MALWARE ANALYSIS

Traccia:

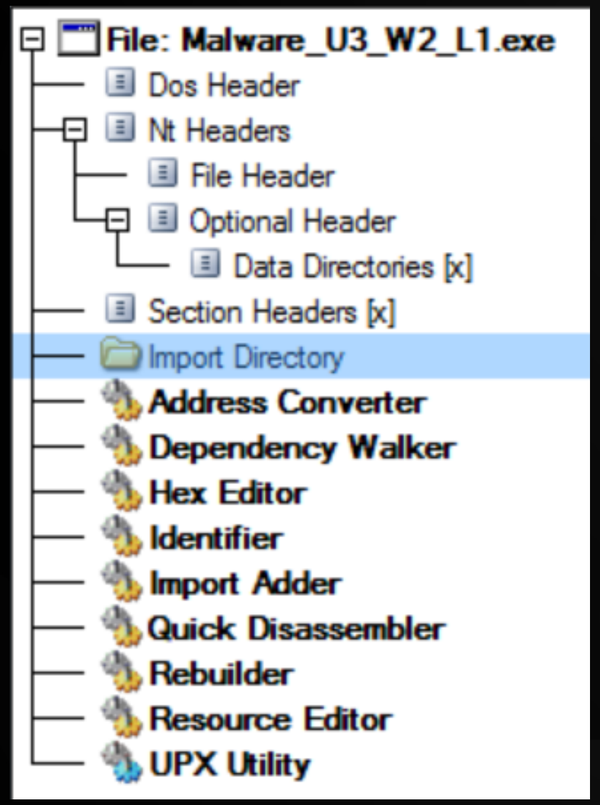
Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1» presente sul Desktop della vostra macchina virtuale dedicata all’analisi dei malware, rispondere ai seguenti quesiti:

- Indicare le librerie importate dal malware, fornendo una descrizioneper ognuna di esse.

- Indicare le sezionidi cui si compone il malware, fornendo una descrizioneper ognuna di essa

- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

Andremo a effettuare un’analisi dinamica, mediante l’uso del tool CFF Explorer. Quindi, viene analizzato il file contenente un malware in un ambiente protetto, nel nostro caso all’ interno della macchina di windows 7.



Il tool ci da informazioni, in particolare, sulle librerie in “Import directory” e sulle sezioni in “Section headers”.

LIBRERIE

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	9	00000000	00000000	00000000	0000216C	00002010
ADVAPI32.dll	3	00000000	00000000	00000000	00002179	00002000
MSVCRT.dll	13	00000000	00000000	00000000	00002186	00002038
WININET.dll	2	00000000	00000000	00000000	00002191	00002070

LIBRERIE

- Kernel32.dll : è una libreria a collegamento dinamico (DLL) nel sistema operativo Windows. Gioca un ruolo cruciale nel funzionamento di Windows poiché contiene numerose funzioni e procedure utilizzate da varie applicazioni e dal sistema operativo stesso.

- Advapi32.dll : contiene le funzioni per interagire con i servizi ed i registri del sistema operativo.

- Wininet.dll : contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

- MSVCRT.dll : contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C.

SEZIONI

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
00000200	00000208	0000020C	00000210	00000214	00000218	0000021C	00000220	00000222	00000224
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000002DC	00001000	00001000	00001000	00000000	00000000	0000	0000	60000020
.rdata	00000372	00002000	00001000	00002000	00000000	00000000	0000	0000	40000040
.data	0000008C	00003000	00001000	00003000	00000000	00000000	0000	0000	C0000040

SEZIONI

- .text: contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l’unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto.

- .rdata: include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall’eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer.

- .data: contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma. Una variabile si dice globale quando non è definita all’interno di un contesto di una funzione, ma bensì è globalmente dichiarata ed è di conseguenza accessibile da qualsiasi funzione all’interno dell’eseguibile.

ANALISI

NANO-Antivirus	Trojan.Win32.Click3.iaupgs	Rising	Trojan.Clicker-Agent!8.13 (CLOU
Sangfor Engine Zero	Suspicious.Win32.Save.a	SecureAge	Malicious
Skyhigh (SWG)	Generic.ait	Sophos	Mal/Generic-S
Symantec	Trojan Horse	Tencent	Malware.Win32.Gencirc.10be33c
Trellix (FireEye)	Generic.mg.8363436878404da0	TrendMicro	TROJ_GEN.R002C0DHD20
TrendMicro-HouseCall	TROJ_GEN.R002C0DHD20	Varist	W32/Agent.DJC.gen!Eldorado
VBA32	Trojan.Click	VIPRE	Gen:Variant.Ser.Ulise.216
VirIT	Trojan.Win32.Generic.CMEY	ViRobot	Trojan.Win32.S.StartPage.3072
Webroot		WithSecure	Trojan.TR/Downloader.Gen

Subsystem	0000013C	Word	0003	Windows Console
DllCharacteristics	0000013E	Word	0000	Click here

Si noti che, dopo un’analisi,il malware lavora su S.O.
Questo tipo di malware potrebbe sfruttare le caratteristiche delle Dynamic Link Libraries (DLL) per nascondere il proprio codice, manipolare l'esecuzione delle applicazioni o eludere le misure di sicurezza (figura).
Inoltre, grazie al tool VirusTotal, si deduce che sia un vero e proprio trojan.
Si deduce che tale malware è trojan che fa da vettore per un rootkit, al fine di agire sul kernel.