CS0424IT — ESERCITAZIONE S10L1
ANALISI STATICA MALWARE

Simone La Porta

GitHub

---

29 luglio 2024

INDICE

1 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:

1. Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse.
2. Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa.
3. Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte.

2 SVOLGIMENTO

2.1 *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:

- **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.
- **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.
- **Risorse del file**: permette di visualizzare e modificare le risorse incorporate nel file, come icone, immagini, stringhe di testo e altri dati.
- **Editor HEX**: include un editor esadecimale per la modifica diretta dei dati binari del file.
- **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.

2.2 *Librerie importate*

Utilizzando CFF Explorer, è possibile elencare tutte le funzioni e le librerie esterne che un file eseguibile o una libreria dinamica (.exe o .dll) necessita per funzionare correttamente. Dalla sezione `Import Directory` (mostrata in Figura 2) del malware in esame, risulta che il file importa le seguenti 4 librerie:

1. **Kernel32.dll**: include le funzioni core del sistema operativo.
2. **Advapi32.dll**: include le funzioni per interagire con registri e servizi Windows.

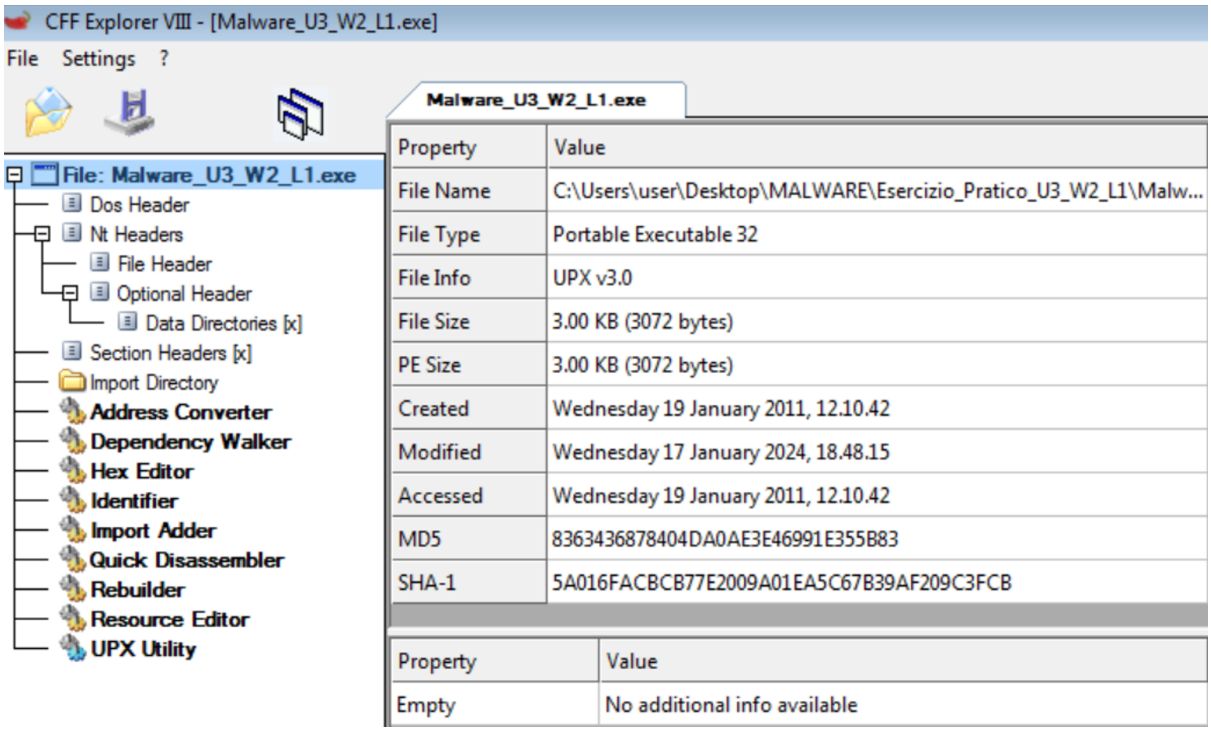


Figura 1: CFF Explorer

3. **MSVCRT.dll**: libreria scritta in C per la manipolazione delle stringhe e l'allocazione della memoria.

4. **Wininet.dll**: include le funzioni per implementare i servizi di rete come FTP, NTP, HTTP.

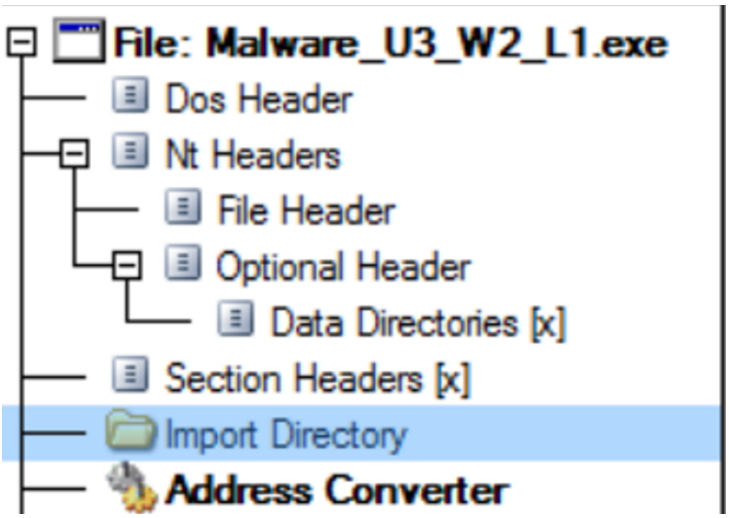


Figura 2: Sezione Import Directory

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

Figura 3: Librerie importate

2.3 *Sezioni del Malware*

L'intestazione 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, nella sezione `Section Header` si può notare che l'eseguibile si compone di 3 sezioni. Purtroppo, sembra che il malware abbia nascosto il vero nome delle sezioni e quindi non si è in grado di capire che tipo di sezioni sono.

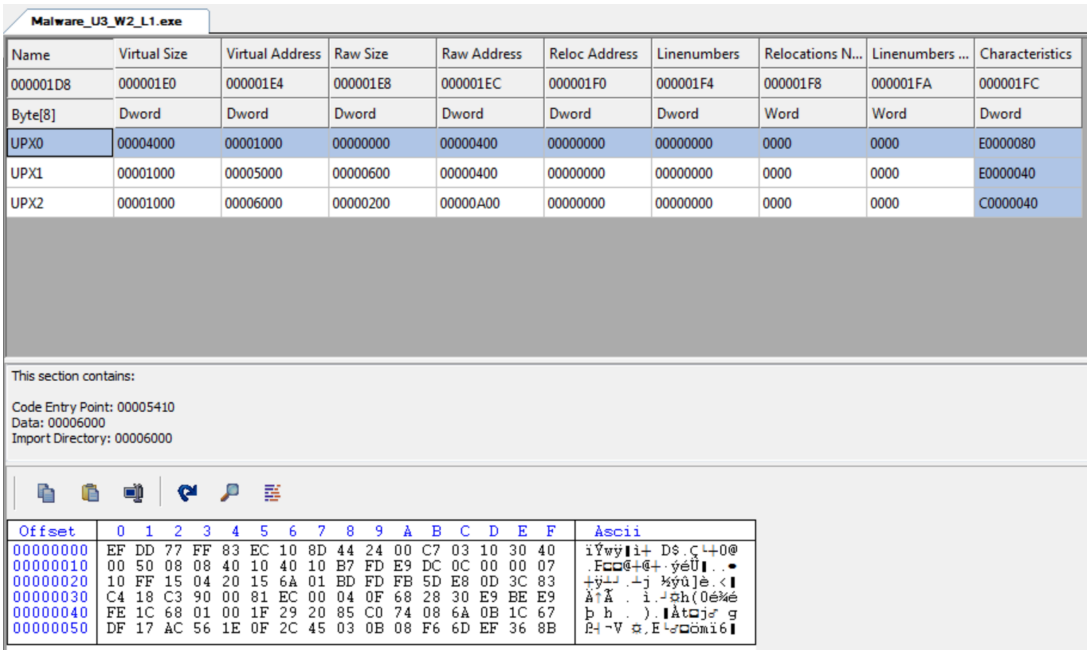
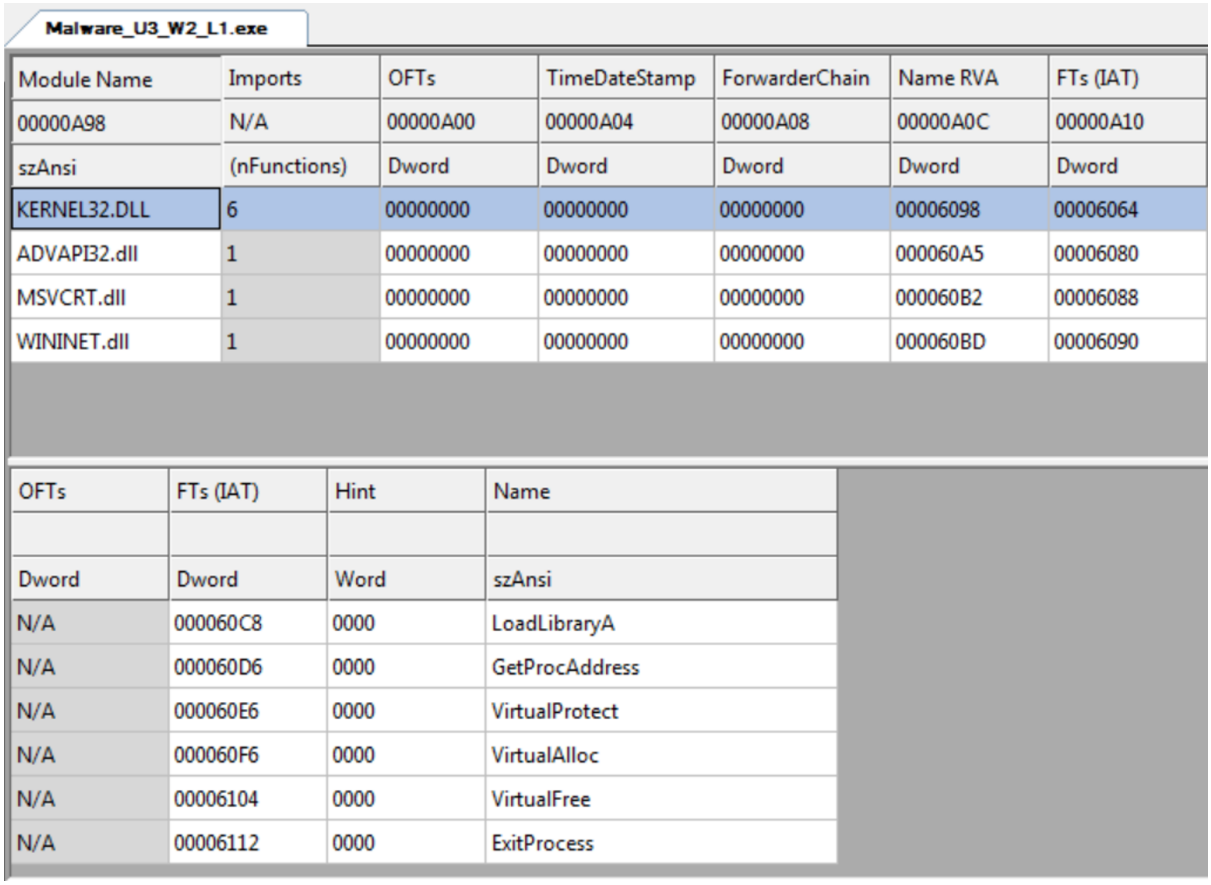


Figura 4: Section Header

2.4 *Considerazioni finali*

Si tratta di un malware avanzato che non consente di recuperare molte informazioni sul suo comportamento con l'analisi statica basica. Ciò è supportato dal fatto che tra le funzioni importate si trovi `LoadLibrary` e `GetProcAddress`, che 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.



Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
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

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