# ANALISI STATICA BASICA MALWARE

Pignatello Giuseppe

# TABLE OF CONTENTS

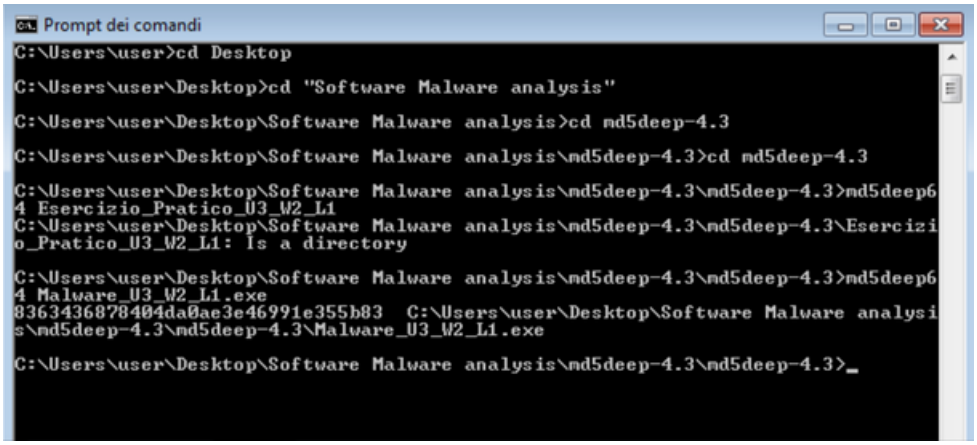
# TIPI DI ANALISI

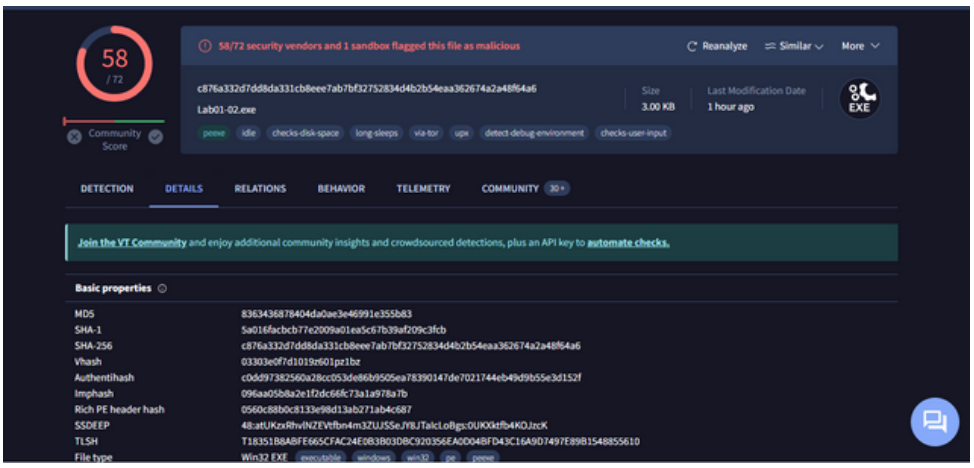
L'analisi statica di un Malware fornisce tecniche e strumenti per analizzare il comportamento di un malicious software senza eseguirlo, a differenza dell'analisi dinamica che presuppone l'esecuzione del Malware in ambiente controllato. Queste due tecniche sono complementari, per un'analisi efficace i risultati dell'analisi statica devono essere confermati dalle analisi dinamiche. Entrambe le tecniche si dividono in "basica" e "avanzata".
Le varie analisi vanno effettuate seguendo questo ordine:
Analisi statica basica --> Analisi dinamica basica --> Analisi statica avanzata --> Analisi dinamica avanzata

Ogni analisi ci permette di rispondere a una domanda ben precisa, cosi da comprendere appieno le funzionalità del Malware.
L'analisi statica basica ci permette di rispondere alla domanda "Cosa dovrebbe fare il Malware?", l'analisi dinamica basica invece ci fa rispondere alla domanda "Cosa fa?", L'analisi statica avanzata "Come lo fa?" e l'analisi dinamica avanzata infine "Come lo fa passo passo?".

# RICAVO HASH (MD5)

A cosa serve ricavare l'hash da un Malware?
Ci permette di effettuare ricerche su internet sul malware, senza rischiare di infettare il nostro computer. Per ricavarlo, esiste un tool, chiamato md5deep-4.3. Per utilizzarlo ci spostiamo di directory fino ad arrivare alla directory "md5deep-4.3" e eseguiamo il comando md5deep64 "nome Malware", in questo caso quindi md5deep64 "Malware_U3_V2_L1".
Il nostro hash è "8363436878404da0ae3e46991e355b83".
Adesso, cerchiamo l'Hash su Virus Total, questo è il risultato:




Come vediamo, Virus total ci conferma che il file è un file malevolo e ci da qualche idea di quello che potrebbe essere, ovvero un trojan downloader.

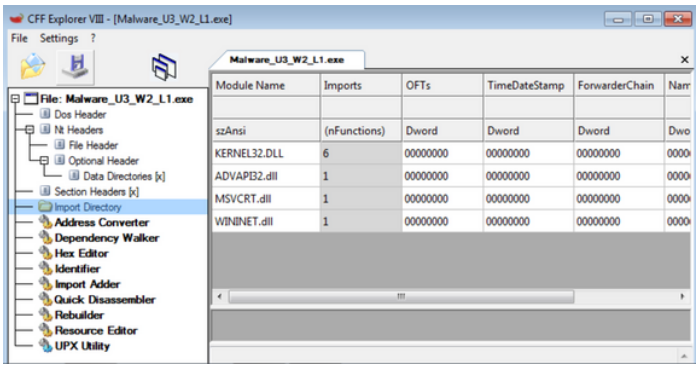
Piignatello Giuseppe

# LIBRERIE E SEZIONI UTILIZZATE

Utilizzando il tool CFF Explorer, abbiamo la possibilità di vedere le librerie e le sezioni dell'header che sono state utilizzate per costruire il Malware. Le librerie note sono:
Kernel32.dll = contiene le principali funzioni per interagire col Sistema Operativo
Advopi32.dll = contiene le funzioni per interagire con i servizi e i registri del Sistema Operativo
WSock32.dll e Ws2-32.dll = contengono funzionalità di network, come i socket, le funzioni connect e bind (Usate quando il malware usa funzionalità di rete).
Wininet.dll = contiene funzioni per implementare protocolli (come HTTP, FTP)
Gdi32.dll = contiene funzioni per l'implementazione e la manipolazione della GUI
MSVCRT.dll = contiene funzioni per manipolare le stringhe e l'allocazione di memoria.

Per quanto riguarda invece le sezioni, le più utilizzate sono:
.text = contiene le istruzioni che la CPU eseguirà una volta che il software sarà avviato.
.data = include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile
.rsrc = contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma
.rdata = include le risorse utilizzate dall'eseguibile come ad esempio icone, immagini, menu e stringhe che non sono parte dell'eseguibile stesso.

Ecco cosa abbiamo ricavato utilizzando CFF Explorer:




Per quanto riguarda le sezioni, erano nascoste e non ci hanno portato a nulla, esistono però dei codici scritti in C++ che permettono di spacchettare queste sezioni e capire cosa c'è al loro interno.

Pignatello Giuseppe

# CONSIDERAZIONE FINALE

Il Malware potrebbe essere un Trojan Loader, in primo luogo perchè le ricerche tramite Virus Total ce lo lasciano pensare, ma in secondo luogo perchè, andando a dare un'occhiatta all'interno delle librerie, erano presenti librerie che aprivano internet e altre librerie che facevano partire dei cicli, che farebbero pensare ai download di ulteriori Malware. Per evitare di incorrere in queste situazioni spiacevoli consigliamo sempre di scaricare risorse solo da siti affidabili, aggiornare costantemente il sistema operativo, non aprire link e fare delle scansioni costantemente per monitorare il traffico di rete.

# GRAZIE PER L'ATTENZIONE!