

S10L1,

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.

Malware_U3_W2_L1.exe						
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.

Malware_U3_W2_L1.exe									
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	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



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii	
00000000	4D	5A	90	00	03	00	00	00	00	04	00	00	00	FF	FF	00	00	NZyy..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	00@.
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	E0	00	00	00
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	00	. 9. . Ii, IiTh

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.

Strings output:

!This program cannot be run in DOS mode.

Rich
UPX0
UPX1
UPX2
3.04
UPX?
AI3
h<0
L\$,
QlI
" z
RU\$
u+W
.hP
t=p
sHR
iPd
S`
a\`Y
t@E
DmM
;0I
PQ6
<23h
MalService
sHGL345
http://w
warean
ysisbook.co
om#Int6net Explo!r 8FEI
.0<
SystemTimeToFile
GetMo
NaA
Cvg
*Waitab'r
Process
OpenMu\$x
ZSB+
ForS
ing
ObjectU4
[Urtb
CtrlDisp ch

OpenMu\$x
ZSB+
ForS
ing
ObjectU4
[Urtb
CtrlDisp ch
SCM
8_e
Xcpt
mArg
sus
5nm@_
t_fd
i9H
m<e
9,p
vty
dll37n
olfp
PEL
dW!6
.4t
lB`.rd
@.&
0'0
~S
u A
GIu
PTj
XPTPSW
KERNEL32.DLL
ADVAPI32.dll
MSVCRT.dll
WININET.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
CreateServiceA
exit
InternetOpenA