Analisi statica basica

Pablo Andres Balbuena Rios

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

Librerie importate dal malware

Le libreria che troviamo sono:

- KERNEL32.DLL: contiene le funzioni principali per interagire con il sistema operativo.
- 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.
- WININET.dll: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Module Name	Imports
szAnsi	(nFunctions)
KERNEL32.DLL	6
ADVAPI32.dll	1
MSVCRT.dll	1
WININET.dll	1

Le sezioni

KERNELL32.DLL:

LoadLibrary e GetProcAddress: sono funzioni utilizzate per caricare altre funzioni addizionali durante l'esecuzione.

- LoadLibraryA: è utilizzata per caricare dinamicamente una DLL nel processo corrente.
- GetProcAddress: è utilizzata per ottenere l'indirizzo di una funzione all'interno di quella DLL.

"VirtualProtect, VirtualAlloc e VirtualFree" sono funzioni per la gestione della memoria virtuale.

- VirtualProtect: è utilizzata per modificare i diritti di accesso di una porzione di memoria virtuale già allocati.
- VirtualAlloc: è utilizzata per allocare una nuova porzione di memoria virtuale.
- VirtualFree: è utilizzata per liberare una porzione di memoria virtuale precedentemente allocata tramite VirtualAlloc.
- ExitProcess: viene utilizzata per terminare il processo corrente.

KERNELL32.DLL

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

Le sezioni

ADVAPI32.dll:

- CreateServiceA: è utilizzata per creare un nuovo servizio di sistema. La versione "A" indica che la funzione accetta stringhe ASCII.

MSVCRT.dll:

- Exit: è utilizzata per terminare immediatamente il programma e restituire un codice di uscita al sistema operativo

WININET.dll:

- InternetOpenA: è utilizzata per inizializzare una sessione WinINet, consentendo l'apertura di connessioni Internet e l'esecuzione di altre operazioni di rete.

ADVAPI32.dll

N/A	00006120	0000	CreateServiceA

MSVCRT.dll

N/A	00006130	0000	exit

WININET.dll

N/A	00006136	0000	InternetOpenA

Considerazione finale

- Il malware «Esercizio_Pratico_U3_W2_L1», dalle caratteristiche possiamo notare che si tratta di un malware runtime, perché chiamerà la libreria successivamente con la funzione "LoadLibrary".
- Si può anche notare che il malware si collega ad Internet attraverso la funzione di WININET e può caricare altre funzioni nel processo, in seguito può creare un servizio di sistema attraverso la modifica di diritti d'accesso per poi allocare o eliminare, porzioni di memoria virtuale.