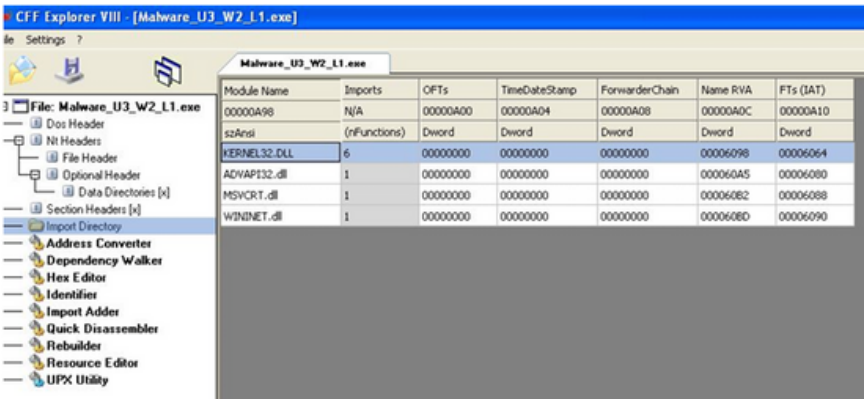
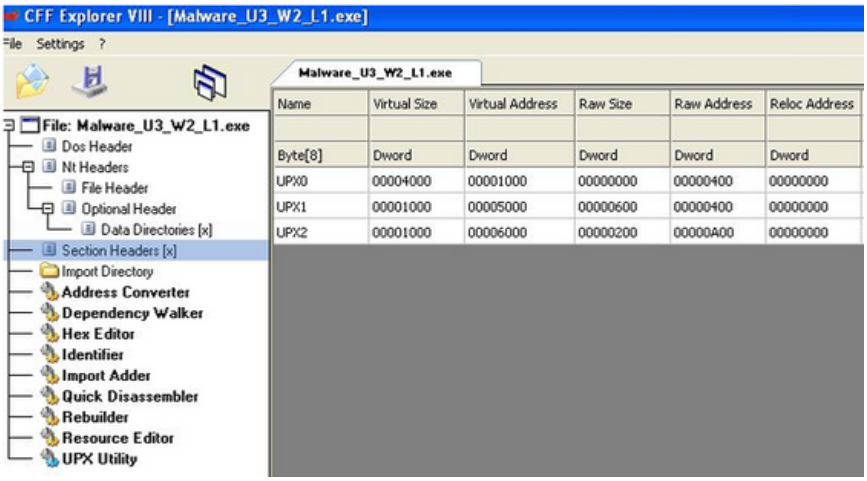
Analisi statica basica

Traccia:
Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi statica basica. 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'analisi statica è una componente fondamentale dell'analisi forense e della sicurezza informatica, permettendo agli analisti di ottenere informazioni preziose su file sospetti senza eseguirli, riducendo così il rischio di infezione.





Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain
00000A98	N/A	00000A00	00000A04	00000A08
szAnsi	(nFunctions)	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000
ADVAPI32.dll	1	00000000	00000000	00000000
MSVCRT.dll	1	00000000	00000000	00000000
WININET.dll	1	00000000	00000000	00000000

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
N/A	00006112	0000	ExitProcess

Importazione delle Librerie

Il malware in questione, identificato come U3_W2_L1, importa quattro librerie fondamentali per la sua esecuzione e interazione con il sistema operativo Windows:

1. Kernel32.dll: Questa è una delle principali librerie del sistema operativo Windows, contenente funzioni di base che permettono la gestione della memoria, dei processi e dei thread. La presenza di questa libreria nell'elenco delle importazioni è comune per la maggior parte dei programmi Windows, in quanto fornisce funzionalità essenziali per l'interazione con il sistema operativo.
2. Advapi32.dll: Questa libreria offre un'interfaccia di programmazione per la gestione di registri, il controllo di accesso e la gestione dei servizi di Windows. La sua importazione suggerisce che il malware potrebbe tentare di modificare le impostazioni di sistema, accedere a informazioni sensibili tramite i registri o interagire con i servizi di Windows per eseguire operazioni potenzialmente malevole.
3. MSVCRT.dll: Si tratta della libreria runtime di Microsoft C, che fornisce funzioni standard C per la manipolazione di stringhe, memoria e altre funzionalità di base. La sua presenza indica che il malware è stato sviluppato utilizzando il linguaggio di programmazione C, facendo affidamento su questa libreria per le operazioni standard.
4. Wininet.dll: Questa libreria è utilizzata per accedere a funzionalità Internet come FTP, HTTP e NTP. L'importazione di questa libreria suggerisce che il malware potrebbe comunicare con server remoti, scaricare ulteriori payload o esfiltrare dati attraverso la rete.

Sezioni del Malware

L'analisi delle sezioni di un file eseguibile offre una visione della struttura e delle funzionalità del codice. Nel caso di U3_W2_L1, l'esame attraverso CFF Explorer rivela che l'eseguibile è composto da tre sezioni. Tuttavia, il nome delle sezioni è stato deliberatamente nascosto o alterato, rendendo difficile identificarne il contenuto o lo scopo specifico senza un'analisi più approfondita. Questa tattica è spesso utilizzata dagli autori di malware per ostacolare l'analisi e nascondere le vere intenzioni del codice malevolo.

Considerazione Finale

Il malware U3_W2_L1 dimostra caratteristiche di sofisticatezza, come evidenziato dall'uso di tecniche di importazione dinamica delle librerie tramite le funzioni LoadLibrary e GetProcAddress. Questo approccio permette al malware di caricare ulteriori librerie durante l'esecuzione, rendendo più difficile per gli analisti identificare tutte le dipendenze e le funzionalità del malware senza eseguire un'analisi dinamica. L'ocultamento dei nomi delle sezioni e l'importazione dinamica delle librerie sono indicatori di un livello avanzato di ingegneria malevola, volto a evitare il rilevamento e l'analisi.

In conclusione, l'analisi statica del malware U3_W2_L1 rivela un'entità sofisticata con potenziali capacità di manipolazione del sistema, esfiltrazione di dati e comunicazione con server remoti. La presenza di tecniche di evasione come l'ocultamento delle sezioni e l'importazione dinamica delle librerie evidenzia la necessità di approfondire l'analisi con tecniche dinamiche per comprendere pienamente le capacità e l'intento del malware.