

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 con una serie di parametri, come ad esempio il numero di funzioni importate da ciascuna libreria.

Nello screen si possono notare le librerie importate nel programma

Module Name	Imports	OFTs	TimeStamp	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.

The screenshot shows the CFF Explorer interface. On the left, the 'File: Malware_U3_W2_L1.exe' is loaded, and the 'Section Headers [x]' are expanded. The main pane displays a table of sections:

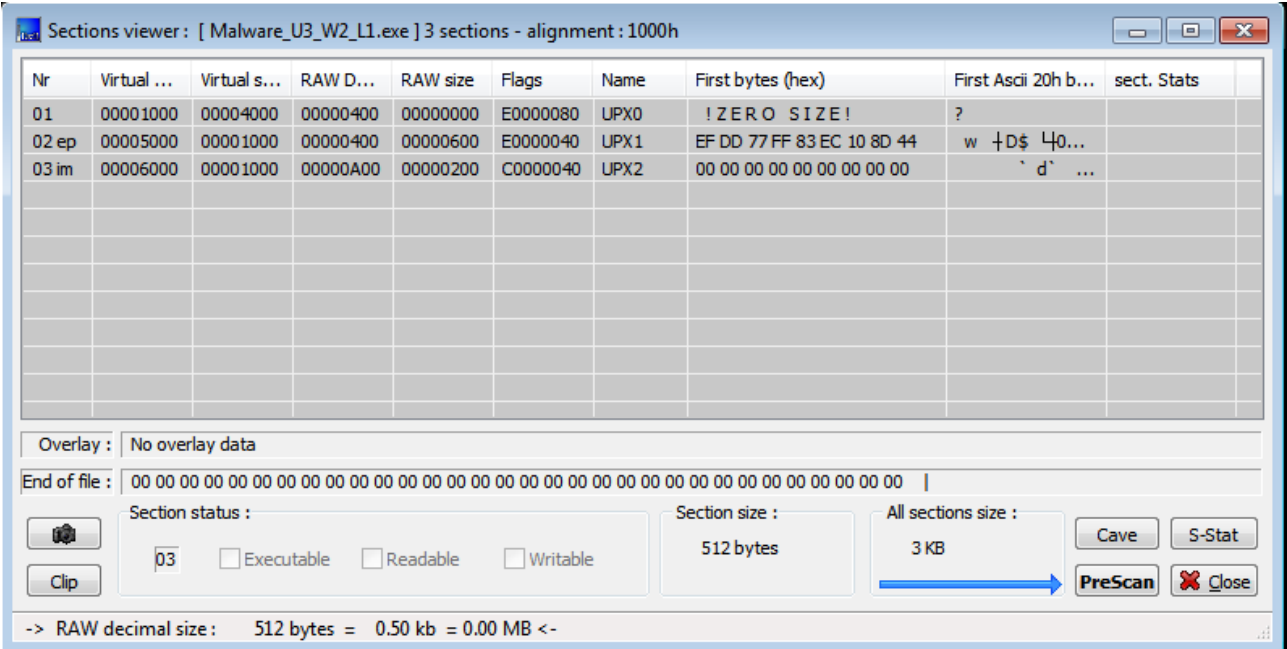
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linen
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000
UPX1	00001000	00005000	00000600	00000400	00000000	00000
UPX2	00001000	00006000	00000200	00000A00	00000000	00000

Below the sections table, the 'Offset' and 'Ascii' columns are visible, showing the raw data and its ASCII representation:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ .L...
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	E0	00	00	00
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	is.progra
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	t.be.run.
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	mode....\$
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	šÁe \$ rŮŠ
00000080	E3	C1	65	8F	A7	A0	0B	DC	A7	A0	0B	DC	A7	A0	0B	DC	

Si è deciso di utilizzare un altro tool adatto a questo tipo di analisi per mostrarre 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.

Etichetta di minaccia popolare

trojan.ulise/startpage

Categorie di minacce

troiano

Etichette di famiglia

A questo punto

Analisi dei fornitori di sicurezza

Vuoi automatizzare i controlli?

AhnLab-V3	Trojan.Win32.StartPage.C26214
Alibaba	TrojanClicker:Win32/Generic.47e7b5e4
ALYac	Trojan.Startpage.3072
Antiy-AVL	Trojan.Win32.SGeneric
Arcabit	Trojan.Ser.Ulise.216
Avast	Win32:Generazione di malware
MEDIO	Win32:Generazione di malware
Avira (senza nuvole)	TR/Downloader.Gen

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.