Malware analysis

S10

Team

GIORNO 1

L1

Analisi Statica Basica

Traccia giorno 1

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:

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

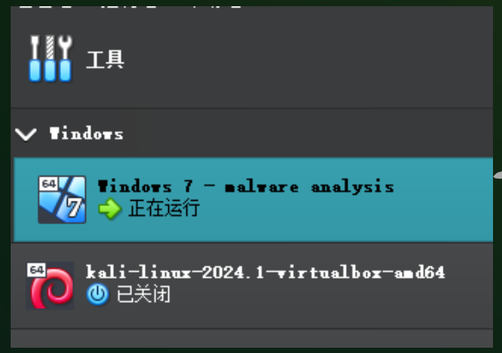
02 Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa

03 Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

Per utilizzare Cff per analizzare il malware, è necessario seguire questi passaggi:

1. Scaricare e installare Windows 7.
2. Aprire la cartella "soft malware".
3. Avviare Cff Explorer.
4. Importare il file "Malware_U3_W2_L1" in Cff Explorer.

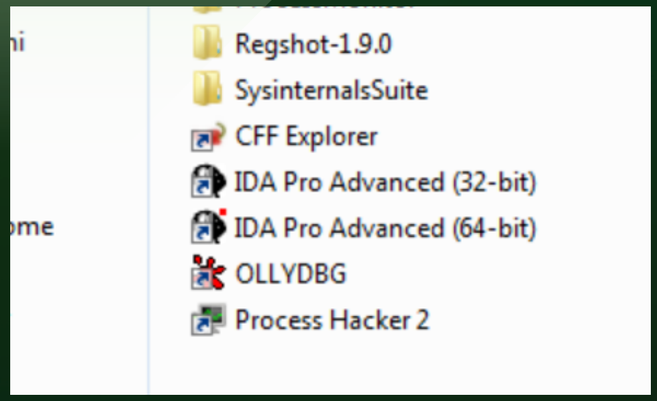
Questi passaggi permetteranno di analizzare il malware utilizzando Cff Explorer su Windows



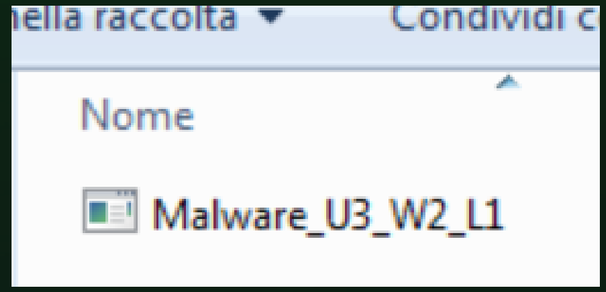
01

02

03



04



CFF Explorer

CFF Explorer è uno strumento avanzato per l'analisi e la modifica di file eseguibili su Windows, parte della suite di strumenti chiamata Explorer Suite, sviluppata da NTCore. È particolarmente utile per programmatori, analisti di malware e ricercatori di sicurezza informatica. Ecco alcune delle sue funzionalità principali:

1. Visualizzazione della struttura dei file PE: Permette di esplorare e modificare le intestazioni e le sezioni dei file Portable Executable (PE), come .exe e .dll.
2. Modifica degli import e degli export: Consente di visualizzare e modificare le tabelle degli import e degli export, essenziali per comprendere le dipendenze di un programma.
3. Risorse del file: Permette di visualizzare e modificare le risorse incorporate nel file, come icone, immagini, stringhe di testo e altri dati.
4. Editor HEX: Include un editor esadecimale per la modifica diretta dei dati binari del file.
5. Disassemblatore: Offre funzionalità di disassemblaggio per analizzare il codice macchina del file eseguibile.

CFF Explorer è utilizzato frequentemente nell'analisi di malware perché consente di esaminare la struttura interna dei file eseguibili sospetti, identificare potenziali comportamenti dannosi e apportare modifiche per ulteriori analisi o mitigazioni.

LIBRERIE IMPORTATE

elenca tutte le funzioni e le librerie esterne che un file eseguibile o una libreria dinamica (.exe o .dll) necessita per funzionare correttamente.

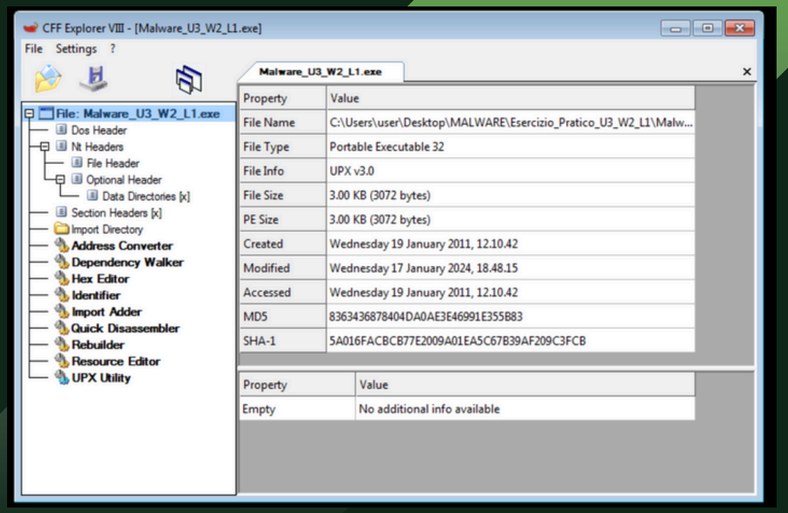
Utilizzando CFF Explorer, vediamo dalla sezione import directory che il malware U3_W2_L1 importa 4 librerie:

1.Kernel32.dll, che include le funzioni core del sistema operativo

2.Advapi32.dll, che include le funzione per interagire con registri e servizi Windows

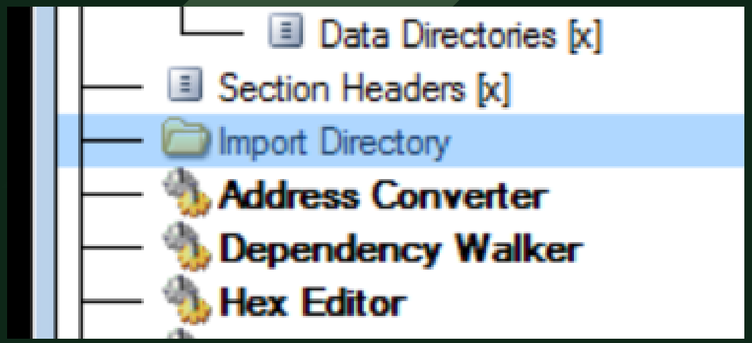
3.MSVCRT.dll, libreria scritta in C per la manipolazione scritte o allocazione memoria

4.Wininet.dll, include le funzione per implementare i servizi di rete come ftp, ntp, http



Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090



SECTION HEADER

testazione delle sezioni (section header) di un file eseguibile (PE, Portable Executable) su Windows è una parte cruciale che descrive le caratteristiche delle diverse sezioni del file. Ogni sezione può contenere codice, dati, risorse o altre informazioni necessarie per l'esecuzione del programma.

Da CFF Explorer, dalla sezione «section header» vediamo che l'eseguibile si compone di 3 sezioni. Purtroppo sembra che il malware abbia nascosto il vero nome delle sezioni e quindi non siamo in grado di capire che tipo di sezioni sono.

Malware_U3_W2_L1.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

Considerazione finale

Si tratta di un malware avanzato che non ci consente di recuperare molte informazioni sul suo comportamento con l'analisi statica basica.
Ciò è supportato dal fatto che tra le funzioni importate troviamo «LoadLibrary e GetProcAddress», che ci fanno pensare ad un malware che importa le librerie a tempo di esecuzione (runtime) nascondendo di fatto le informazioni circa le librerie importate a monte.

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

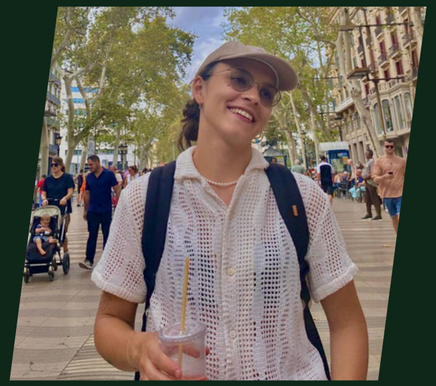
TEAM ALBA

Zhongshi Liu

Mario Marsicano

Luca Lenzi

Giovanni Sannino



Mara Dello Russo

Andre Vinicius

THANK YOU