

Malware Analysis

Analisi Statica Basica

Traccia:

Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi statica basica.

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

Le librerie importate dal malware sono:

Kernel32.dll: che include le librerie per interagire con il sistema operativo

Advapi32.dll: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft

Msvcrt.dll: contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output in stile linguaggio C

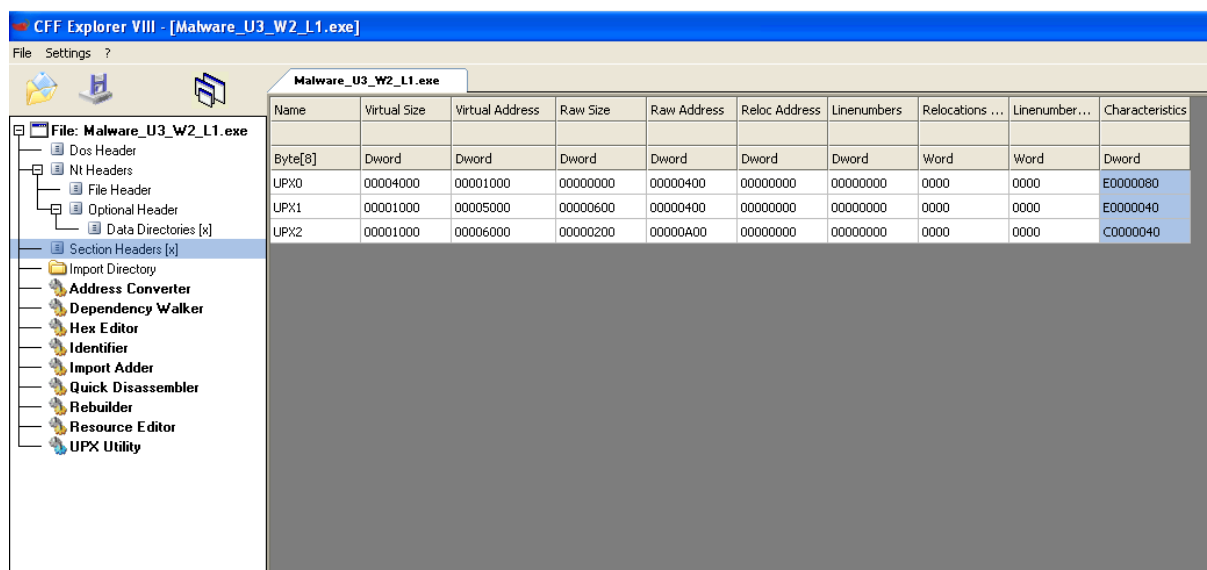
Wininet.dll: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File: **Malware_U3_W2_L1.exe**

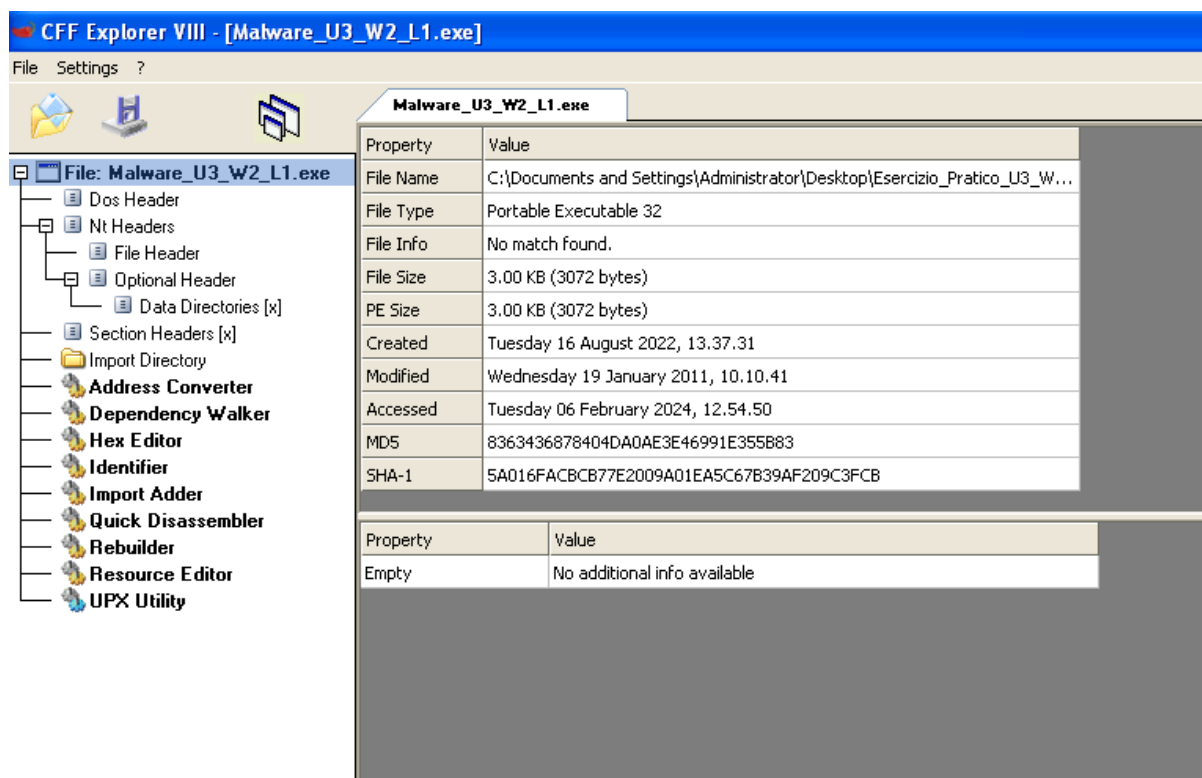
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
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



Dalla sezione Headers possiamo notare che sono presenti 3 componenti del malware, tuttavia non sono stato in grado di rilevare dati interessanti di analisi.

Infine possiamo andare a recuperare l'hash di identificazione del malware dalla pagine iniziale di CFF Explore e andare a cercare su internet se si tratta di un malware noto.



Questa è la scansione da Virus Total:

57

172

Community Score

57 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Size3.00 KB

Last Analysis Date1 hour ago

EXE

Lab01-02.exe

peexe checks-disk-space checks-user-input detect-debug-environment idle long-sleeps upx via-tor

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY30+

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat labeltrojan.ulise/startpage

Threat categoriestrojan downloader

Family labelsulise startpage trojanclicker

Security vendors' analysis

Do you want to automate checks?

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:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/Downloader.Gen
Baidu	Win32.Trojan-Clicker.Agent.ad	BitDefender	Gen:Variant.Ser.Ulise.216