U3 W10 L1

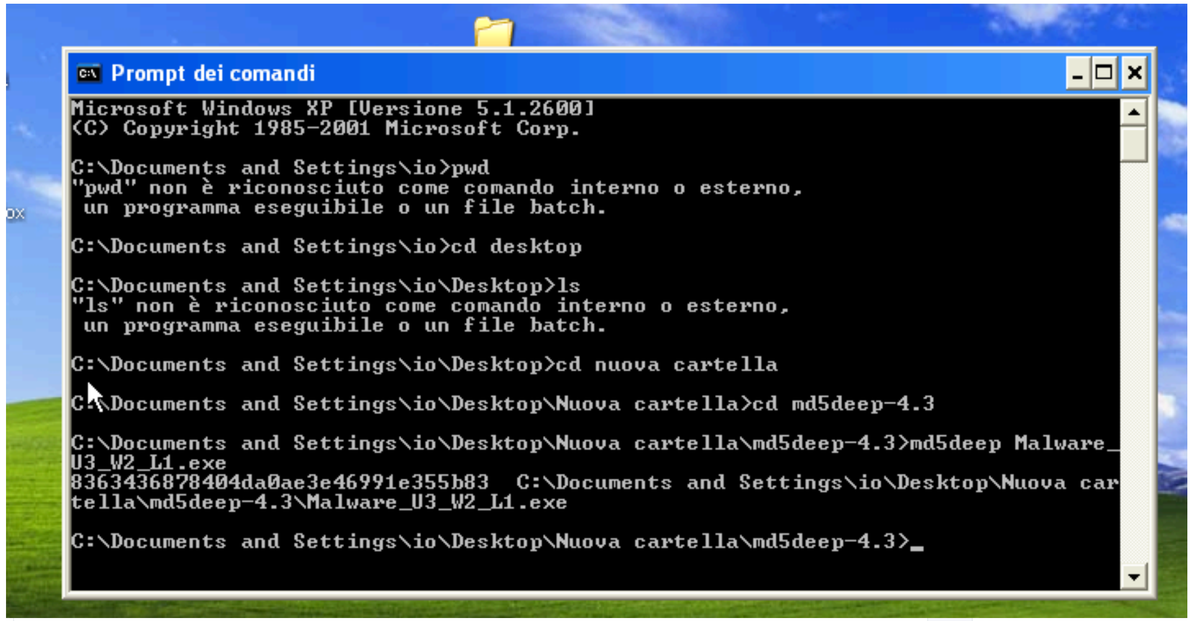
Analisi statica Malware

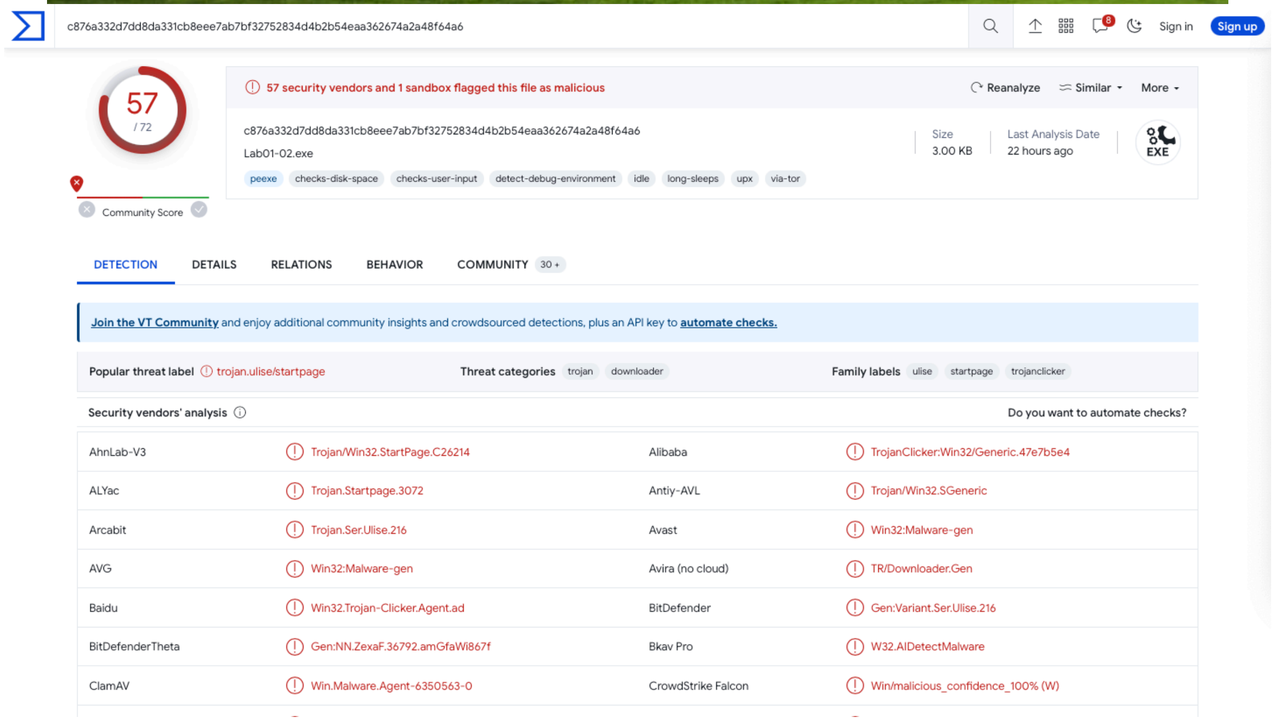
Vincenzo Colletta

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.





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.

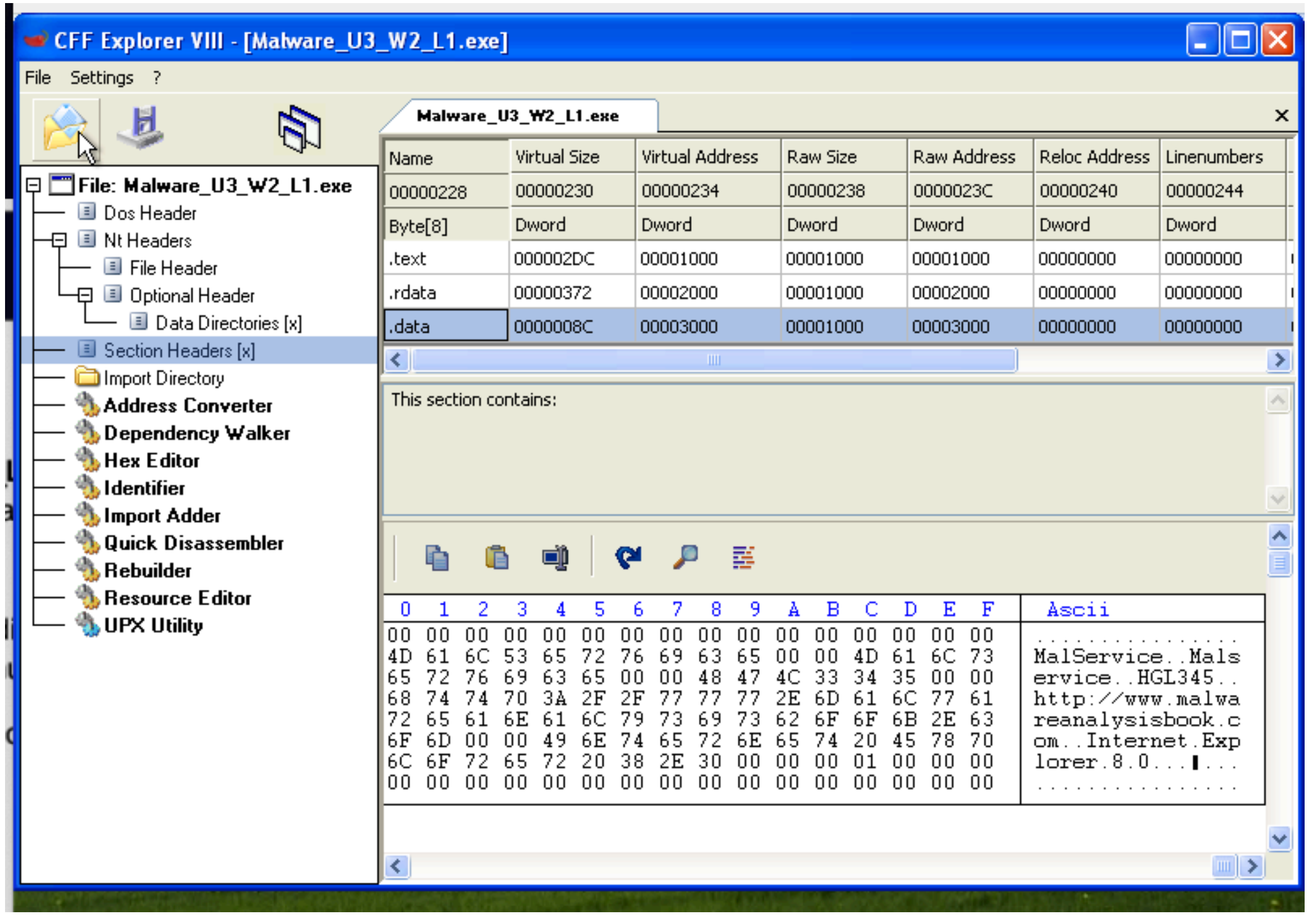
ADVAPI32.dll:
Descrizione: Fornisce molte funzioni avanzate per la gestione dei servizi, la sicurezza, il registro di sistema e altri aspetti critici del sistema.

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.