

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:

- 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 esse**
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte**

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

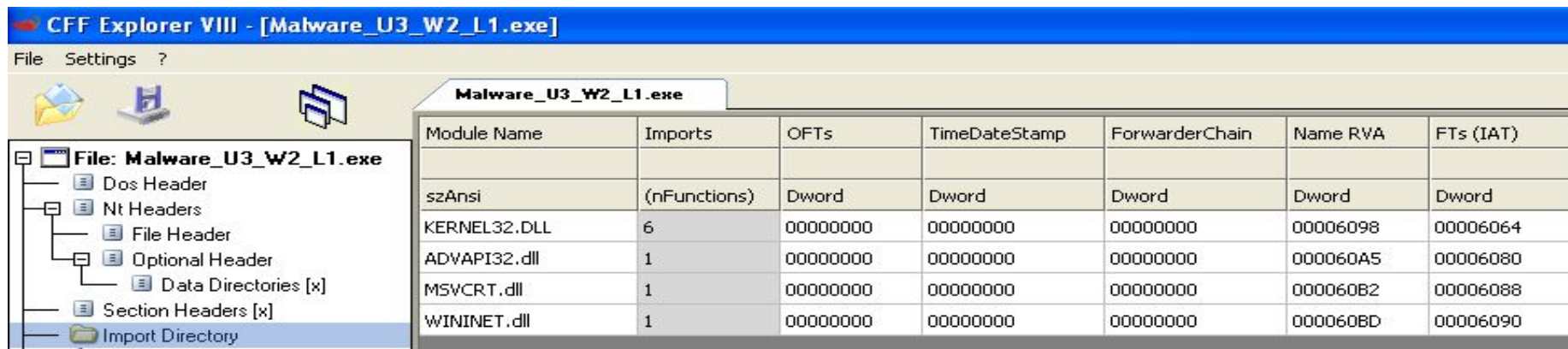
Property	Value
File Name	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W...
File Type	Portable Executable 32
File Info	No match found.
File Size	3.00 KB (3072 bytes)
PE Size	3.00 KB (3072 bytes)
Created	Tuesday 16 August 2022, 13.37.31
Modified	Wednesday 19 January 2011, 10.10.41
Accessed	Monday 27 November 2023, 14.30.33
MD5	8363436878404DA0AE3E46991E355B83
SHA-1	5A016FACBCB77E2009A01EA5C67B39AF209C3FCB

Property	Value
Empty	No additional info available

Per prima cosa ho aperto il file eseguibile **Esercizio_pratico_U3_W2_L1** contenente il malware da analizzare.

Dalla sezione **Import Directory** visualizziamo le librerie che il file eseguibile deve importare per poter funzionare. In questo caso visualizziamo quattro librerie dinamiche:

- **KERNEL32.DLL**: ha al suo interno le funzioni principali che servono al malware per interagire con il sistema operativo
- **ADVAPI32.DLL**: contiene le funzioni per interagire con i registri del sistema operativo
- **MSVCRT.DLL**: contiene le funzioni per manipolare le stringhe e l'allocazione della memoria
- **WININET.DLL**: contiene le funzioni per implementare alcuni protocolli HTTP, NTP e FTP



CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

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

Ogni libreria, sulla colonna **(nFuncionts)** mostra il numero di funzioni che quella singola libreria contiene. Per esempio, la libreria KERNEL32.DLL contiene **9 funzioni** una volta spaccettato il file dalla funzione di CFF Explorer alla voce **UPX Utility**.

Alla voce **section headers** si visualizzano le sezioni di cui si compone il malware:

Malware_U3_W2_L1.exe									
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000002DC	00001000	00001000	00001000	00000000	00000000	0000	0000	60000020
.rdata	00000372	00002000	00001000	00002000	00000000	00000000	0000	0000	40000040
.data	0000008C	00003000	00001000	00003000	00000000	00000000	0000	0000	C0000040

Le tre sezioni di cui si compone il malware sono:

.text, .rdata e .data

- **.text**: contiene le istruzioni che la CPU deve eseguire una volta che il software viene avviato.
- **.rdata**: include le informazioni sulle librerie e le funzioni eseguite dal software.
- **.data**: contiene le variabili globali del file eseguibile che devono essere accessibili da qualsiasi parte del programma e non solo a seguito di una specifica funzione

Da un' ulteriore analisi vediamo come una volta caricato il file su CFF Explorer questo ci fornisca il codice HASH **8363436878404da0ae3e46991e355b83**. Andandolo ad inserire su Virus Total, otteniamo il seguente risultato:

57

172

Community Score

57 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Size
3.00 KB

Last Analysis Date
21 hours 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

COMMUNITY 30 +

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

Popular threat label **trojan.ulise/startpage**

Threat categories trojan downloader

Family labels ulise 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
BitDefenderTheta	Gen:NN.ZexaF.36792.amGfaWi867f	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Malware.Agent-6350563-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.chek77	Cybereason	Uusefa

Vediamo come per **57** vendors su **72** il file rappresentato dal codice Hash sia un Malware, nello specifico potrebbe essere un Trojan.

Vediamo sui dettagli del file che si tratta di un eseguibile:

File type Win32 EXE executable windows win32pe peexe

Vediamo come il file sia stato compresso con **UPX**, utilizzato per ridurre la dimensione dei file e renderli meno individuabili da parte dell'utente o dell'antivirus.