

Report analisi statica malware

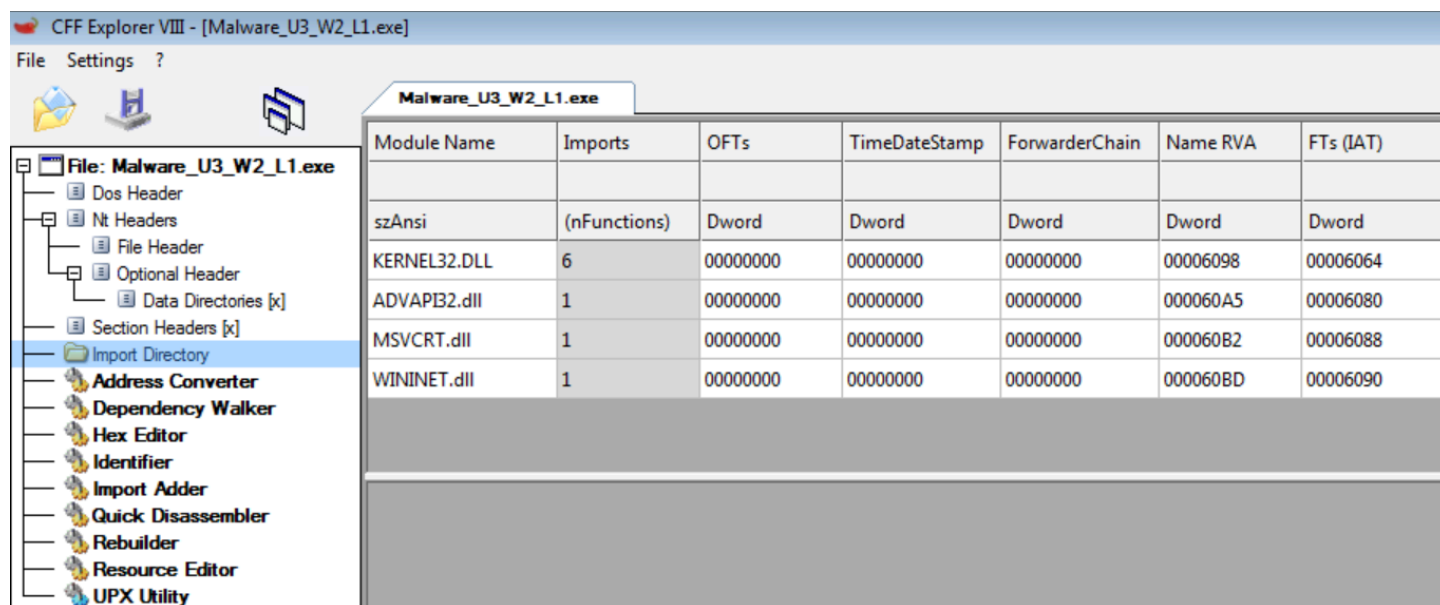
Traccia

Traccia: Esercizio Analisi statica 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

Svolgimento traccia 1

L'immagine mostra la tabella delle importazioni del file eseguibile, evidenziando le librerie DLL (Dynamic Link Library) che il malware carica e utilizza. Ecco una spiegazione delle librerie elencate:



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

KERNEL32.DLL:

Questa è una delle librerie più fondamentali di Windows e contiene funzioni per la gestione della memoria, dei file, dei processi e dei thread, oltre a molte altre funzioni di sistema di basso livello. Il fatto che il malware importi funzioni da questa libreria suggerisce che potrebbe voler manipolare file, gestire processi o eseguire altre operazioni di sistema.

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

File: Malware_U3_W2_L1.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
 - Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

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

ADVAPI32.dll:

La libreria ADVAPI32 contiene funzioni avanzate API di Windows, molte delle quali sono legate alla gestione della sicurezza e delle operazioni del registro. Importare funzioni da questa libreria può indicare che il malware cerca di accedere o modificare voci del registro di sistema o gestire i privilegi e le autorizzazioni degli utenti.

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

File: Malware_U3_W2_L1.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
 - Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000AA5	N/A	00000A14	00000A18	00000A1C	00000A20	00000A24
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	00006120	0000	CreateServiceA

MSVCRT.dll:

Questa libreria è parte del Microsoft Visual C++ Runtime e contiene funzioni di base per la gestione di input/output, stringhe, gestione della memoria e altre operazioni standard in C. Il malware potrebbe usare funzioni da questa libreria per operazioni di calcolo e gestione dei dati.

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

File: Malware_U3_W2_L1.exe

Dos Header

Nt Headers

File Header

Optional Header

Data Directories [x]

Section Headers [x]

Import Directory

Address Converter

Dependency Walker

Hex Editor

Identifier

Import Adder

Quick Disassembler

Rebuilder

Resource Editor

UPX Utility

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000AB2	N/A	00000A28	00000A2C	00000A30	00000A34	00000A38
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	00006130	0000	exit

WININET.dll:

WININET è una libreria di Windows che offre funzioni per l'accesso a Internet, inclusi protocolli come HTTP e FTP. L'importazione di questa libreria è spesso un indicatore che il malware potrebbe tentare di comunicare con server remoti, scaricare o caricare dati, o svolgere altre attività di rete.

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

File: Malware_U3_W2_L1.exe

Dos Header

Nt Headers

File Header

Optional Header

Data Directories [x]

Section Headers [x]

Import Directory

Address Converter

Dependency Walker

Hex Editor

Identifier

Import Adder

Quick Disassembler

Rebuilder

Resource Editor

UPX Utility

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000ABD	N/A	00000A3C	00000A40	00000A44	00000A48	00000A4C
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	00006136	0000	InternetOpenA

Interpretazione

L'uso di queste librerie suggerisce che il malware potrebbe essere progettato per eseguire una serie di operazioni, tra cui:

manipolazione di file e processi (KERNEL32.DLL)

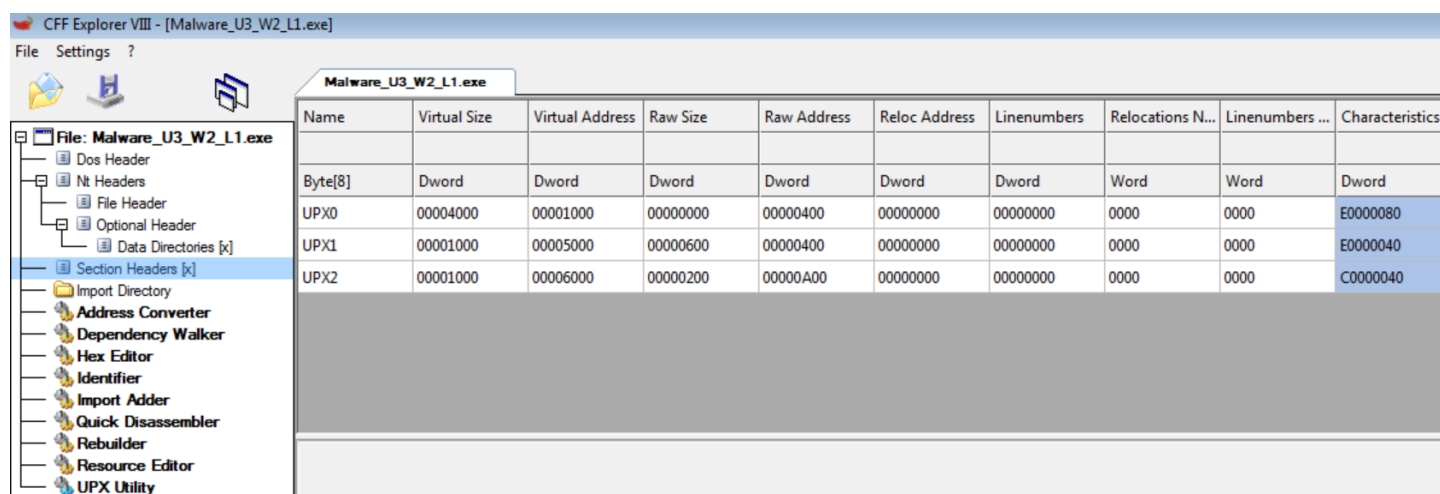
effettuare modifiche al registro di sistema o gestione delle autorizzazioni (ADVAPI32.dll)

comunicazioni di rete (WININET.dll)

operazioni generali di calcolo e gestione dei dati (MSVCRT.dll)

Svolgimento traccia 2

L'immagine mostra una schermata del software **CFF Explorer**, utilizzato per analizzare i file eseguibili di Windows. Nella parte visibile, vediamo la sezione **"Section Headers"**, che contiene informazioni sulle varie sezioni di un eseguibile. Le sezioni indicate sono "UPX0", "UPX1" e "UPX2".



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

Ecco una spiegazione delle sezioni indicate:

UPX0, UPX1, UPX2: Queste sezioni sono etichettate con il prefisso "UPX", che suggerisce che il file è stato compresso utilizzando UPX (Ultimate Packer for eXecutables). **UPX** è un compressore di eseguibili che riduce le dimensioni del file, rendendolo più difficile da analizzare senza decomprimerlo.

UPX0: Tipicamente contiene il codice compresso del programma.

UPX1: Di solito è la sezione che contiene l'originale (non compresso) del programma.

UPX2: Può essere utilizzata per dati o codice aggiuntivi.

Virtual Size: Indica la dimensione della sezione in memoria quando il file viene caricato. Spesso è più grande della dimensione fisica su disco a causa di allineamenti o dati non compressi.

Virtual Address: Questo è l'indirizzo in memoria in cui la sezione sarà caricata.

Raw Size: La dimensione della sezione nel file su disco.

Raw Address: Indica dove inizia la sezione all'interno del file su disco.

Reloc Address e Linenumbers: Questi campi non contengono informazioni significative in questo contesto, spesso sono zero per file compressi o protetti.

Considerazioni finali

Dalle scansioni effettuate in precedenza, è possibile dedurre che il malware in questione stia utilizzando delle librerie e delle funzioni per connettersi ad internet e scaricare altri malware che andranno ad intacchare il sistema operativo e le locazioni della memoria.