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

Soluzione

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

Utilizzando CFF Explorer, possiamo vedere che:

- Kernel32.dll include le funzioni centrale del sistema operativo
- Advapi32.dll include le funzioni per interagire con i servizi
- MSVCRT.dll è una libreria per l'allocazione memoria
- Wininet.dll include le funzioni per implementare i servizi di rete

Nella sezione «section header» vediamo come si compone il malware, diviso in tre sezioni.

Byte[8]	Dword	Dword	Dword	Dword	Dword
UPX0	00004000	00001000	00000000	00000400	00000000
UPX1	00001000	00005000	00000600	00000400	00000000
UPX2	00001000	00006000	00000200	00000A00	00000000

Si può capire che è un malware che riesce a nascondere le informazioni, questo porta a non avere molte informazioni sul suo comportamente tramite l'analisi statica.