Esercizio S10L1
Analisi statica basica

Samuele Conti

Task

L’esercizio ci chiede di recuperare info su un Malware tramite l’analisi statica

Side Tasks

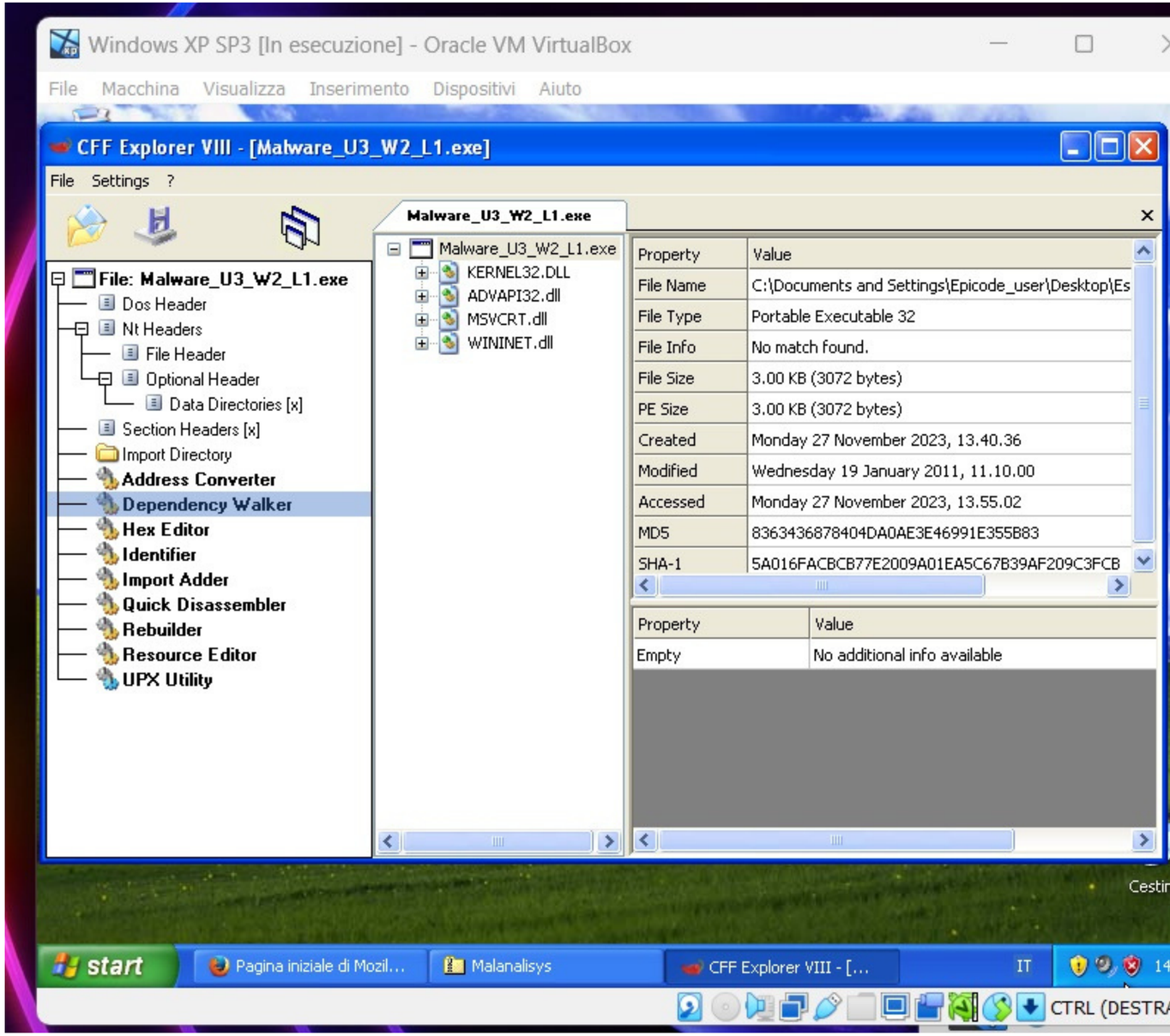
- Indicare le librerie importate dal malware
- Indicare le sezioni di cui si compone il malware
- Aggiungere una considerazione finale

Analisi statica basica

Lo scopo dell’analisi statica basica è se un dato file è malevolo e fornire informazioni riguardo le sue funzionalità

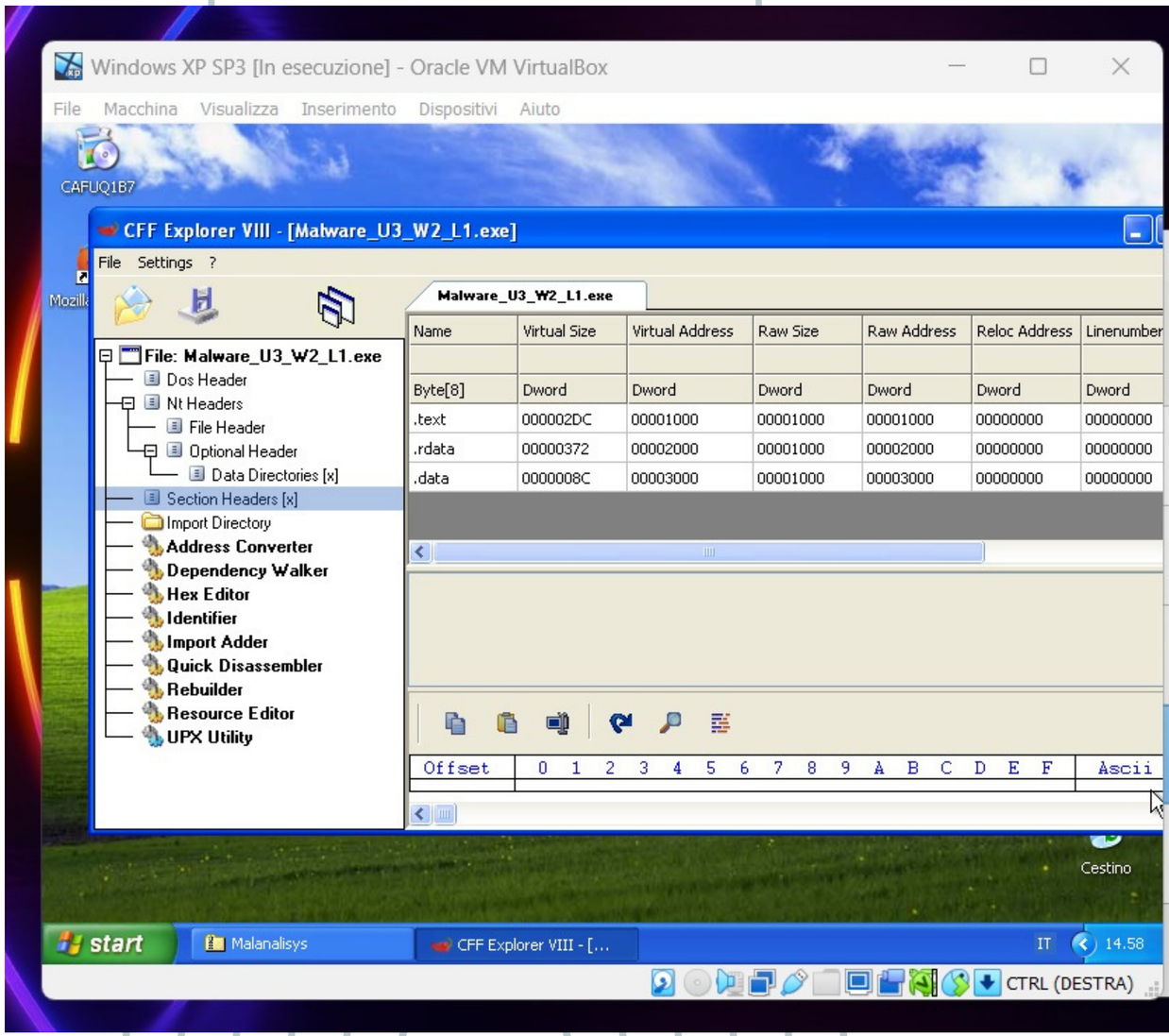
Caricando il malware datoci dall'esercizio tramite CFF Explorer, vediamo che il malware ha importato le seguenti librerie:

- Kernel32.dll (contiene funzioni principali per interagire con S.O.)
- Advapi32.dll (contiene funzioni principali per interagire con S.O Microsoft)
- MSVCRT.dll (funzioni che manipolano stringhe, allocazione memorie e servizi in/out in stile C)
- Wininet.dll (funzioni che implementano protocolli di rete)



Abbiamo spacchetato il file ed abbiamo potuto vedere le varie sezioni di cui si compone il malware:

- .text (contengono istruzioni che la CPU eseguirà una volta che il malware sarà avviato)
- .rdata (include info sulle librerie e le funzioni importate ed esportate dall'eseguibile)
- .data (contiene dati/ variabili globali del malware, che devono essere disponibili da qualsiasi parte del programma)



Come verifica finale ho controllato il codice hash sul sito VirusTotal il il quale mi ha fornito che probabilmente l’entità di questo malware è un Trojan