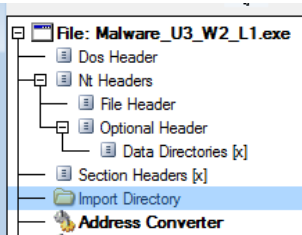


S10L1

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, Indicare le sezioni di cui si compone il malware.**

Analisi statica (*cff explorer*)



Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (U
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	000060
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	000060
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	000060
WININET.dll	1	00000000	00000000	00000000	000060BD	000060

Librerie:

- Kernel32.dll: è una libreria di sistema essenziale in ambienti Windows.
- Advapi32.dll: è un'altra libreria di sistema essenziale nei sistemi operativi Windows, rivolta particolarmente alla sicurezza e alla gestione degli account utente.
- Msvcrt.dll: fornisce molte delle funzionalità di base necessarie per l'esecuzione di programmi scritti in linguaggio C o C+.

- Wininet.dll: è una libreria di sistema di Windows che fornisce funzionalità per l'accesso a risorse su Internet.

Funzioni

KERNEL32.DLL	6	00000000	00000000	00000000	00006098	000060C8
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	000060C8
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	000060C8
WININET.dll	1	00000000	00000000	00000000	000060BD	000060C8

OFTs	FTs (IAT)	Hint	Name
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

- **Kernel32.dll**
 - loadlibraryA: è una delle funzioni di base del sistema Windows utilizzata per caricare una libreria dinamica (DLL).
 - GetProcAddress: è una funzione di Windows utilizzata per ottenere un puntatore a una funzione esportata da una libreria dinamica (DLL).
 - VirtualProtect: è utilizzata per modificare i permessi di accesso di una regione di memoria virtuale.

- VirtualAlloc: è una funzione utilizzata per allocare una nuova regione di memoria virtuale all'interno di un processo.
- VirtualFree: è una funzione utilizzata per liberare una regione di memoria virtuale.

ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	000060A5
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	000060B2
WININET.dll	1	00000000	00000000	00000000	000060BD	000060BD

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

● Advapi32.dll

- CreateServiceA: Questa funzione consente di registrare un nuovo servizio nel sistema operativo Windows.

MSVCRT.dll	1	00000000	00000000	00000000	000060B2	000060B2
WININET.dll	1	00000000	00000000	00000000	000060BD	000060BD

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

● Msvcrt.dll

- Exit: La funzione exit è utilizzata per terminare il programma corrente.

WININET.dll	1	00000000	00000000	00000000	000060BD	000060
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
N/A	00006136	0000	InternetOpenA			

- **Wininet.dll**

- InternetOpenA:viene utilizzata per inizializzare una sessione di accesso a Internet.

Sezioni

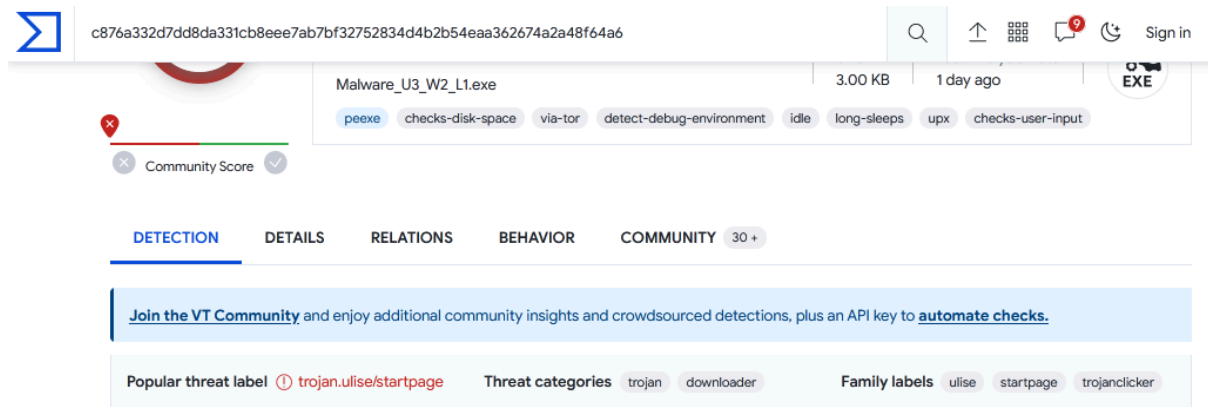
.text:Questa sezione contiene il codice eseguibile del programma.

.rdata:Questa sezione contiene dati che non possono essere modificati durante l'esecuzione del programma.

.data:In questa sezione vengono solitamente dichiarate variabili e costanti.

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

Scansione



Trojan: è un tipo di malware progettato per sembrare un programma legittimo o utile mentre svolge funzionalità dannose sul dispositivo dell'utente senza il suo consenso.

CONSIDERAZIONE FINALE SUL MALWARE

Secondo il mio punto di vista, questo malware va ad avviarsi automaticamente ogni volta che si avvia il proprio pc (*CreateServiceA*), inoltre va ad allocarsi all'interno di un processo e inietta codice dannoso (*VirtualAlloc*).

Come ultima fase, stabilisce una connessione ad un server (*InternetOpenA*) per inviare le informazioni sensibili rubate oppure per scaricare altri malware (**downloader**).