

# S10/L1

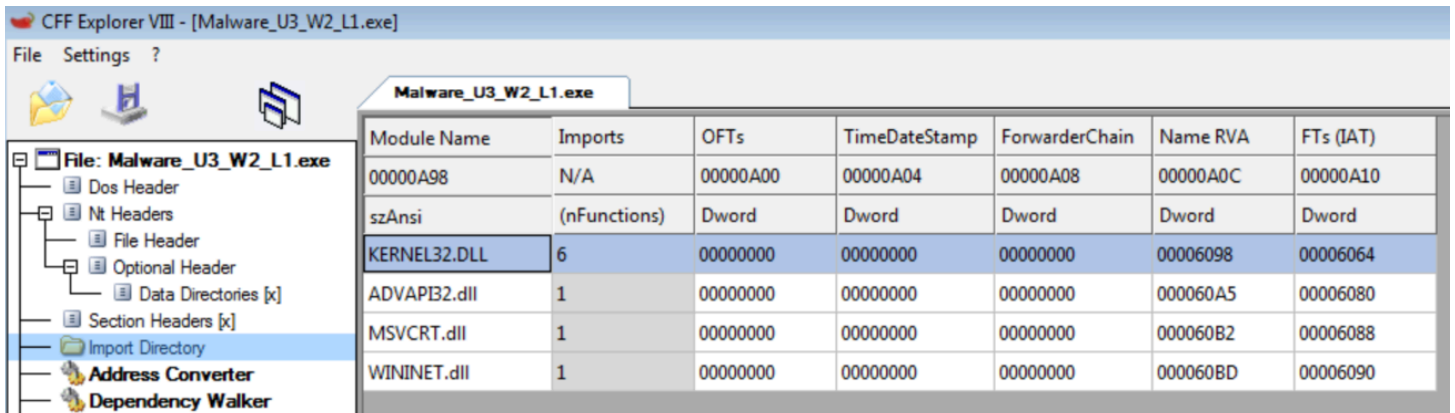
Stefano Di Prospero  
NetRaiders

## ANALISI STATICA BASICA

### 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



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)
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

File: Malware\_U3\_W2\_L1.exe

- Dos Header
- Nt Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker

Con l'analisi di CFF possiamo notare quali sono le librerie presenti:

- KERNEL32.DLL; esso contiene le funzioni usate per interagire con l'OS.
  - ADVAPI32.DLL; interagisce con servizi e registri del sistema operativo.
  - MSVCRT.DLL; ha funzioni capaci di manipolare, ad esempio, stringhe, allocazioni memoria.
  - WININET; ha funzioni che implementano protocolli di rete.

CFF Explorer VIII - [Malware\_U3\_W2\_L1.exe]

File Settings ?

Malware\_U3\_W2\_L1.exe

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

Come possiamo notare il malware è composto da 3 sezioni.  
Sfortunatamente non siamo in grado di capire le di che tipo sono data anche l'assenza del nome

Dopo un'analisi iniziale si può notare che non è un malware base poich  sembra essere un malware che importa le librerie solo quando ne viene richiesta l'esecuzione, ovvero in RUNTIME.

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
0000A98	N/A	0000A00	0000A04	0000A08	0000A0C	0000A10
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
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

La libreria KERNEL32.dll presenta due funzioni: ***LoadLibraryA*** e ***GetProcAddress***. Queste due funzioni sono messe a disposizione dall'OS per chiamare la libreria solo all'occorrenza, impedendoci di sapere quale sono le librerie senza l'esecuzione del malware.