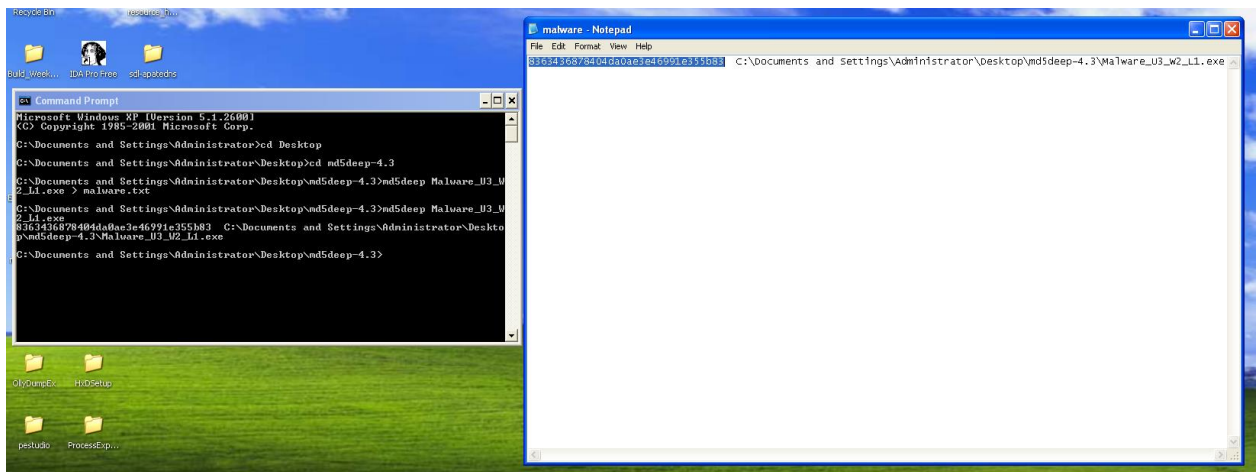


# Analisi Malware Statica


Nell'esercizio di oggi analizziamo staticamente un malware presente su macchina virtuale Windows XP. Il malware in questione è denominato “**Malware\_U3\_W2\_L1**” ed useremo gli strumenti di analisi **VirusTotal** e **CFF Explorer**.

## Analisi Malware: ricerca hash su VirusTotal

Per prima cosa, ricaviamo le **hash** dell'eseguibile utilizzando **md5deep**, come mostrato nell'immagine sottostante: a sinistra le hash nel terminale mentre a destra in output in un file di testo.



Prendiamo l'hash forniteci e lo inseriamo nel tool online **VirusTotal**: in questo modo, se il malware è già stato incontrato ed analizzato, possiamo vedere i dettagli del file e capire il tipo di eseguibile che stiamo indagando. Nel nostro specifico caso, il malware in questione è presente sul database del sito: possiamo vedere che è un **trojan** riconosciuto dalla maggior parte degli anti-malware considerati.

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: 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.amGfaWl867f	Bkav Pro	W32:AlDetectMalware

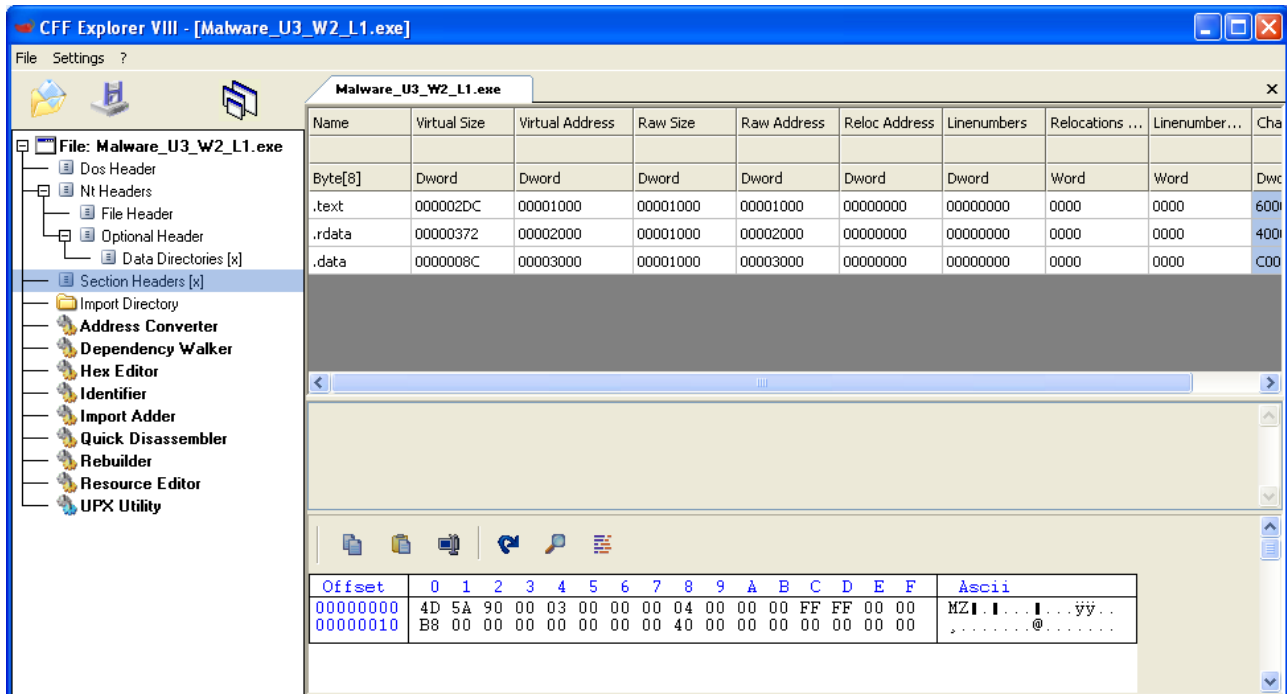
Continuando la nostra indagine sul sito, possiamo vedere come il malware stesso vada ad **aprire** delle **connessioni con altri IP** qui specificati; possiamo immaginare che si tratti di un **downloader**, ossia di un malware in grado di scaricare file autonomamente una volta avviato.

Contacted Domains (34) ⓘ			
Domain	Detections	Created	Registrar
106.89.54.20.in-addr.arpa	1 / 88	-	-
125.21.88.13.in-addr.arpa	2 / 88	-	-
154.210.82.20.in-addr.arpa	1 / 88	-	-
183.209.82.20.in-addr.arpa	1 / 88	-	-
2.155.190.20.in-addr.arpa	0 / 88	-	-
212.161.61.168.in-addr.arpa	1 / 88	-	-
234.151.42.104.in-addr.arpa	1 / 88	-	-
234.173.86.20.in-addr.arpa	1 / 88	-	-
25.140.123.92.in-addr.arpa	1 / 88	-	-
254.11.238.8.in-addr.arpa	0 / 88	-	-

Contacted IP addresses (59) ⓘ			
IP	Detections	Autonomous System	Country
104.86.182.10	0 / 88	20940	US
104.86.182.50	0 / 88	20940	US
104.96.203.51	0 / 88	20940	US
104.99.239.138	0 / 88	20940	US
13.107.39.203	1 / 88	8068	US
13.107.4.50	4 / 88	8068	US
13.224.247.103	0 / 88	16509	US
13.224.247.119	0 / 88	16509	US
13.224.247.16	0 / 88	16509	US
13.224.247.21	0 / 88	16509	US
131.253.33.203	0 / 88	8068	US

## Analisi tramite CFF Explorer.

Volendo andare più nel dettaglio, analizziamo ulteriormente il malware utilizzando **CFF Explorer**, ottenendo gli **headers** e le **librerie** da cui dipende il software. Analizziamo di seguito gli headers messi in evidenza nell'immagine sottostante.

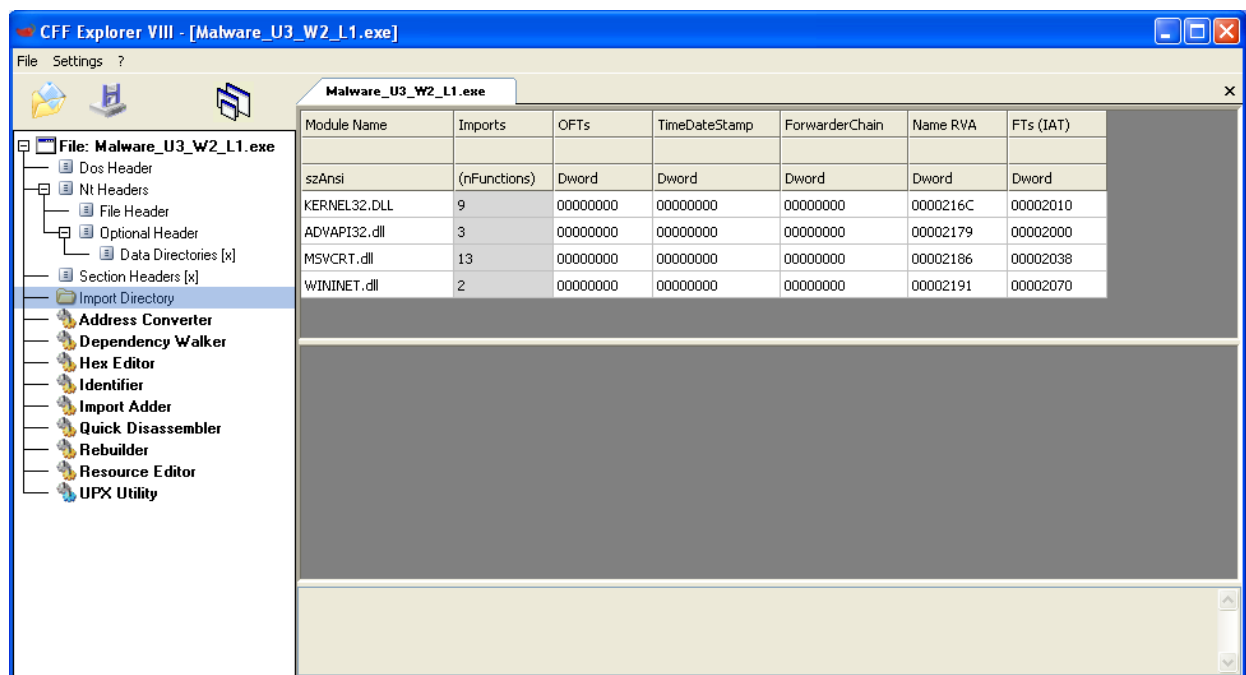


Gli headers possono darci un'idea del funzionamento del malware:

- **.text** : contiene le istruzioni che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto;
- **.rdata** : include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile;
- **.data** : contiene tipicamente i dati e le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

Analizziamo di seguito le librerie individuate, come mostrate nell'immagine a fine presentazione:

- **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.



Ricapitolando, il malware preso in esame è un **trojan** il cui scopo è probabilmente quello di collegarsi a predeterminati indirizzi IP e scaricare da essi altri file autonomamente.