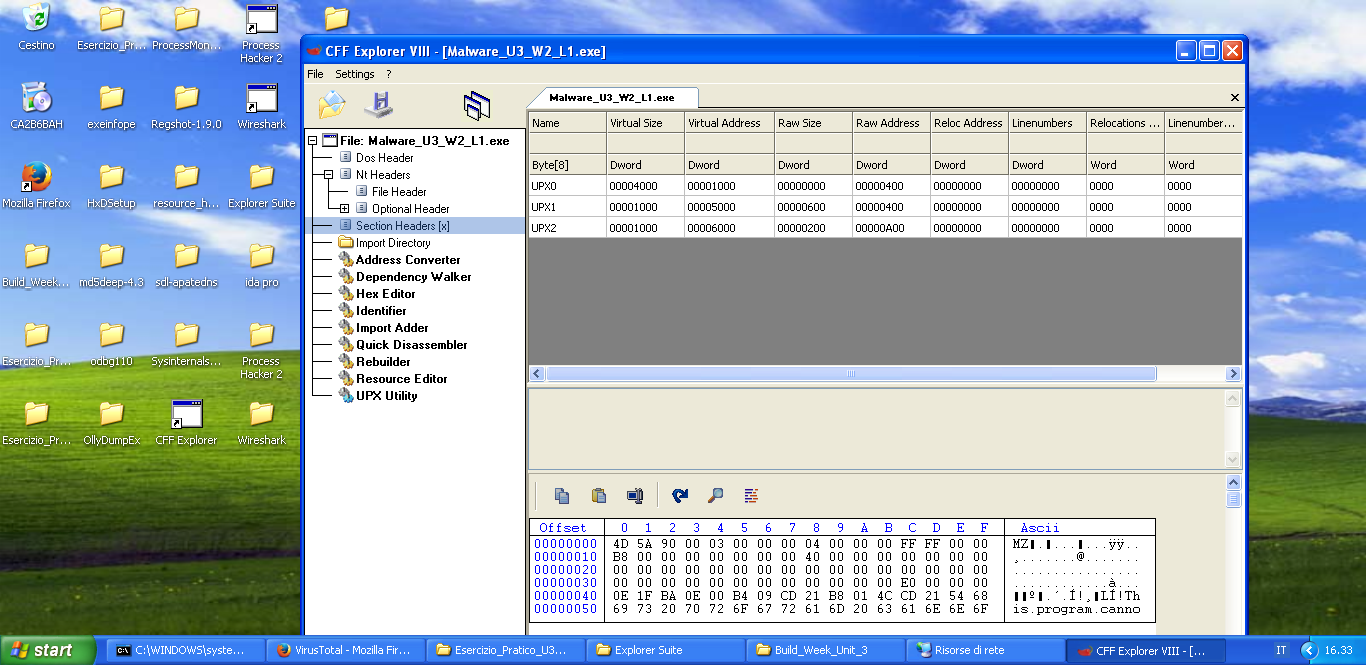
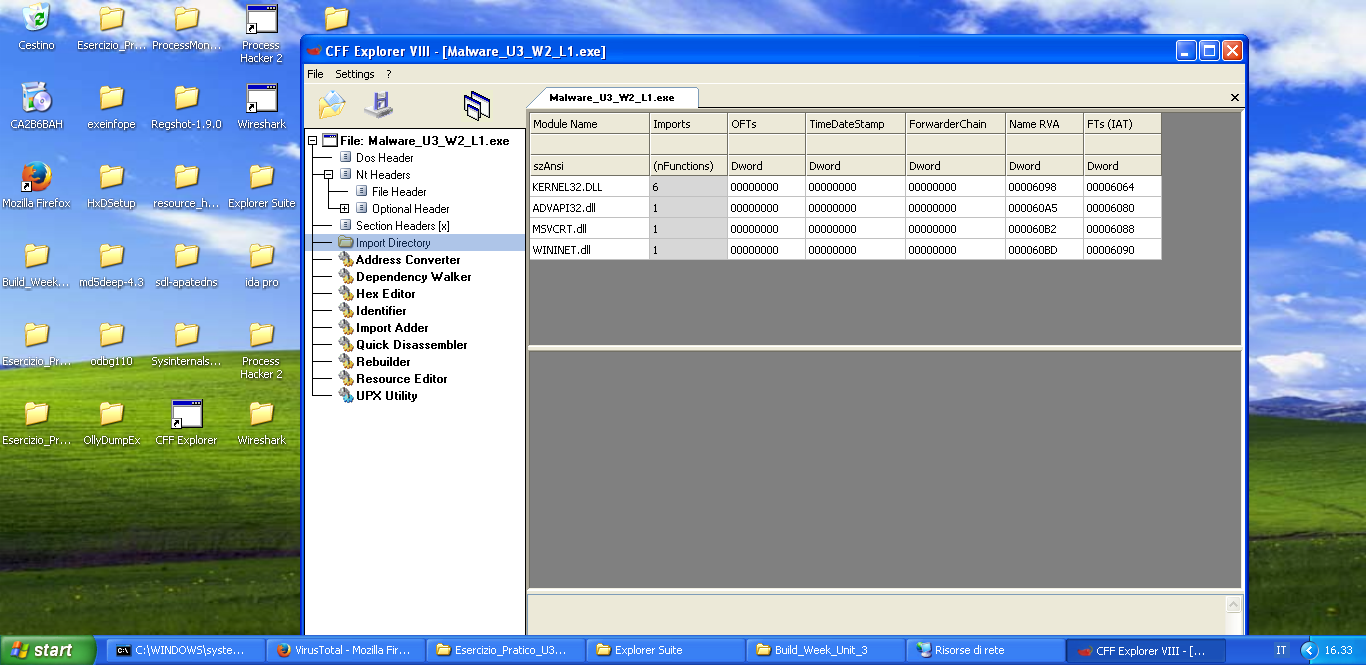
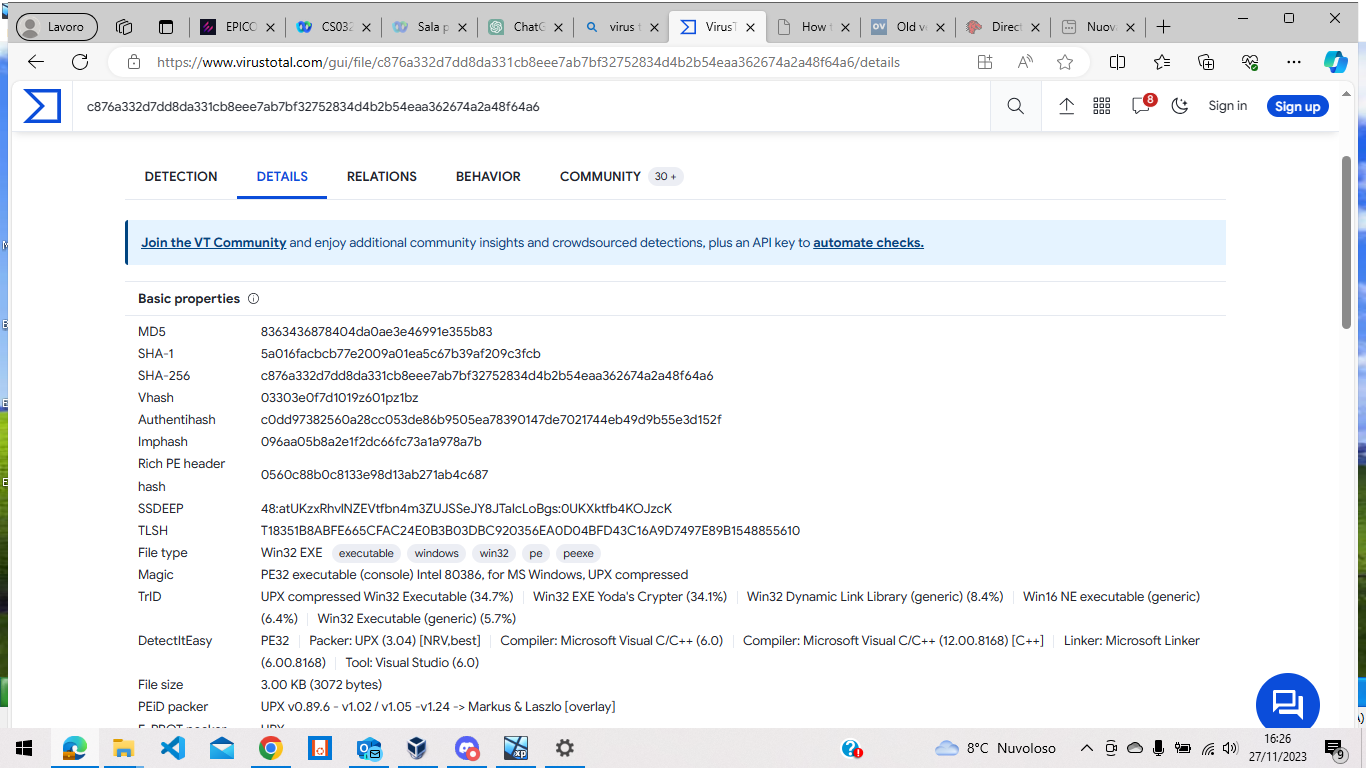
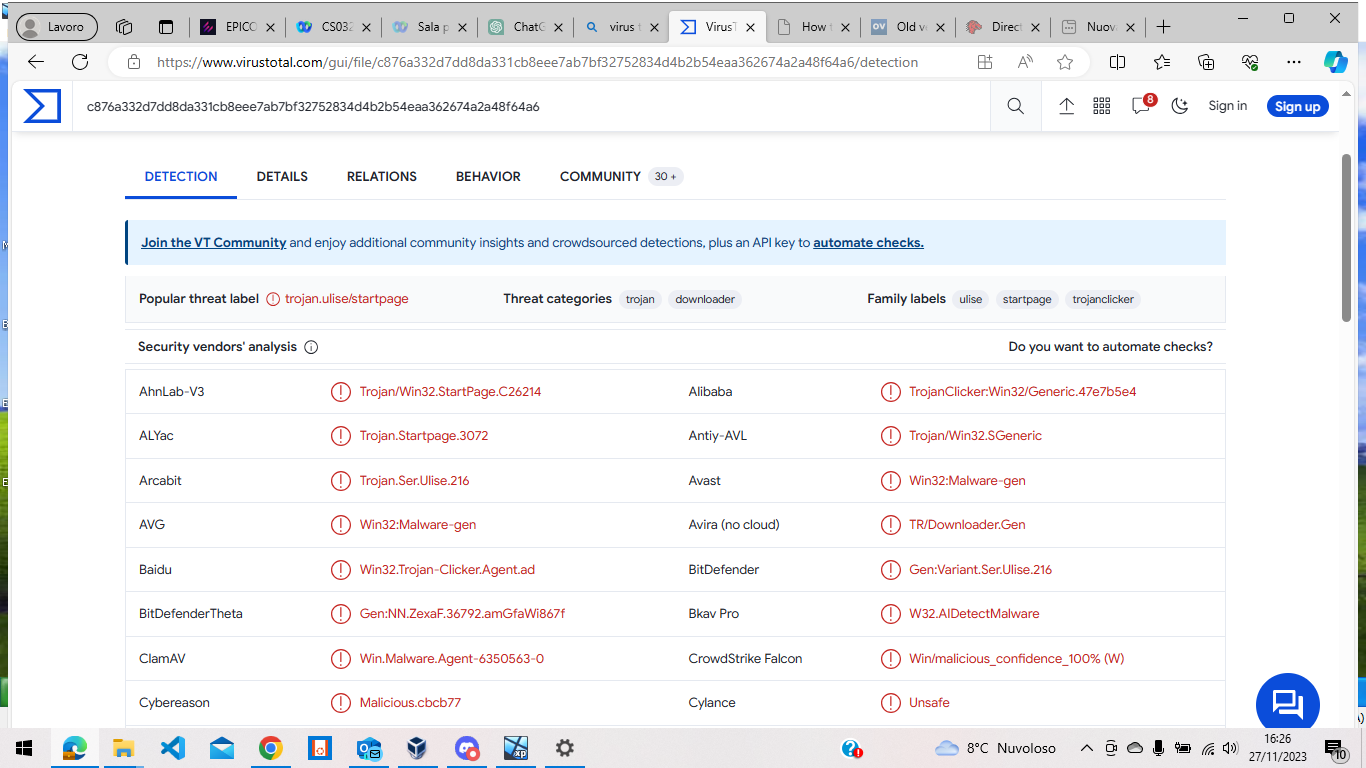
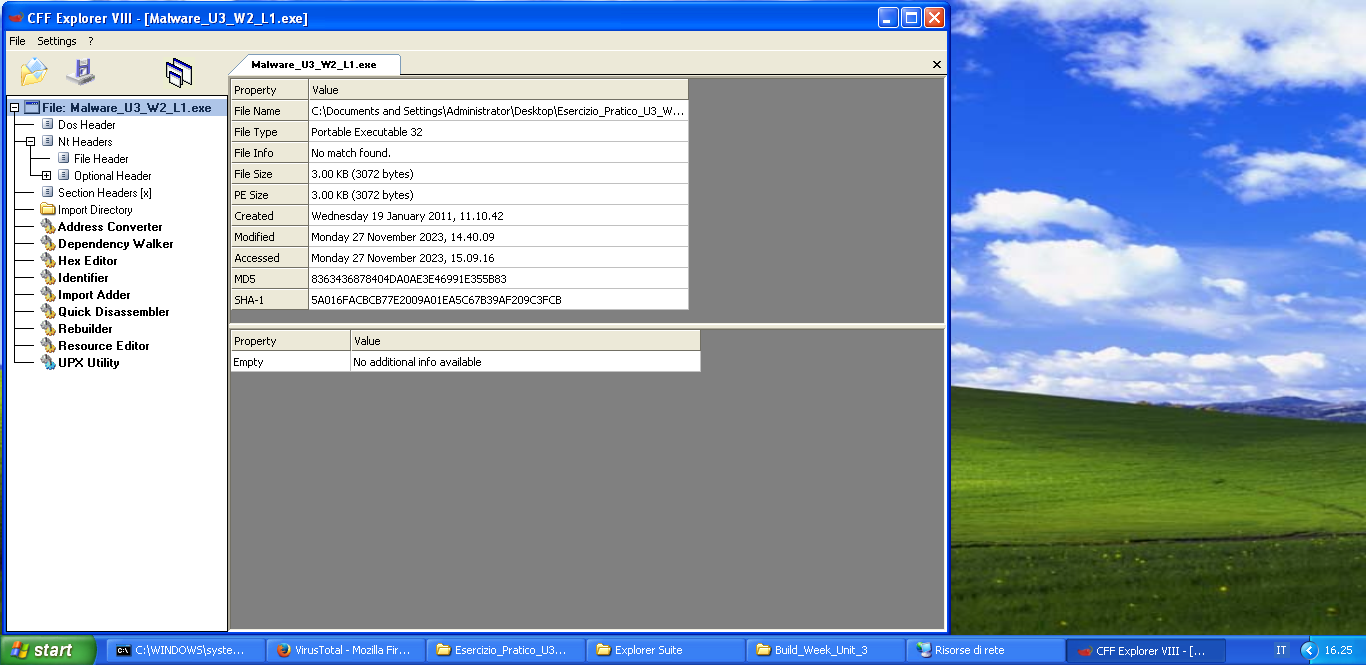
Analisi statica basica

Con riferimento al file eseguibile contenuto nella cartella «Esercizio\_Pratico\_U3\_W2\_L1» presente sul Desktop della vostra macchina virtuale dedicata all’analisi dei malware, rispondere ai seguenti quesiti:

• Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse

• Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa





Queste informazioni indicano che il file è un'applicazione Windows a 32 bit con un'estensione .exe. Le dimensioni virtuali e raw del file sono relativamente piccole, il che suggerisce che il malware è relativamente semplice. L'assenza di linee di codice indica che il malware è stato compresso.

L'immagine mostra anche che il malware è stato compilato utilizzando il compilatore UPX. UPX è un programma di compressione del codice che viene spesso utilizzato per nascondere il codice malware.

In base alle informazioni fornite dall'immagine, è possibile fare le seguenti considerazioni sull'analisi di questo malware:

L'analisi statica del malware sarà probabilmente difficile, poiché il codice è compresso.

L'analisi dinamica del malware sarà probabilmente più efficace, poiché il codice verrà decompilato durante l'esecuzione.

L'analisi del malware dovrebbe concentrarsi sulle seguenti aree:

Le funzioni di ingresso e uscita del malware

Le funzioni di comunicazione del malware

Le funzioni di evasione del malware