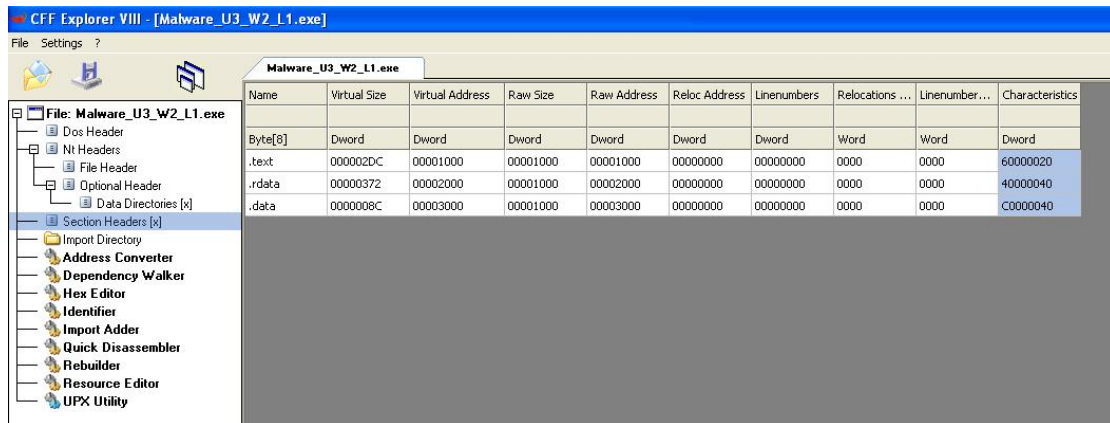


# ESERCIZIO S10/L1

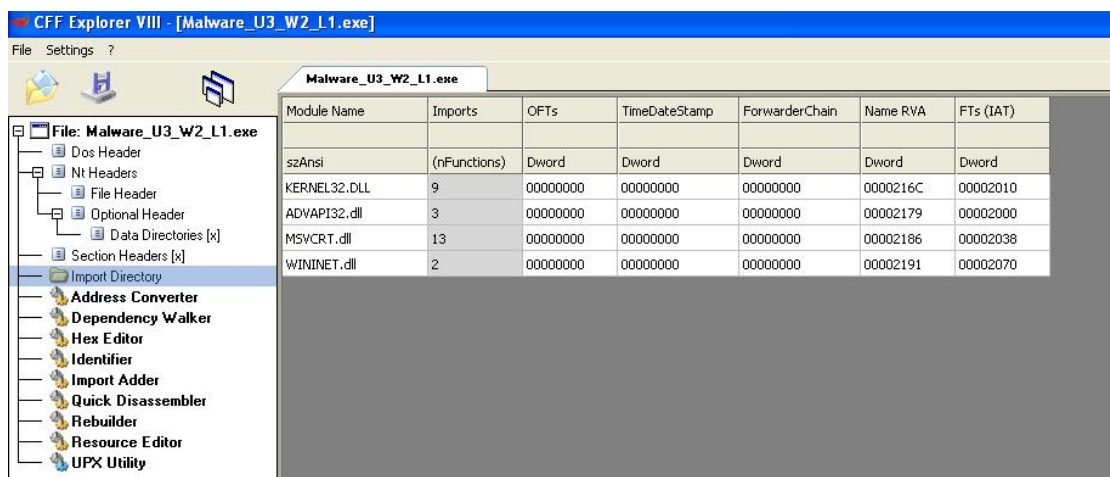
Avendo un file sospetto possiamo analizzarlo usando CFF Explorer, un programma che analizza il file e che ci mostra il suo contenuto.



.text: contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato.

.rdata: include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer.

.data: contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.



Kernel32.dll: contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.

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

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

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

Sempre da CFF explorer ricaviamo persino l’hash del programma  
8363436878404da0ae3e46991e355b83

E usiamo il sito “virustotal” per verificare se è sicuro. Ed in effetti come possiamo veder si tratta di un troian.

57  
/ 172

Community Score

57 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Size3.00 KB

Last Analysis Date22 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

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.S/Generic
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.amGfaW/867f	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Malware.Agent-6350563-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.cbcb77	Cylance	Unsafe
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
DrWeb	Trojan.Click3.12740	Elastic	Malicious (moderate Confidence)
Emsisoft	Gen:Variant.Ser.Ulise.216 (B)	eScan	Gen:Variant.Ser.Ulise.216