Report sull'Analisi Statica di un Malware

Data 05/02/24

Introduzione

Nella sessione teorica del mattino, ci siamo concentrati sull'analisi statica di un malware, utilizzando un file eseguibile situato nella cartella "Esercizio_Pratico_U3_W2_L1" sul desktop della macchina virtuale dedicata all'analisi dei malware. Questo report offre una panoramica delle informazioni raccolte durante l'analisi, includendo le librerie importate dal malware, la composizione delle sezioni del malware e una considerazione finale basata su tali informazioni.

Librerie Importate

Con l'utilizzo di un software comune per l'analisi dei malware chiamato CFF Explorer è stato possibile identificare le librerie importate nel malware. Per fare ciò una volta caricato il file malevolo nel programma in questione abbiamo cliccato sulla sezione chiamata "Import Directory", in questa sezione il programma mostra una tabella delle librerie utilizzate nel programma conuna serie di parametri, come ad esempio il numero di funzioni imporatte da ciascuna libreria.

Nello screen si possono notare le librerie imporatte nel programma

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

KERNEL32.DLL:

Descrizione: KERNEL32.DLL è una libreria essenziale di Windows che fornisce funzionalità di basso livello al sistema operativo. Contiene routine per la gestione della memoria, gestione dei processi, gestione dei file e molte altre funzioni di sistema fondamentali.

ADVAPI32.dll:

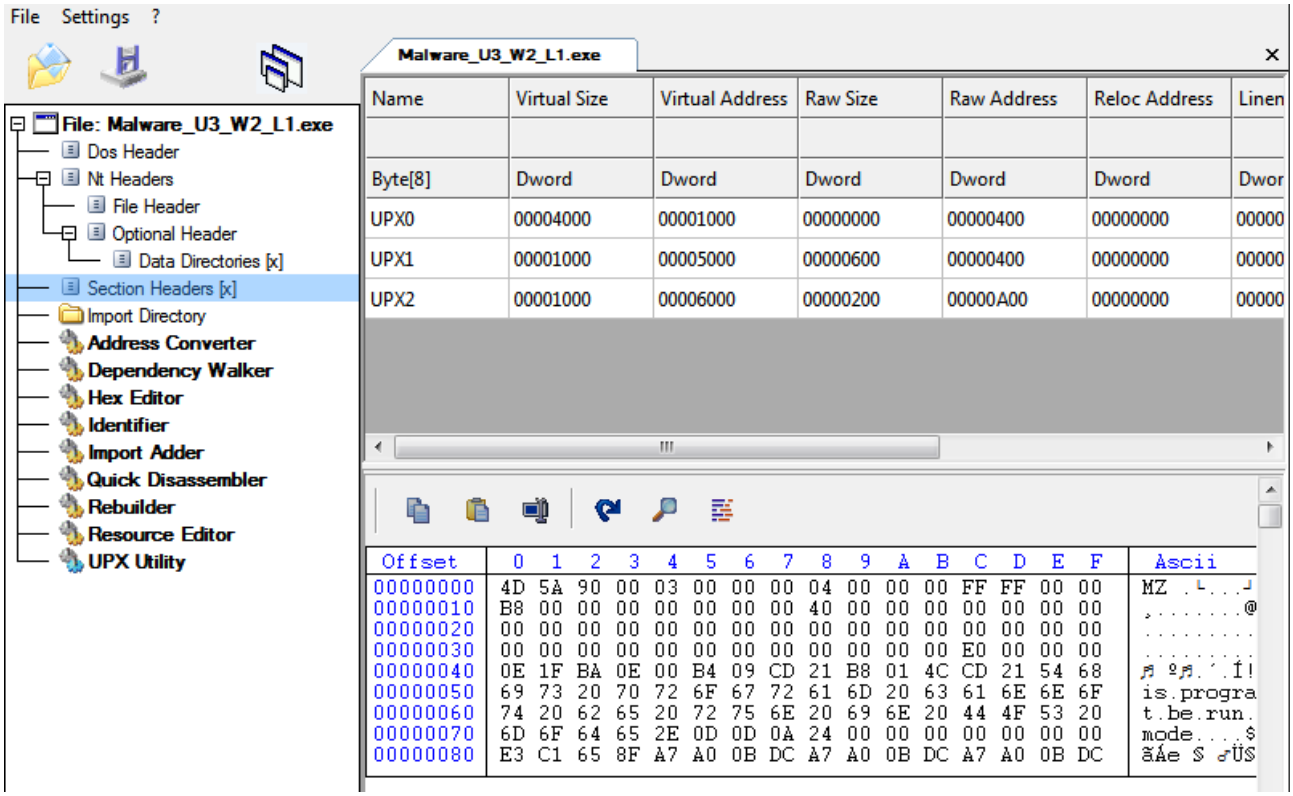
Descrizione: ADVAPI32.dll è una libreria di Windows che contiene le funzioni per l'Advanced Windows 32 Base API. Tra le sue funzionalità ci sono la gestione del Registro di sistema, la sicurezza, la crittografia e l'autenticazione.

MSVCRT.dll:

Descrizione: MSVCRT.dll è la libreria della runtime del compilatore Microsoft Visual C++. Fornisce funzioni standard di runtime per le applicazioni sviluppate con Visual C++.

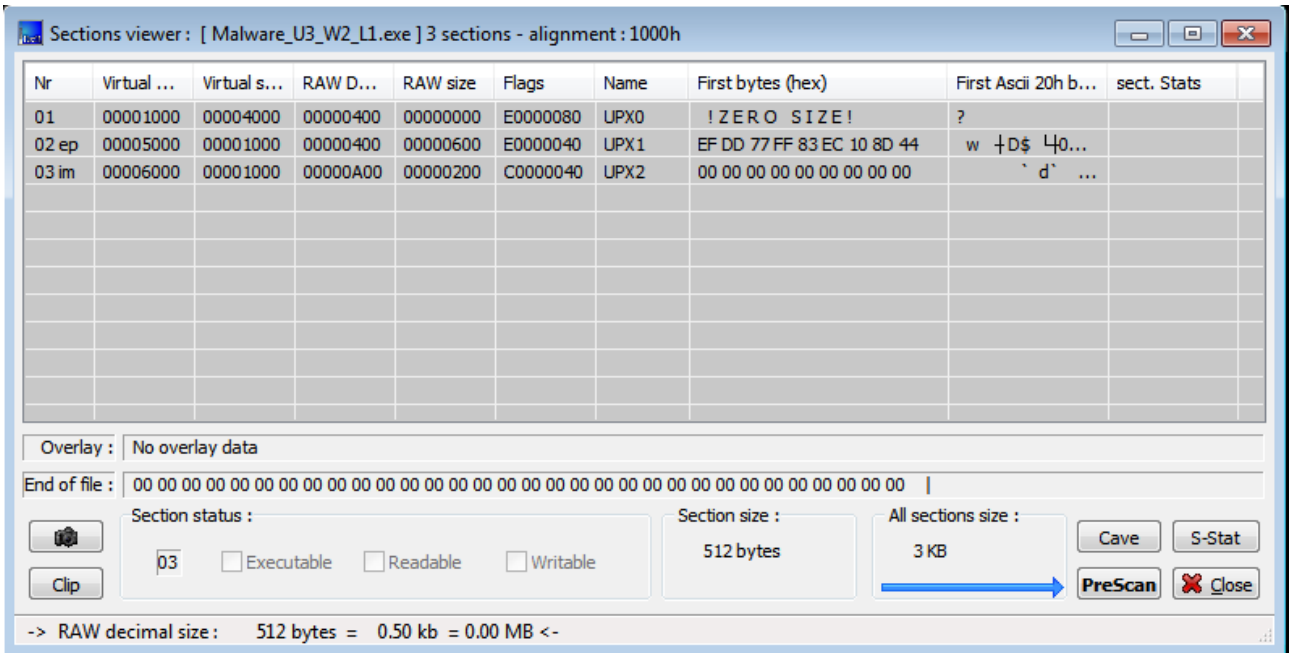
Sezioni del Malware

Durante l'analisi delle sezioni del malware tramite il programma CFF Explorer, è emerso che le sezioni del programma avevano nomi non riconosciuti. Questo ha reso difficile comprendere il funzionamento dettagliato di ciascuna sezione. Tuttavia, è importante notare che la mancanza di nomi comprensibili può essere un segno di tentativi da parte del malware di nascondere il suo comportamento reale.

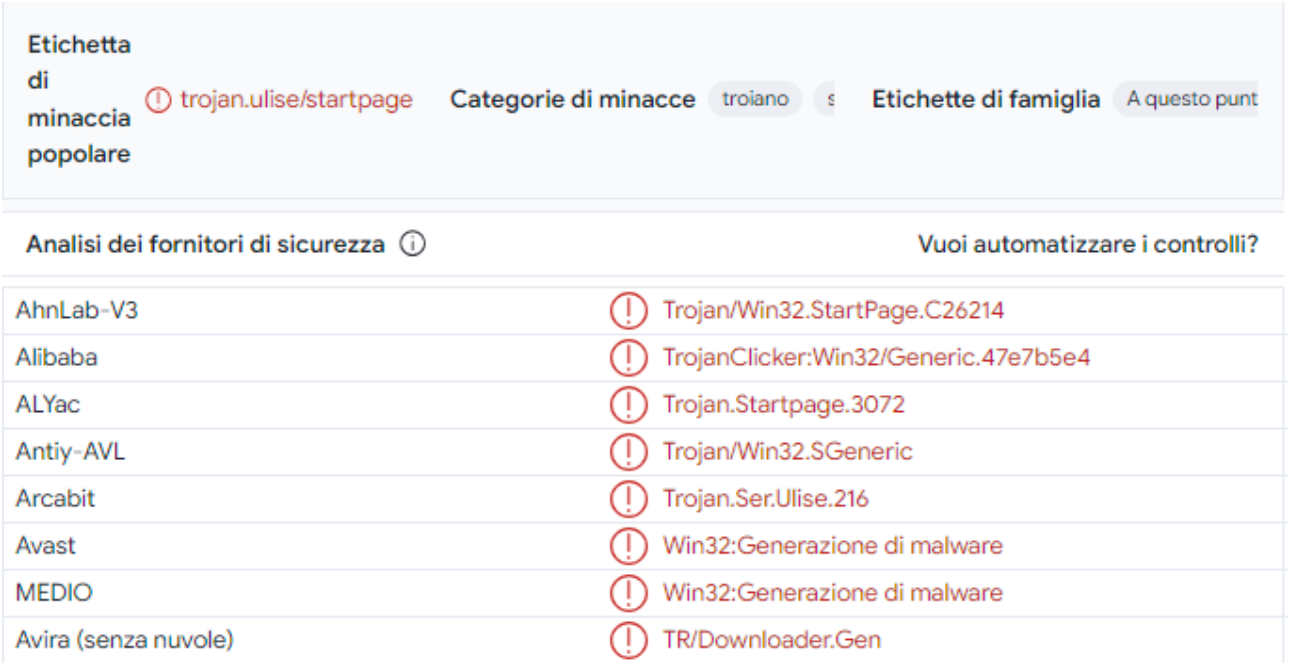


Si è deciso di utilizzare un altro tool adatto a questo tipo di analisi per mostarre le sezioni del codice malevolo. Il programma in questione è stato ExeinfoPE.

Dall'analisi effettuata abbiamo ottenuto lo stesso risultato ottenuto dal programma CFF Explorer; le sezioni presentano sempre dei nomi non riconosciuti per cui non è stato possibile identificare la funzione delle varie sezioni.



Inoltre, l'utilizzo di un hash MD5 del file malware su VirusTotal ha rivelato che il file corrisponde a un trojan noto. Questa corrispondenza suggerisce che il malware è già stato identificato e categorizzato da diverse soluzioni antivirus, indicando una potenziale minaccia conosciuta.



Conclusioni

In conclusione, l'analisi statica del malware ha fornito importanti indicazioni sulle librerie utilizzate e ha sottolineato la presenza di un trojan noto. La mancanza di informazioni dettagliate sulle sezioni del malware sottolinea la sofisticazione delle tecniche utilizzate per nascondere il comportamento. È fondamentale adottare misure di sicurezza adeguate per prevenire e mitigare potenziali danni derivanti da questo tipo di minacce conosciute.

L'identificazione precoce e la risposta tempestiva possono essere chiavi nella gestione di tali rischi per la sicurezza informatica.