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

L'esercizio di oggi riguardava l'analisi di un malware, nello specifico tramite la tecnica dell'analisi statica, cioè senza eseguirlo.

Tramite l'utilizzo del tool CFF Explorer abbiamo individuato le librerie importate, come visibili nell'immagine seguente.

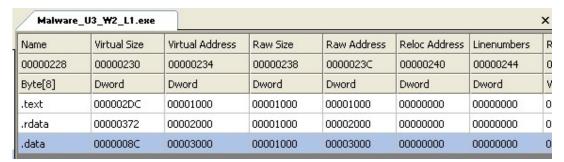
Module Name		mports	OFTs		TimeDateStamp	ForwarderChain	Name RVA
00000A98 N/A		I/A	00000A	400	00000A04	00000A08	00000A00
szAnsi (nf		nFunctions)	Dword		Dword	Dword	Dword
KERNEL32.DLL 6		0000		000	00000000	00000000	00006098
ADVAPI32.dll 1			000000	000	00000000	00000000	000060A5
MSVCRT.dll 1			000000	000	00000000	00000000	000060B2
WININET.dll 1		1 00		000	00000000	00000000	000060BD
<	1			1111			
<				111			
OFTs	FTs (IAT)	Hint		Name		7	
	FTs (IAT)	Hint					
OFTs Dword		Word		Name	oraryA		
OFTs Dword N/A	Dword	Word 0000		Name szAnsi LoadLib	oraryA cAddress		
OFTs Dword N/A N/A	Dword 000060C8	Word 0000 0000		Name szAnsi LoadLib	cAddress		
OFTs	Dword 000060C8 000060D6	Word 0000 0000 0000		Name szAnsi LoadLib GetProd	cAddress Protect		
OFTs Dword N/A N/A N/A	Dword 000060C8 000060D6	Word 0000 0000 0000 0000		Name szAnsi LoadLib GetProd VirtualP	cAddress Protect		

PRATICA S10L1- Giorgio Trovesi

Entrando nel dettaglio queste librerie servono:

- KERNEL32: è una componente fondamentale del sistema operativo e viene utilizzata per l'esecuzione di operazioni di basso livello come la creazioni di processi, manipolazione di file e directory, accesso a risorse del sistema. Al suo interno vi sono funzioni come "LoadLibraryA" e"GetProcAddress" che serviranno a chiamare le librerie all'occorrenza, questa casistica è denominata importazione a tempo di esecuzione delle librerie;
- ADVAPI31: contiene le funzioni per interagire con i servizi e registri del sistema operativo;
- **MSVCRT:** contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate input/output, come nel linguaggio C;
- **WININET:** contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP,NTP.

Successivamente abbiamo individuato le sezione di cui si compone il malware:



- .text: contiene istruzioni che la CPU eseguirà una volta che il software sarà avviato;
- .rdata: contiene le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile;
- .data: contiene di solito i dati e le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

Il malware è un trojan downloader che potrebbe essere utilizzato per scaricare sulla vittima una Backdoor.

