

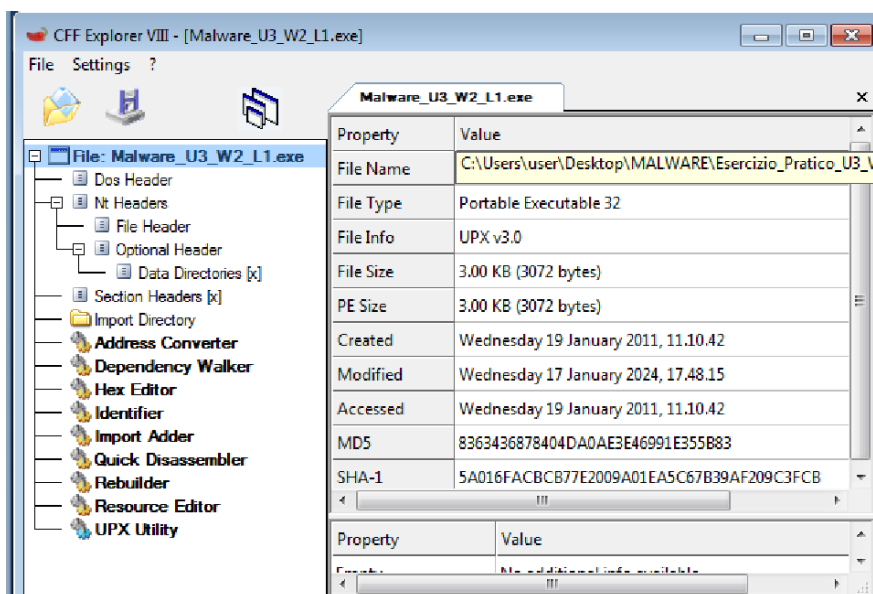
PRATICA S10-L1

SCOPO: In questa Pratica dobbiamo:

- Indicare le librerie importate dal malware,fornendo una descrizione per ognuna di esse.
- Indicare le sezioni di cui si compone il malware,fornendo un descrizione per ognuna di essa.
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte.

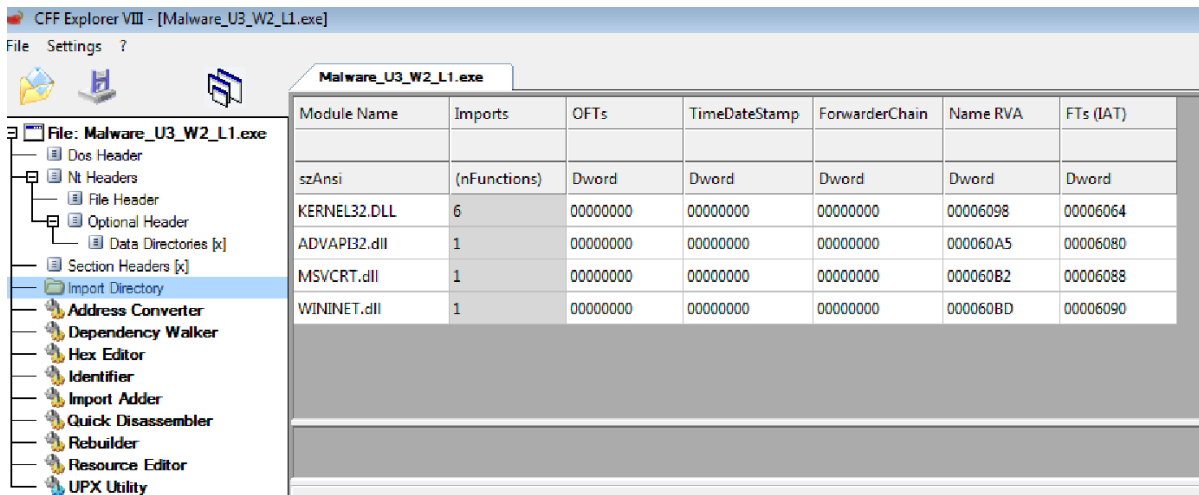
1-)Indicazione delle Librerie importate con un descrizione per ognuno di essa.

Per vedere le Librerie importate abbiamo utilizzato il tool **CFF EXPLORER**, che è un'applicazione software utilizzata principalmente per l'analisi dei file eseguibili e dei file binari su piattaforma Windows.dopo aver eseguito i vari passaggi abbiamo ottenuto la cattura seguente:



Poi cliccando su “import Directory”, abbiamo ottenuto l'elenco delle librerie importate qua sotto:

PRATICA S10-L1



-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 e i registri del sistema operativo.

-MSVCRT.dll : contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output.

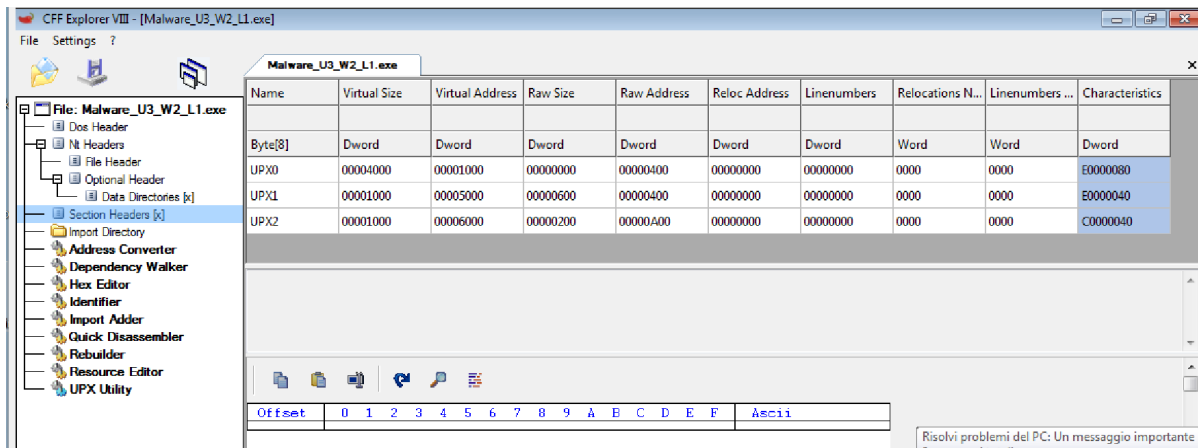
-WININET.dll : contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP.

2-)-Indicazione delle sezioni di cui si compone il malware,con descrizione per ognuna di essa.

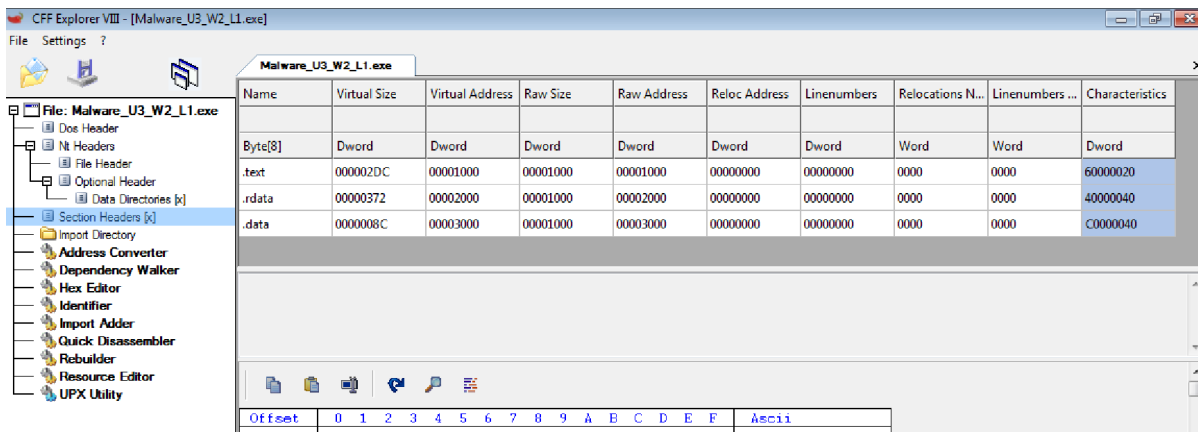
Per ottenere le sezioni di cui si compone il malware,abbiamo selezionato “section headers” e abbiamo ottenuto gli upx.che sono strumenti per la compressione e la decompressione per i file eseguibili.

Abbiamo ottenuto un esempio che possiamo vedere sulla cattura qua sotto:

PRATICA S10-L1



Dopo questo clicando su “UPX Utility” e tornando su section headers abbiamo ottenuto il risultato seguente:



Dove `.text` ; `.rdata` ; `.data` sono le tre sezioni di cui è composto il nostro eseguibile.

.txt :contiene le istruzioni che la CPU eseguirà una volta che il software sarà avviato.

.rdata include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile.

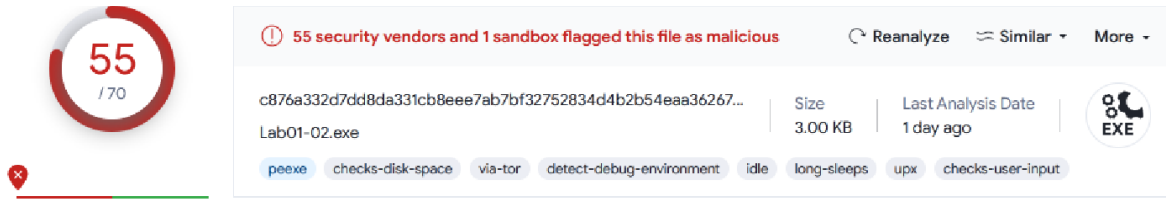
.data :contiene tipicamente i dati/le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

3-Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte.

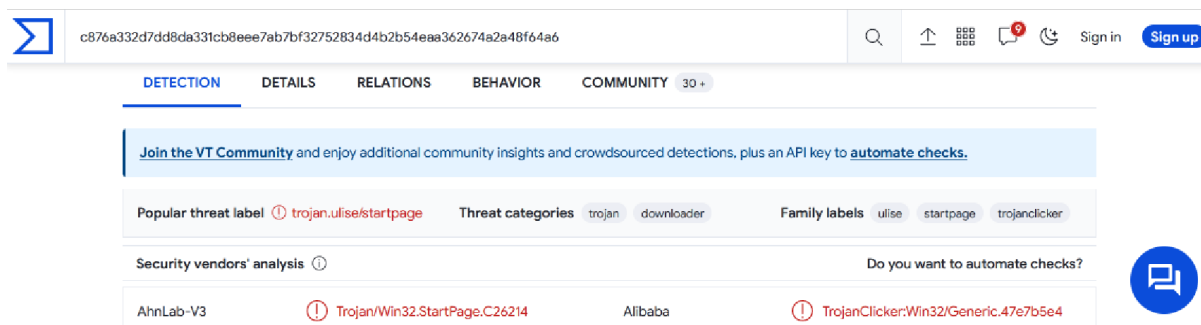
PRATICA S10-L1

Per fare questo abbiamo usato "VirusTotal" che è un servizio online gratuito che fornisce una piattaforma per analizzare file e URL sospetti o potenzialmente dannosi utilizzando vari motori di scansione antivirus e anti-malware.

Abbiamo aperto il servizio VirusTotal e abbiamo caricato il nostro file, Dopo la scansione abbiamo ottenuti i risultati seguenti:

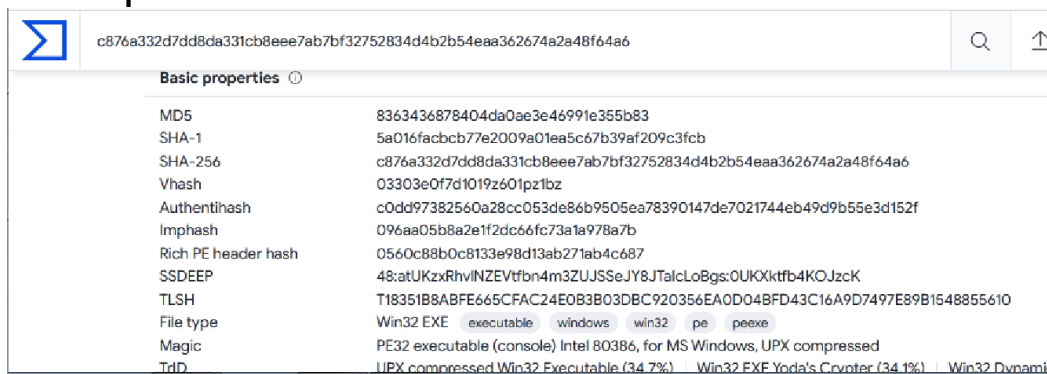


Qua ci dà i numeri di venditore di anti-malware che hanno segnalato il file che abbiamo inserito su questo servizio come malware.




Qua Virus Total ci fa capire che il nostro malware è un Trojan ovvero , un tipo di malware progettato per sembrare legittimo o innocuo, ma che in realtà contiene un codice dannoso che può causare danni al sistema dell'utente o comprometterne la sicurezza.

Se clicchiamo su Details otteniamo più informazioni sul nostro malware come possiamo vedere sulle catture sotto.



PRATICA S10-L1



c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Creation Time	2011-01-19 16:10:41 UTC
First Seen In The Wild	2010-11-20 23:29:33 UTC
First Submission	2011-07-02 17:02:09 UTC
Last Submission	2024-02-12 16:49:03 UTC
Last Analysis	2024-02-11 14:45:29 UTC

Names

Lab01-02.exe

Malware_U3_W2_L1.exe

Practical Malware Analysis Lab 01-02.exe_

Lab01-02.exe infected