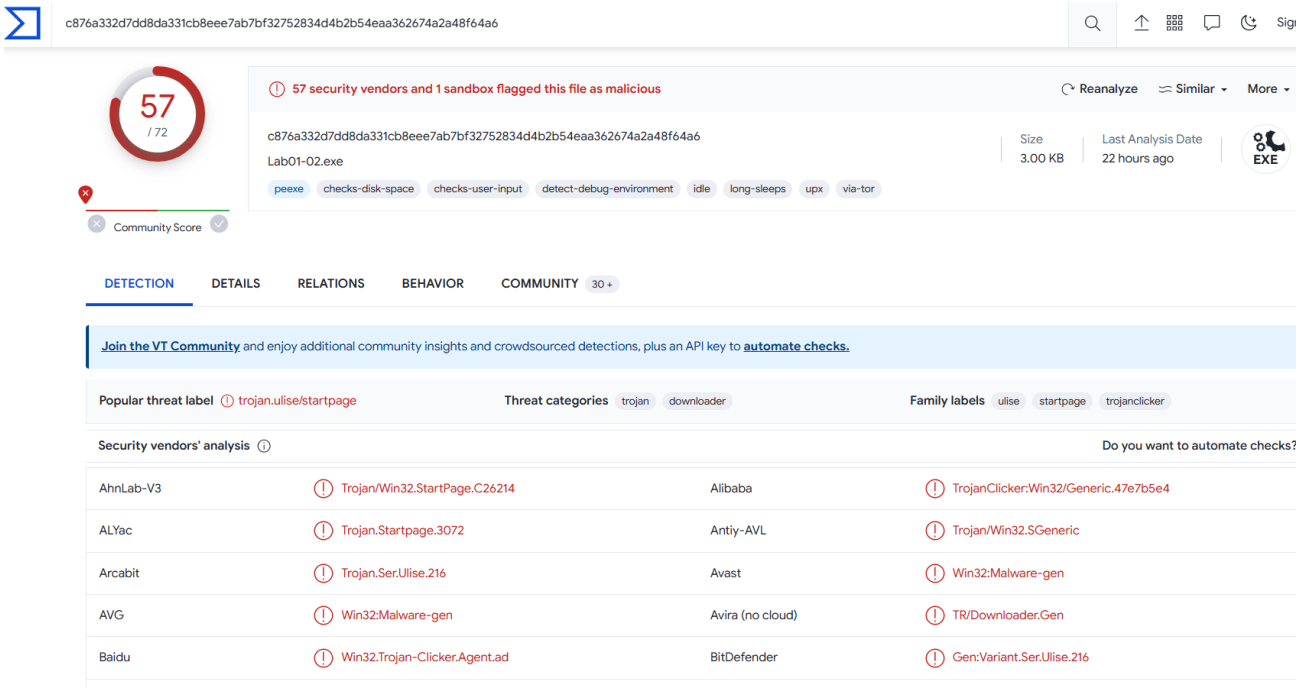
Analisi statica basica

Il Malware è un **Trojan:**



Il Trojan è un tipo di malware che si nasconde come software affidabile per infiltrarsi nel sistema senza essere rilevato. Una volta all'interno, può rubare dati, danneggiare il sistema o fornire accessi non autorizzati. Si maschera da software legittimo e si diffonde tramite email, link sospetti o altre vulnerabilità, rappresentando una minaccia grave e diffusa.

Le librerie importate dal malware sono le seguenti:

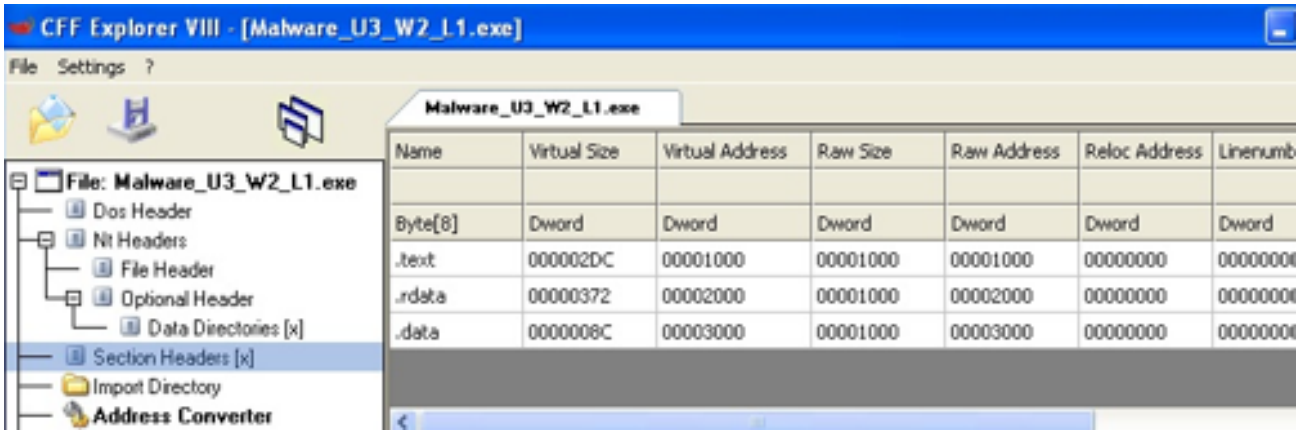
- **MSVCRT.dll**: Contiene funzioni per stringhe, allocazione memoria e I/O in stile C.
- **Wininet.dll**: Include funzioni per protocolli di rete come HTTP, FTP, NTP.
- **Kernel32.dll**: Funzioni chiave per operare su file e gestire la memoria.
- **Advapi32.dll**: Per interagire con i servizi e i registri del sistema operativo Microsoft.

Le sezioni del malware sono parti o segmenti che lo compongono e includono codice, dati e funzionalità specifiche.

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
UPX0	4096	16384	0	0	d41d8cd98f00b204e9800998ecf8427e	-1
UPX1	20480	4096	1536	7.07	ad0f236c2b34f1031486c8cc4803a908	5848.3
UPX2	24576	4096	512	2.8	f998d25f473e69cc89bf43af3102beea	53922

UPX (upx0, upx1, upx2) è una tecnica di compressione che riduce le dimensioni complessive di un file eseguibile. Questa compressione agisce sull'intero file mantenendo le funzionalità dell'applicazione. Ogni uno di questi livelli di compressione ha un impatto diverso sulle dimensioni del file e sulle prestazioni durante l'esecuzione del malware.



Le sezioni specifiche all'interno:

- **.text**: Questa sezione contiene le istruzioni eseguibili dalla CPU una volta avviato il software. È la sezione che la CPU esegue principalmente, mentre le altre sezioni contengono dati o informazioni di supporto.
- **.rdata**: Qui si trovano le informazioni sulle librerie e sulle funzioni importate o esportate dall'eseguibile. Queste informazioni possono essere esplorate tramite strumenti come CFF Explorer.
- **.data**: Questa sezione contiene dati e variabili globali accessibili da qualsiasi parte del programma eseguibile. Le variabili globali sono accessibili da qualsiasi funzione all'interno dell'eseguibile e non sono definite all'interno di una funzione specifica.