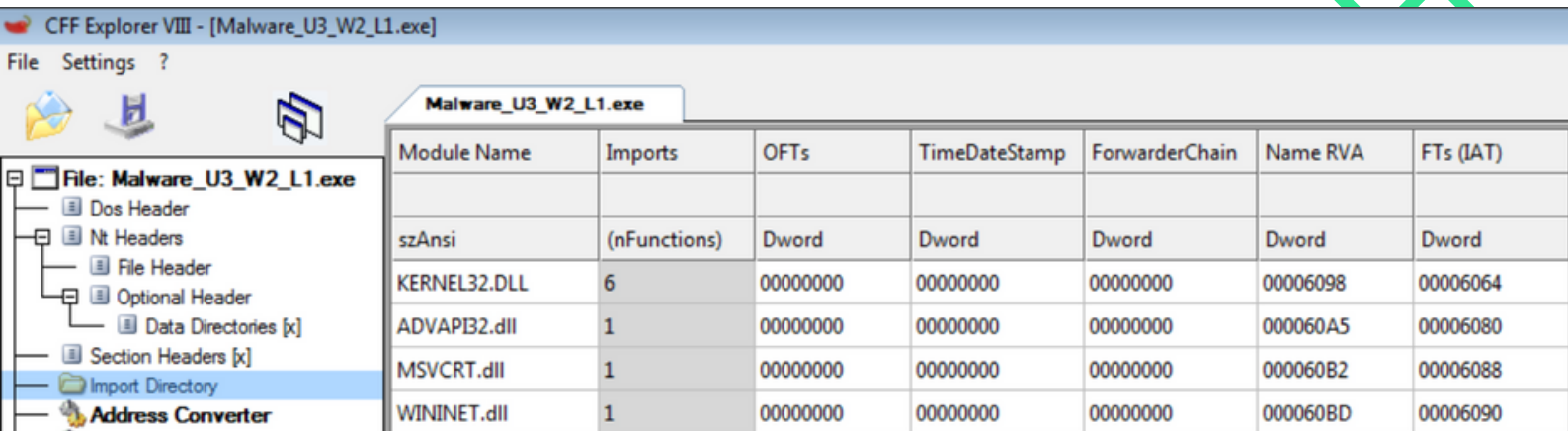
S10L1

Jacopo Trovato



Analisi statica basica

Su la macchina "Windows XP malware analysis" bisogna andare a prendere il file "Esercizio_Pratico_U3_W2_L1" e grazie ad "CFF explorer" fare un'analisi statica basica.



CFF Explorer VIII - [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

All'interno del file si trovano 4 cartelle:

1. KERNEL32.DLL= Include le funzioni fondamentali per l'interazione con il sistema operativo, come ad esempio la manipolazione dei file e la gestione della memoria. Dentro questa cartella ci sono 6 funzioni

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

2. ADVAPI32.dll= Include le funzioni per interagire direttamente con i servizi e i registri del sistema operativo. Al suo interno si trova una funzione.

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006120	0000	CreateServiceA

3. MSVCRT.dll = Comprende funzioni per manipolare stringhe, gestire l'allocazione di memoria e altre operazioni comuni come le chiamate per l'input/output, simili a quelle presenti nel linguaggio C. Contiene una funzione.

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006130	0000	exit

4. WININET.dll = Offre funzioni per implementare alcuni protocolli di rete tra cui HTTP, FTP e NTP. Anch'essa contiene una sola funzione.

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006136	0000	InternetOpenA