

U3 W10 L1

Analisi statica Malware

Vincenzo Colletta

Creazione dell'Hash

Per capire con che tipo di file abbiamo a che fare, andiamo a creare un hash del file, tramite un tool chiamato md5deep.

Una volta creato l'hash, andiamo ad inserirlo su Virustotal, che confronterà il nostro hash con la tabella da lui memorizzata, così da darci alcune informazioni generali.

Prompt dei comandi

Microsoft Windows XP [Versione 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\io>pwd
"pwd" non è riconosciuto come comando interno o esterno,
un programma eseguibile o un file batch.

C:\Documents and Settings\io>cd desktop

C:\Documents and Settings\io\Desktop>ls
"ls" non è riconosciuto come comando interno o esterno,
un programma eseguibile o un file batch.

C:\Documents and Settings\io\Desktop>cd nuova cartella
C:\Documents and Settings\io\Desktop\Nuova cartella>cd md5deep-4.3

C:\Documents and Settings\io\Desktop\Nuova cartella\md5deep-4.3>md5deep Malware_U3_W2_L1.exe
8363436878404da0ae3e46991e355b83 C:\Documents and Settings\io\Desktop\Nuova cartella\md5deep-4.3\Malware_U3_W2_L1.exe

C:\Documents and Settings\io\Desktop\Nuova cartella\md5deep-4.3>_

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

57
/ 72

Community Score

57 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Size 3.00 KB

Last Analysis Date 22 hours ago

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)

Librerie importate

Analizzando il contenuto del Malware attraverso l'uso di VirusTotal, ci rendiamo conto che queste sono le librerie contenute all'interno del file.

Imports

- + ADVAPI32.dll
- + KERNEL32.DLL
- + MSVCRT.dll
- + WININET.dll

ADVAPI32.dll:

Descrizione: Fornisce molte funzioni avanzate per la gestione dei servizi, la sicurezza, il registro di sistema e altri aspetti critici del sistema.

KERNEL32.dll:

Descrizione: Contiene le funzioni di base del kernel del sistema operativo, inclusi gestione memoria, processi, file, input/output, e altro ancora. È fondamentale per molte operazioni di basso livello su Windows.

MSVCRT.dll:

Descrizione: Questa libreria fornisce funzioni di runtime della libreria Microsoft Visual C++, come gestione della memoria, input/output, matematica e altro ancora.

WININET.dll

Descrizione: Questa libreria è utilizzata per l'accesso a Internet, fornendo funzioni per la comunicazione con server tramite vari protocolli (HTTP, FTP, etc.) e la gestione dei dati scambiati.

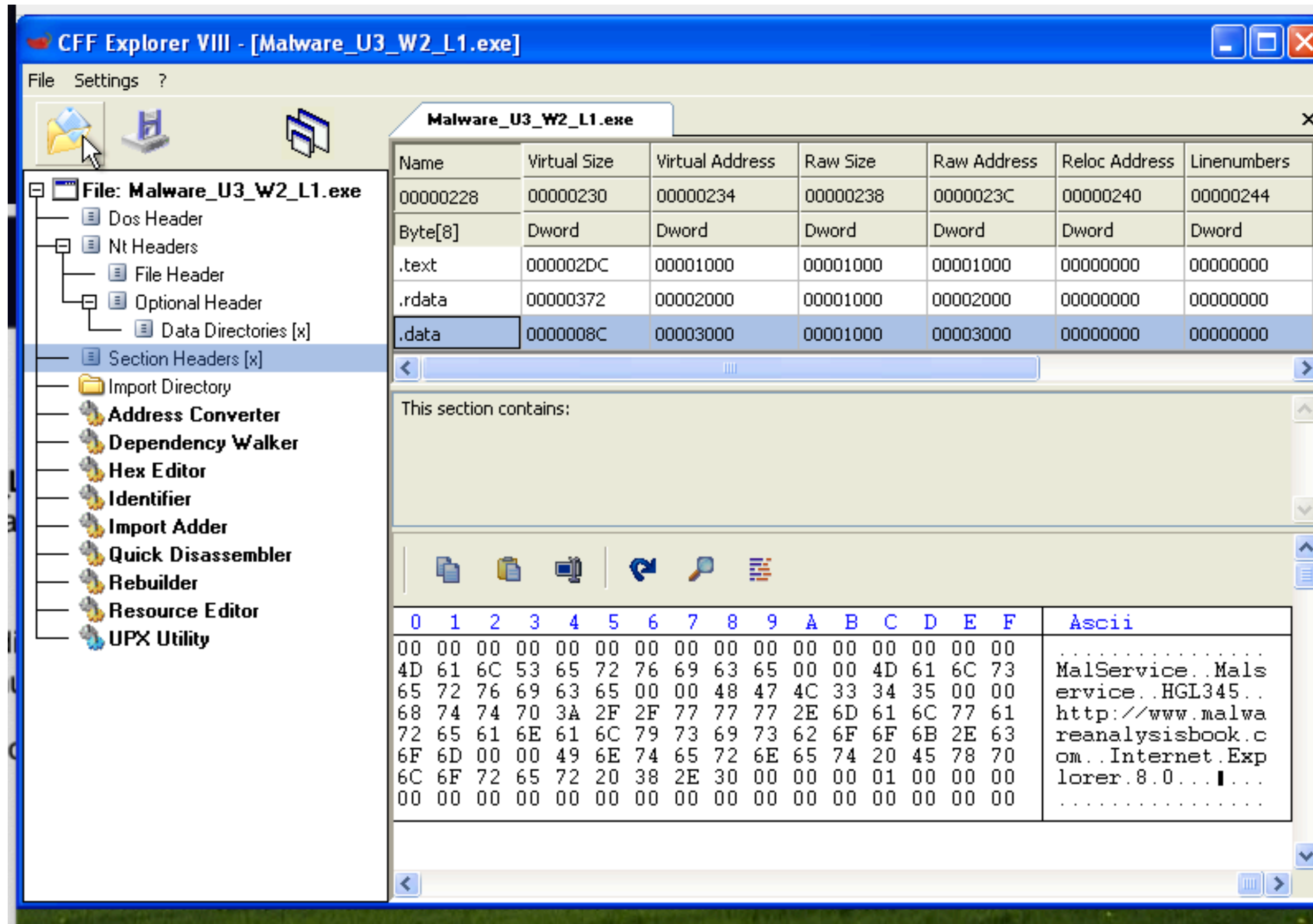
Sezioni del Malware

Qui vediamo le sezioni del Malware:

.text: Contiene la sezione ESEGUIBILE del programma. Spesso è la parte principale del Malware, contenente le istruzioni eseguibili.

.data: Questa sezione contiene dati variabili utilizzati durante l'esecuzione del programma. Potrebbe includere informazioni come configurazioni, variabili o altri dati necessari al malware.

.rdata: Questa sezione solitamente contiene dati in sola lettura, come costanti o stringhe che il malware utilizza durante l'esecuzione.



Considerazioni

L'uso di librerie di sistema comuni come ADVAPI32.dll, KERNEL32.dll, MSVCRT.dll e WININET.dll non è necessariamente indicativo di un malware, in quanto queste librerie sono ampiamente utilizzate dalle applicazioni legittime su Windows per svolgere diverse funzioni.

Tuttavia, l'analisi delle sezioni del malware potrebbe indicare un possibile comportamento dannoso, poiché le sezioni .text, .data e .rdata spesso contengono istruzioni eseguibili, dati variabili e costanti utilizzati dal malware durante la sua esecuzione.

La presenza di queste sezioni potrebbe suggerire che il file in questione sia un eseguibile che richiama queste librerie di sistema per eseguire operazioni, ma senza ulteriori informazioni o un'analisi più dettagliata del contenuto del file, non è possibile determinare con certezza se si tratti di un malware.