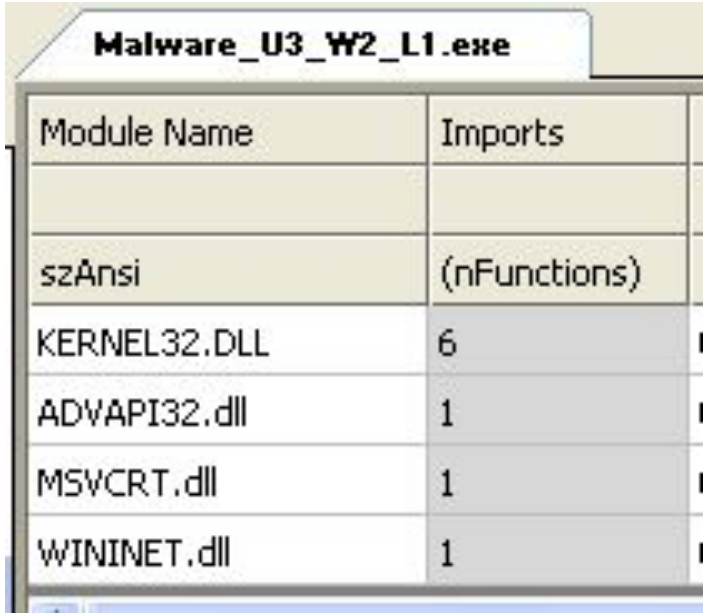
EPICODE

Progetto Alessandro Moscetti 07/11



Utilizzando il tool CFF explorer sono andato ad analizzare il malware.
Le librerie trovate sono:

- KERNEL32.DLL che contiene le funzioni principali per interagire con il sistema operativo.
- ADVAPI32.dll che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo.
- MSVCRT.dll che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro.
- WININET.dll che contiene le funzioni per l'implementazione di alcuni protocolli di rete.

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

Funzioni richiamate nella libreria KERNEL32.DLL:

- LoadLibraryA e GetProcAddress possono essere utilizzate per richiamare altre librerie all'occorrenza di una determinata funzione.
- VirtualProtect modifica i diritti di accesso della memoria per una regione di pagine di un processo.
- VirtualAlloc riserva, impegna o libera pagine di memoria nel processo.
- VirtualFree libera l'area di memoria precedentemente allocata con VirtualAlloc.
- ExitProcess termina il processo in esecuzione.

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006120	0000	CreateServiceA

Funzione richiamata nella libreria ADVAPI32.dll:

- CreateServiceA crea un nuovo servizio o un driver di dispositivo. Questo servizio può essere avviato automaticamente al caricamento del sistema o può essere avviato manualmente.

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006130	0000	exit

Funzione richiamata nella libreria MSVCRT.dll:

- exit termina il programma.

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006136	0000	InternetOpenA

Funzione richiamata nella libreria WININET.dll:

- InternetOpenA crea una sessione su Internet.

Malware_U3_W2_L1.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumb
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000
UPX1	00001000	00005000	00000600	00000400	00000000	00000000
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000

L’eseguibile è composto da 3 sezioni UPX (Ultimate Packer for eXecutables).
Questo formato è utilizzato per comprimere file eseguibili nascondendo la loro funzione o scopo e riducendo notevolmente la dimensioni.
Solitamente la sezione UPX0 all’esecuzione del programma viene estratta nella memoria e utilizzata per decomprimere le sezioni restanti.
UPX1 di solito contiene il codice originale del codice compresso mentre UPX2, comunemente, contiene dati o risorse aggiuntive utilizzate da UPX0 nella decompressione.

Considerazione finale

Tenendo conto delle informazioni trovate possiamo ipotizzare che l'eseguibile sia un downloader perchè va a creare una sessione su Internet.

Grazie per l’attenzione.