### **BENVENUTI LUIGI**

### 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

### Nozioni teoriche utili:

- **Libreria**: in informatica, una libreria, o più raramente biblioteca, è un insieme di funzioni o strutture dati predefinite e predisposte per essere riutilizzate da altri programmi software attraverso un'opportuna procedura di collegamento.

Importazione a tempo di esecuzione (runtime): L'eseguibile richiama la libreria solamente quando necessità di una particolare funzione. Questo comportamento è ampiamente utilizzato dai malware, che «chiamano» una determinata funzione solo all'occorrenza per risultare quanto meno invasivi e rilevabili possibile. Per chiamare la libreria all'occorrenza, si utilizzano delle funzioni messe a disposizione dal sistema operativo come «LoadLibrary» e «GetProcAddress».

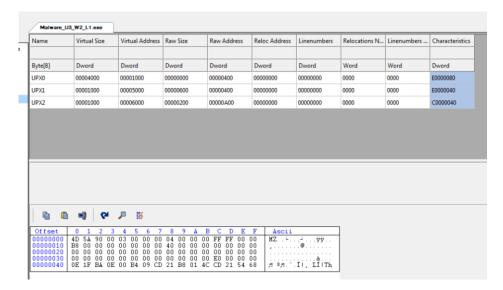
### **Librerie:**

- **KERNEL32.dll:** contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.
- Advapi32.dll: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo.
- **MSVCRT.dll:** contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C.
- Wininet.dll: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000ABD	N/A	00000A3C	00000A40	00000A44	00000A48	00000A4C
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

# Sezioni:

- Il malware ha nascosto i nomi delle sezioni dunque non c'è possibilità di avere indietro informazioni.



# Funzioni libreria Kernel 32:

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	

# Considerazioni sul malware:

Tra le funzioni importate troviamo «LoadLibrary e GetProcAddress», che ci fanno pensare ad un malware che importa le librerie a tempo di esecuzione (runtime) nascondendo di fatto le informazioni circa le librerie importate a monte.



!This	program	cannot	be	run	in	DOS	mode.	O Much
Rich								OpenMu\$x
UPX0								ZŠB+
UPX1								ForS
UPX2								ing
3.04								ObjectU4
UPX!								[Urtb
								CtrlDisp ch
AI3								SCM
hぐØ								8_e
L\$,								Xcpt
$\mathbf{Q}1\mathbf{I}$								mArg
qií "z								
RU\$								รแร E0
u+Ŵ								5nm@_
. hP								t_fd
t=p								19H
sHR								m≺e
i Pd								9.p
ıFq								utu
S								uty d1I37n
a∖'Y								olfp
t@E								PEL
DmM								ά₩16
;0I								4+
PQ6								.4t 1B`.rd
(23h								IB .ra
Ma1Se1	rvice							@.&
sHGL34								0'0
http:/								_~s
warear								u A
ysisbo								GIu
		.1.0 01	PET					PTj
OWHILL	t6net Exp	910:r 81	LI					XPŤPSW
.0<	T . T .							KERNEL32.DLL
Syster	nTimeToF:	ıle						ADVAPI32.dll
GetMo								MSUCRT.d11
NaA								WININET.dll
Cvg								LoadLibraryA
<b>×</b> Waita	ab'r							C-4D011
Proces								GetProcAddress
OpenMu	ι\$x							VirtualProtect
ZŜB+								VirtualAlloc
ForS								VirtualFree
ing								ExitProcess
Object	-114							CreateServiceA
Object	.04							exit
[Urth								InternetOpenA
CtrlD:	isp ch							- II J J J II J J J J J J J J J J J J J