REPORT CS0124

S10L1

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:

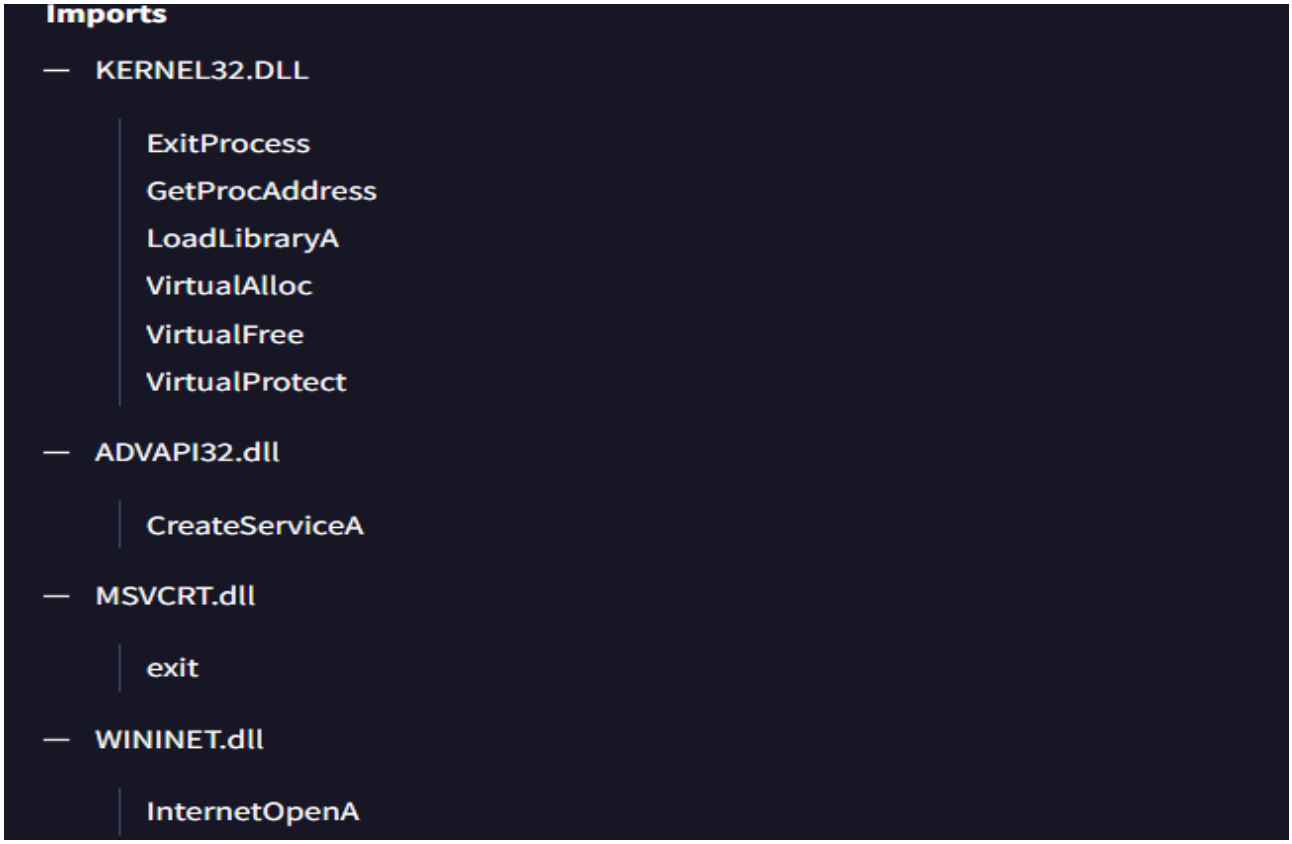
• Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse

• 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

Il primo passo per identificare che tipo di librerie sono state importate all'interno del malware apriamo il file tramire CFF(un tool per analizzare i file e navigarci senza eseguirli).

Dopodiche' ci spostiamo nella sezione import directory e notiamo che abbiamo diverse librerie importate direttamente da windows



KERNEL32.DLL si riferisce al nucleo della macchina, questa libreria gestisce tutta la parte della memoria interna della macchina.

ADVAPI32.DLL e' una libreria advapi32.dll è una parte di una libreria avanzata di servizi di api che supporta i numerosi api compreso i molti chiamate di registrazione e di sicurezza.

MSVCRT.DLL è un modulo che contiene le funzioni di libreria C Standard quale il printf, memcpy e una parte della libreria Runtime di Microsoft C.

WININET.DLL wininet.dll è un modulo che contiene le funzioni Internet-relative usate dalle applicazioni di Windows.

Le tre sezioni di cui si compone il malware, come possiamo vedere, agiscono direttamente sul kernel una volta che avviamo il file

.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

.**text** comprende le istruzioni che il malware andra' ad eseguire

.**rdata** comprende le informazioni delle librerie importate una volta avviato il file

.**data** comprende le informazioni variabili del file eseguibili.

CONSIDERAZIONI

A mio avviso in questo caso stiamo parlando parlando di un trojan. Questo tipo di malware si va a camuffare come un programma normale della macchina e non viene rilevato senza effettuare delle scansioni specifiche. La richiesta di download delle azioni del malware fa anche intendere che ad un certo punto vengono scaricati altri file di tipo malevolo all'interno della macchina target.