Esercizio S10/L1

Malware Analysis

Nell’esercizio di oggi eseguiremo l’analisi statica base di un malware. L’analisi statica base consiste nell’esaminare un eseguibile e capirne il comportamento senza eseguirlo e senza vedere le istruzioni. Essa è molto semplice da eseguire, ma può risultare poco efficace contro malware più sofisticati. Inoltre deve essere complementare con un'analisi dinamica, in cui il malware viene eseguito in ambiente sandbox, per avere un quadro completo della situazione.

Nell’esercizio esamineremo le librerie e le sezioni di cui è composto il malware. Come tool ho scelto CFF explorer. Cominciamo aprendo il file indicatoci dall’esercizio con CFF explorer, poi ci spostiamo nel tab “import directory” come in figura.

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

Dalla figura possiamo notare diverse librerie importate dinamicamente, cioè caricate dal sistema operativo quando il malware viene eseguito:

- KERNEL32.DLL è una libreria che contiene le funzioni necessarie all'interazione con il sistema operativo, come per esempio la manipolazione dei file;

- Advapi32.dll è una libreria che consente di interagire con i servizi e i registri di sistema;

- Msvcrt.dll contiene funzioni per manipolazione di stringhe, allocazione di memoria e altro;

- Wininet.dll contiene le funzioni per l'implementazione di alcuni protocolli come http e ftp.

Passiamo a vedere le sezioni. Dall'immagine sotto possiamo vedere tre sezioni:

- text contiene le istruzioni che verranno eseguite dalla CPU;

- rdata include le informazioni sulle librerie e le funzioni importate ed esportate;

- data contiene i dati e/o le variabili del programma

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword
.text	000002DC	00001000	00001000	00001000	00000000	00000000
.rdata	00000372	00002000	00001000	00002000	00000000	00000000
.data	0000008C	00003000	00001000	00003000	00000000	00000000

Considerazioni finali

Un malware può essere riconoscibile da tutte queste informazioni. In genere hanno poche librerie e tra queste quelle più comuni permettono di caricare librerie esterne o collegarsi ad un altro dominio. Dalle informazioni ottenute su questo malware possiamo intuire che sia in grado di prendere il controllo del nostro sistema, quindi possiamo ipotizzare che sia un RAT oppure un trojan.