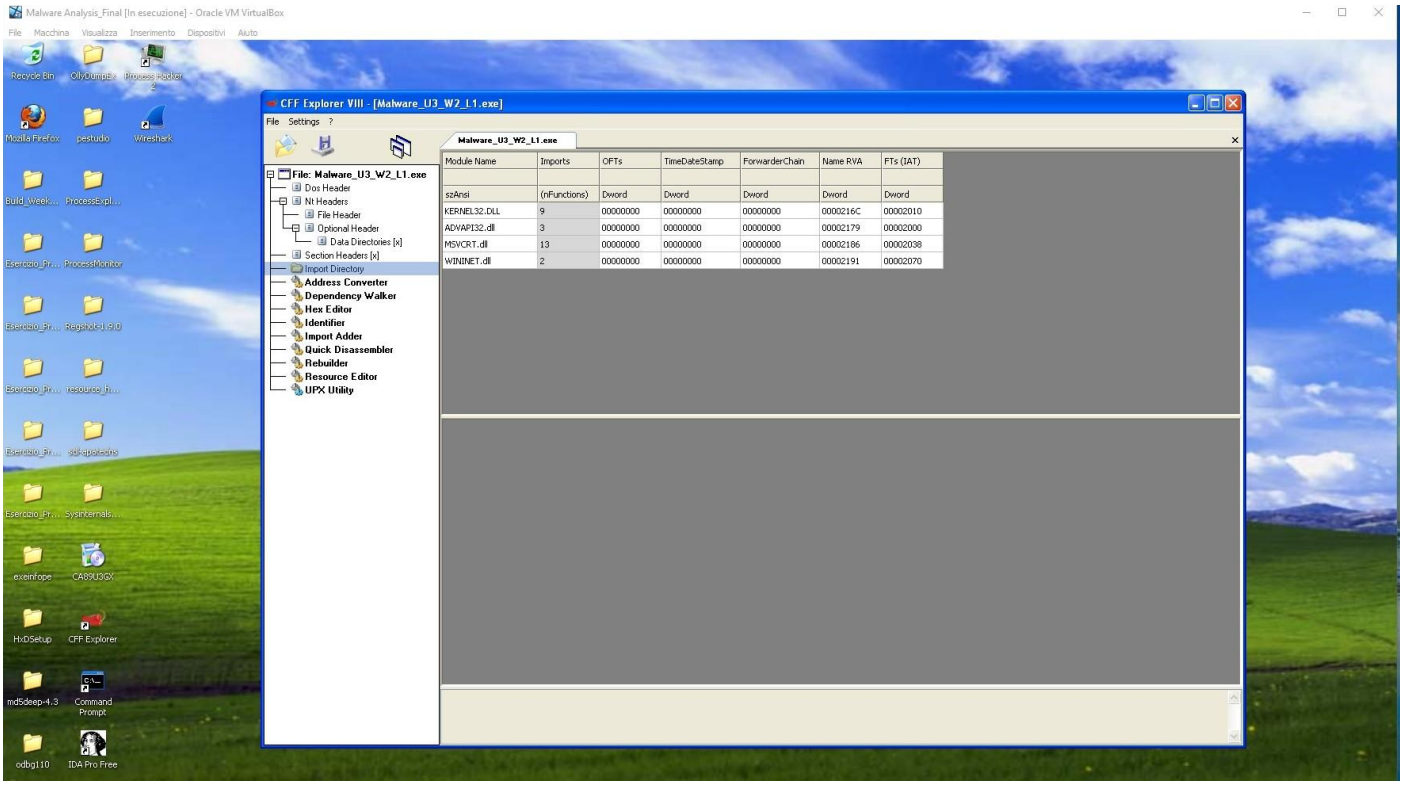
S10/L1 Esercizio 27/11/2023

Nell'esercizio odierno ci viene richiesto di analizzare il contenuto del file Esercizio Pratico U3 W2 L1:

- Indicare le librerie importate e fornirne la descrizione
- Indicare le sezioni di cui si compone il malware e fornirne la descrizione
- Aggiungere una descrizione sul malware in base alle informazioni raccolte

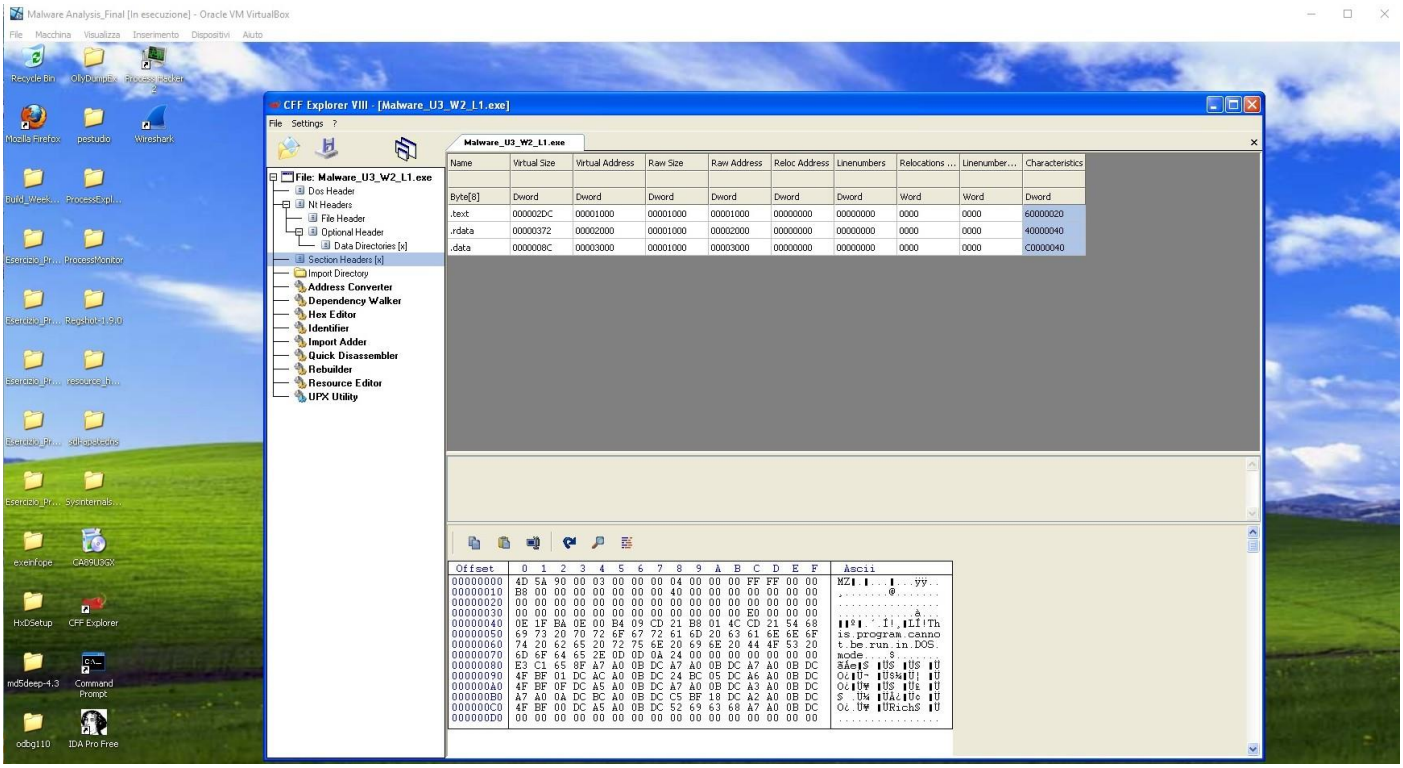
Le **librerie** importate sono le seguenti:

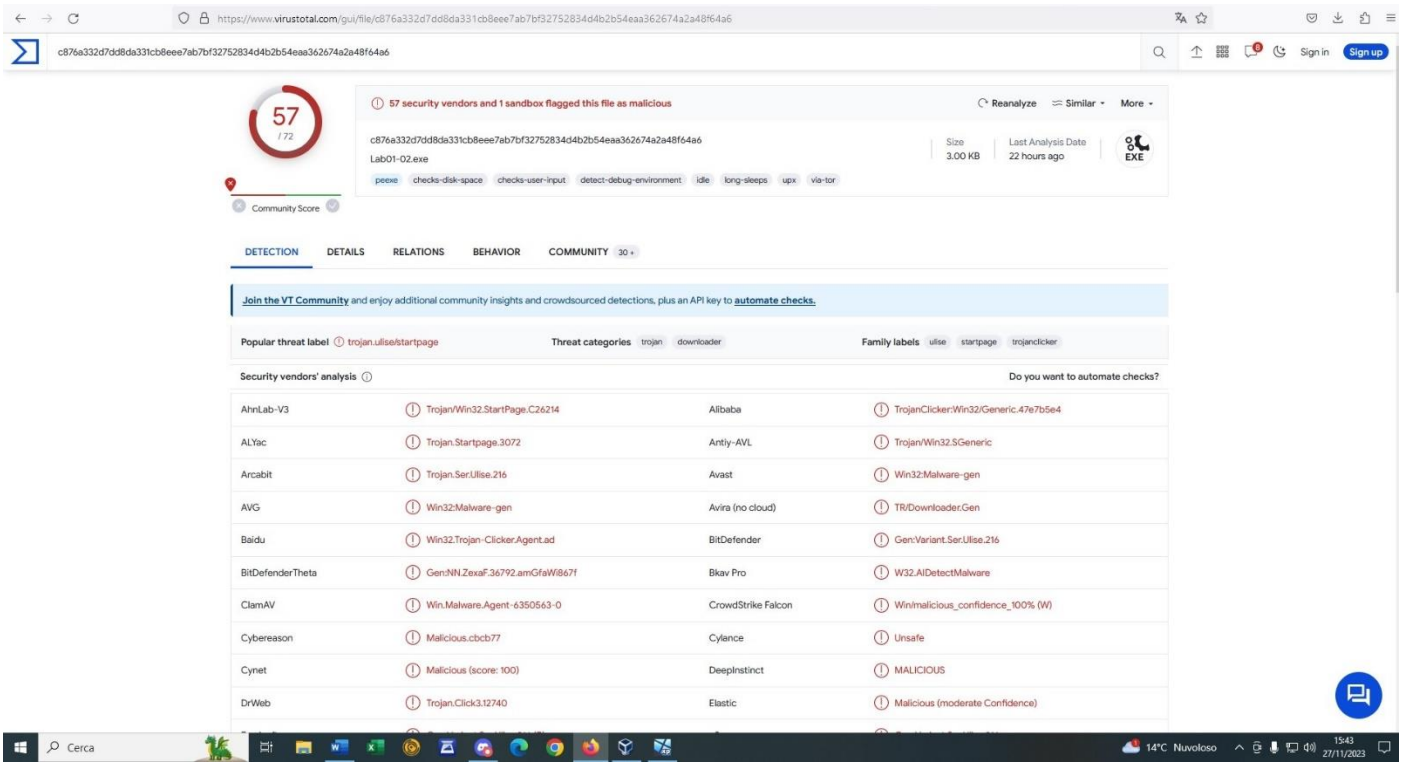
- **KERNEL 32.dll**
  È una libreria presente nei sistemi operativi Windows, fa parte del kernel (il nucleo del sistema operativo) di Windows. Questa libreria fornisce molte funzioni di base essenziali per il funzionamento del sistema operativo e delle applicazioni, ad esempio manipolazione dei file e gestione della memoria
- **ADVAPI 32.dll**
  Anche questa è una libreria presente nei sistemi operativi Windows e fornisce funzioni relative alla sicurezza, alla gestione dei servizi e ad altre operazioni di sistema. Contiene le funzioni per interagire con i servizi ed i registri del sistema operativo
- **MSVCRT.dll**
  E' una libreria fornita da Microsoft per Windows fornisce implementazioni di funzioni standard del linguaggio C e supporta operazioni di input/output, gestione della memoria e altre funzionalità di base del linguaggio e viene spesso utilizzata quando si sviluppano programmi in C o C++ ad esempio contiene funzioni per la manipolazione stringhe e allocazione memoria
- **WININET.dll**
  E' una libreria che fornisce funzionalità di networking per le applicazioni di Windows. Viene spesso utilizzata per effettuare operazioni di rete come l'accesso a risorse su internet, download e upload di file e la gestione delle connessioni HTTP, FTP e NTP

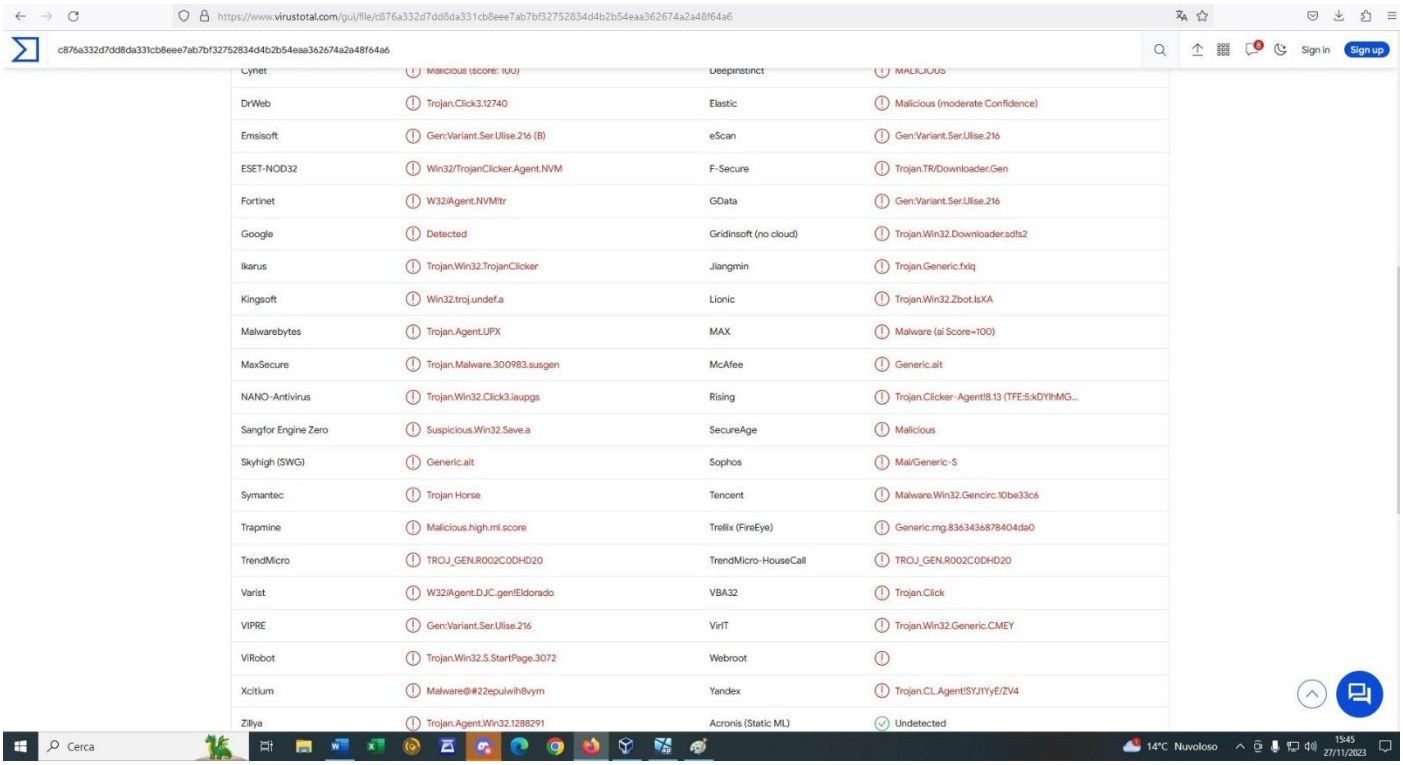


Le **sezioni** di cui si compone il malware da principio ci vengono proposte come UPX0 – UPX1 -UPX2, quindi andiamo su UPX Utility e “spacchettiamo” con il tasto unpack e a quel punto abbiamo le sezioni in chiaro e sono:

- **.text**
  contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l’unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto
- **.rdata**
  include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall’eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer.
- **.data**
  contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.







Abbiamo ricavato il codice hash da MD5 e come possiamo rilevare dalla scansione effettuata con virus total si tratta sicuramente di un malware di tipo trojan, un tipo di software dannoso che si presenta come qualcosa di legittimo o affidabile, ma che in realtà contiene codice dannoso. Nello specifico troviamo il trojan downloader che ha lo scopo di scaricare e installare altri malware sul sistema.