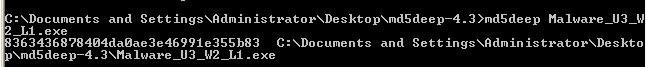
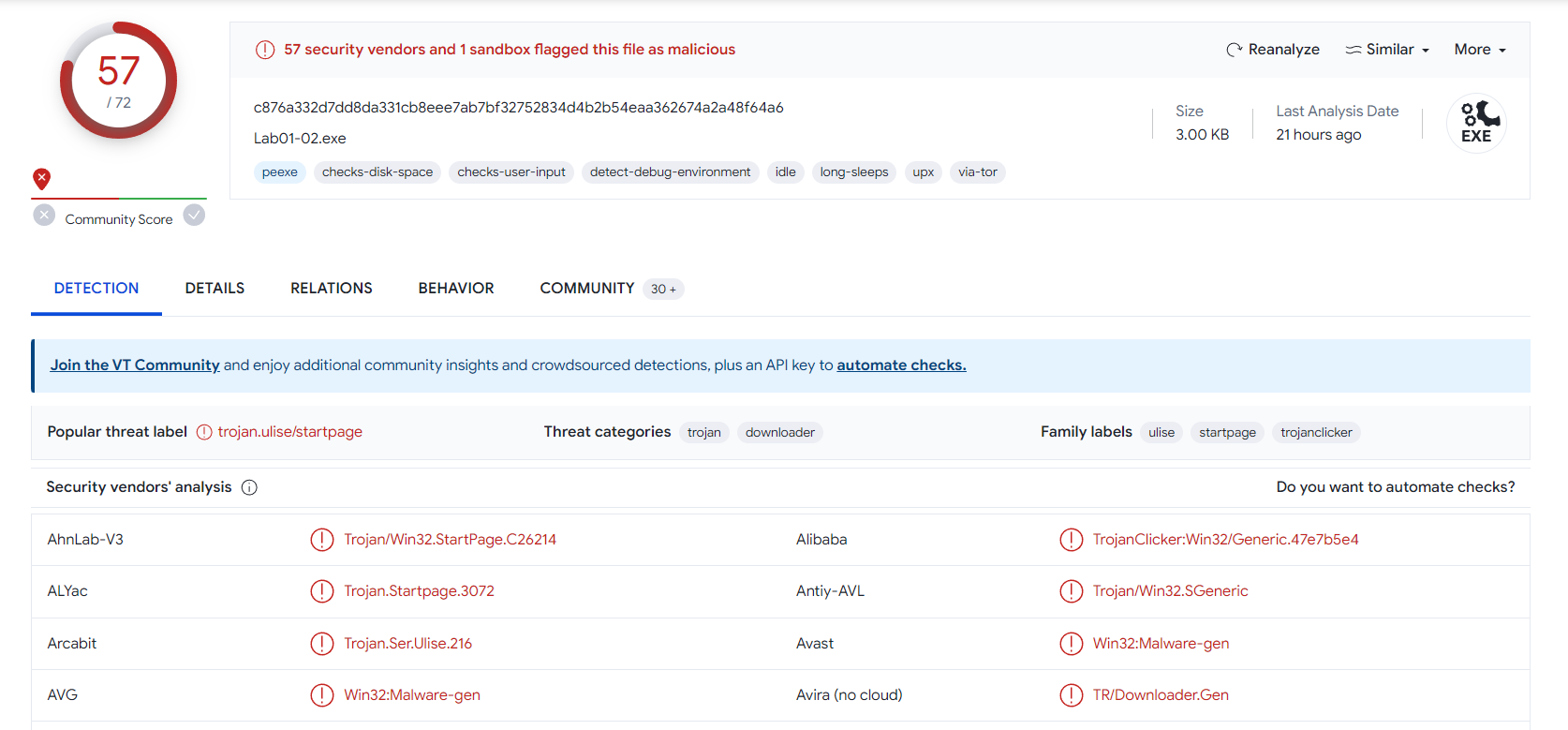
**ANALISI STATICA BASICA**

**Traccia**  
1) Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse.  
2) Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa.  
3) Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte.  
  
**Teoria**Section Headers: è una parte di un file eseguibile che fornisce informazioni su ciascuna sezione all'interno del file. Queste sezioni corrispondono alle diverse parti funzionali del programma, come il codice eseguibile, i dati o le risorse.  
Le intestazioni di sezione sono tipiche nei file di formato Portable Executable (PE), che sono utilizzati dal sistema operativo Windows per rappresentare eseguibili, DLL e altri tipi di file.  
Le informazioni contenute in una sezione header includono:  
Name: Un identificatore per la sezione.  
Virtual Size: La dimensione della sezione in Ram. Indica lo spazio necessario per caricare la sezione in Ram.  
Virtual Address: L'indirizzo virtuale a cui la sezione dovrebbe essere caricata in memoria durante l'esecuzione del programma.  
Raw Size: La dimensione della sezione nel file eseguibile sull’HDD.  
Raw Address: L'indirizzo fisico a cui la sezione dovrebbe essere caricata in memoria fisica. Potrebbe essere 0 se non è richiesta un'allocazione fisica specifica.

Import Directory: è una parte di un file eseguibile che contiene informazioni su funzioni o librerie esterne che il programma utilizza. Questo concetto è particolarmente rilevante nei file di formato Portable Executable (PE) utilizzati dal sistema operativo Windows per rappresentare eseguibili, DLL (Dynamic Link Libraries) e altri tipi di file eseguibili.  
In un file PE, l'import directory è un'area che elenca le librerie dinamiche che il programma deve caricare durante l'esecuzione. Queste librerie, chiamate DLL, contengono funzioni che il programma utilizzerà durante la sua esecuzione. L'import directory contiene le seguenti informazioni:  
Nome della libreria: Il nome della DLL da caricare.  
Tabella degli import: Una tabella che elenca le funzioni specifiche dalla DLL che il programma utilizzerà. Per ciascuna funzione, vengono forniti dettagli come il nome della funzione e l'indirizzo nella memoria virtuale della DLL dove può essere trovata.  
  
  
  
La funzione può essere chiamata in modo:  
Statico: l’exe copia tutte il contenuto delle librerie all’interno del proprio codice.  
Runtime: l’exe richiama la libreria solo quando ne necessita. È il comportamento solito dei malware.  
Dinamico: l’exe richiama la libreria per tutto il tempo in cui è attivo.  
  
**Pratica**  
1) Tramite MD5Deep ci procuriamo l’hash dell’eseguibile.

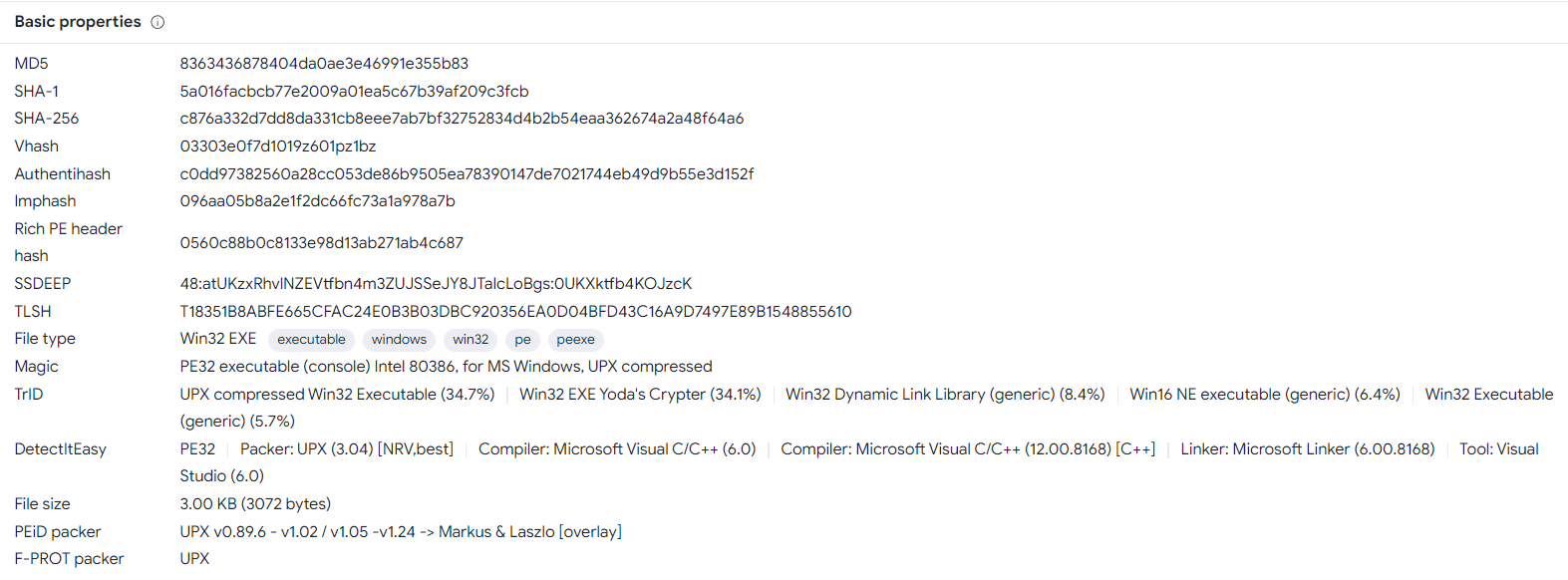


(md5deep “C:\...\PercorsoMalware\...\NomeFile.exe”)  
  
Andiamo ad inserire questo hash su VirusTotal per controllare se si tratta di un malware conosciuto ed eventualmente vedere la sua valutazione.

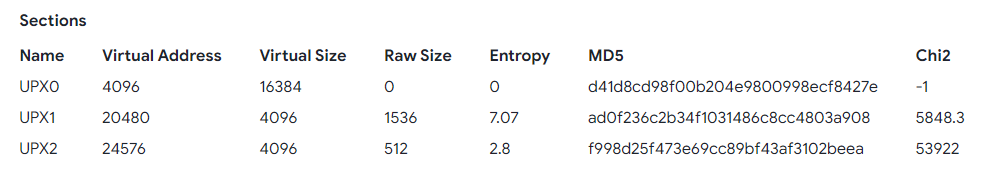




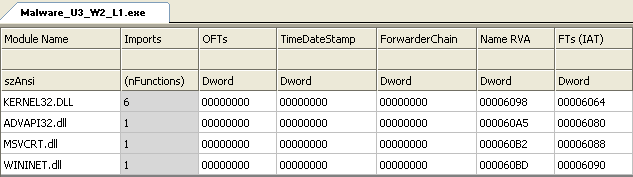
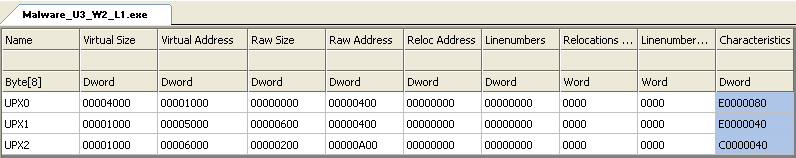
Questo Malware è un Trojan/Downloader.

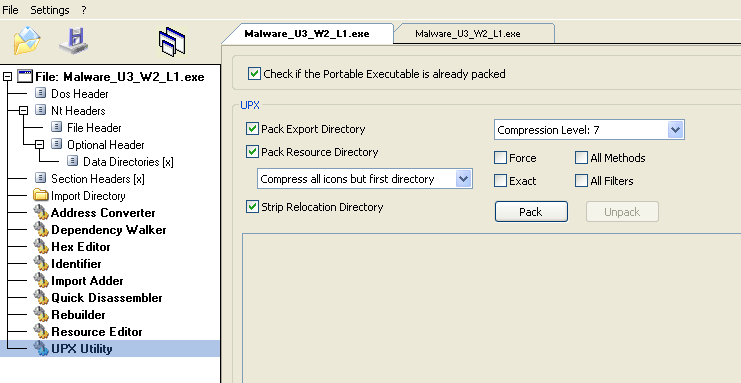
Successivamente, andiamo nella tab “DETAILS” per controllare diverse informazioni quali:  
  
a) Le sue proprietà, diversi sistemi di hashing, la dimensione del file, il tipo, ecc.

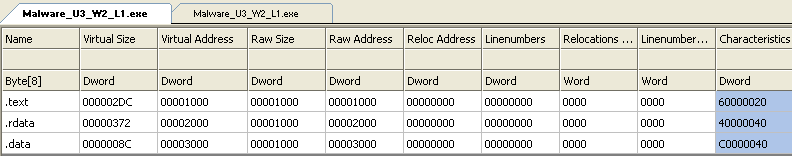
  
b) La “cronologia” del file su VirusTotal

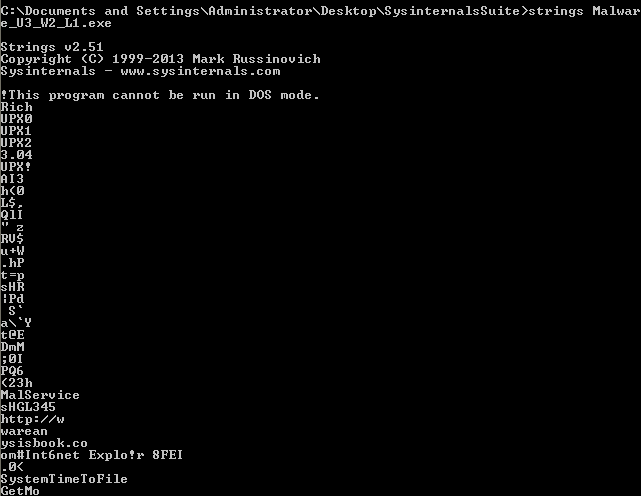
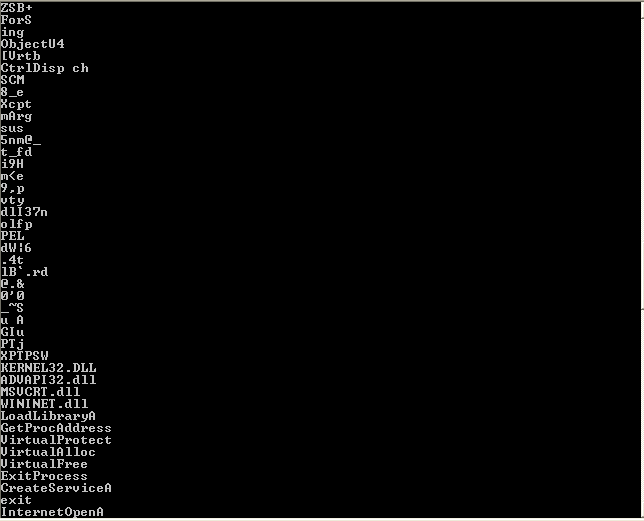
c) Le Sections:  
  
  
  
  
  
  
  
  
In questo caso UPX è un packer open source. Fondamentalmente, quando il file compresso con UPX viene eseguito, tutte le sezioni compresse vengono decompresse in memoria, incluso qualsiasi codice dannoso che un attaccante potrebbe aver memorizzato al suo interno.  
Essendo UPX, bisogna decomprimerle per leggere in chiaro il contenuto.

d) Gli Imports con le relative funzioni:  
  
- Advapi32.dll: contiene le funzioni per interagire con i servizi ed  
i registri del sistema operativo.  
- Kernel32.dll: contiene le funzioni principali per interagire con  
il sistema operativo, ad esempio: manipolazione dei file,   
la gestione della memoria.  
- 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 (Network Time Prot).

2) Possiamo confermare il tutto aprendo il file su CFF Explorer.  
  
Troviamo le Sections e gli Import.

Ogni Import (libreria) avrà poi le sue funzioni.  
  
  
  
  
Da qui ci spostiamo nell’ultima tab “UPX Utility” e clicchiamo su “Unpack”.  


Vedremo in chiaro il contenuto degli UPX.  
Le istruzioniche troviamo sono:  
- .text: le istruzioni che eseguirà la CPU una volta avviato il malware.  
- .rdata: le informazioni sulle librerie importate ed esportate.  
- .data: le variabili globali (cioè accessibili da qualsiasi funzione).

3) SysinternalSuite  




(strings “C:\...\PercorsoMalware\...\NomeFile.exe”)

Ci mostra tutte le stringhe all’interno del file, tra cui le sezioni, un URL scritto in modo scomposto, le librerie e le funzioni.