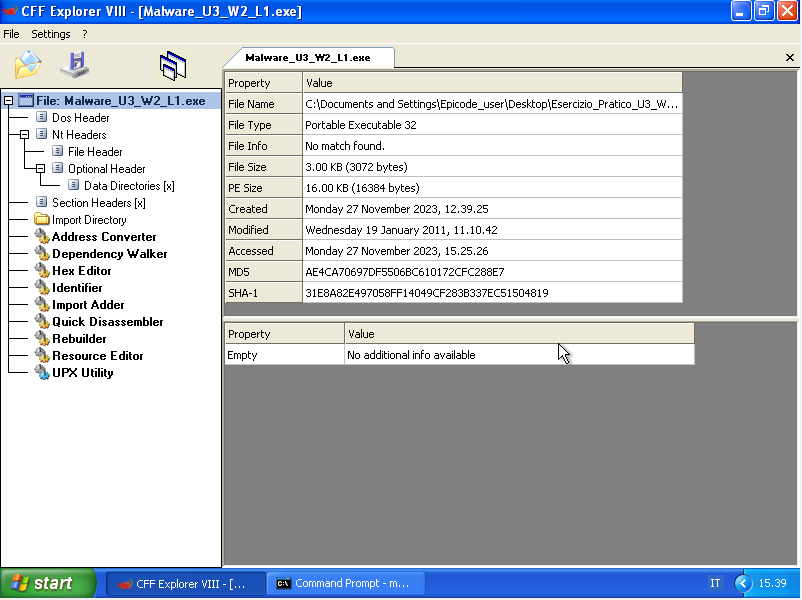
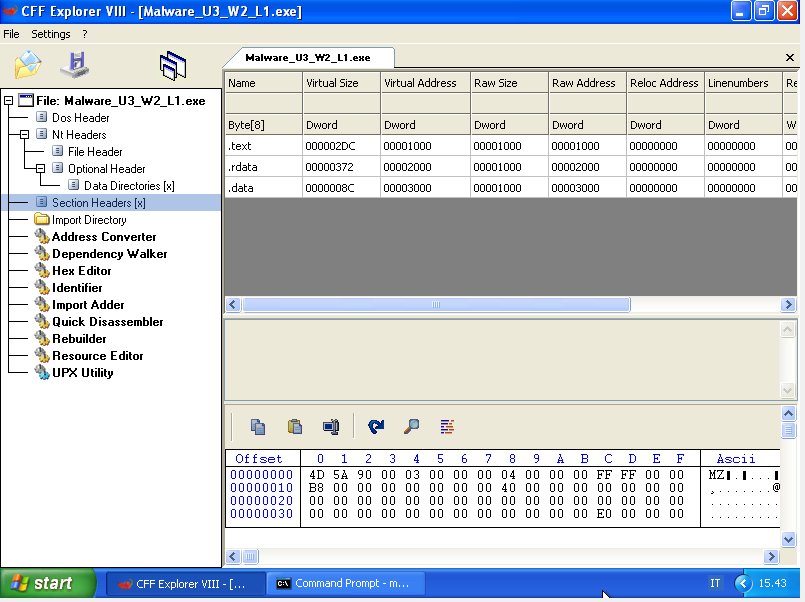
Esercizio S10 L1

Oggi andremo ad effettuare l’analisi di un malware su una macchina virtuale Windows XP

Andiamo quindi a vedere nel dettaglio com’è composto questo eseguibile.

Come prima cosa, controlleremo la sezione “Section Headers” per capire da quali sezioni è composto il file:

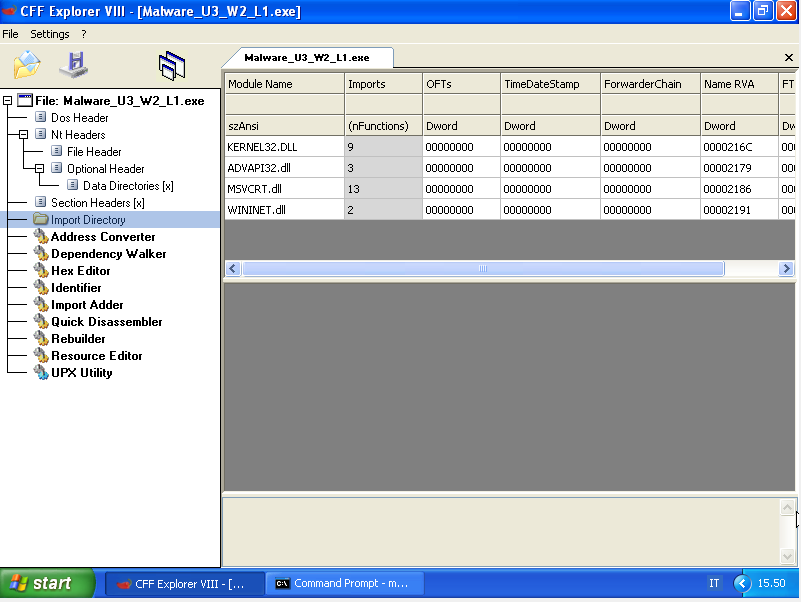
come si nota, sono presenti 3 sezioni e sono .text, .rdata e .data.

La sezione .txt contiene le righe del codice che la CPU andrà ad eseguire una volta che il programma sarà eseguito. Teoricamente, la sezione .txt è l’unica che viene eseguita dalla CPU, in quanto le altre sezioni contengono informazioni a supporto di questa;

La sezione .rdata, invece, contiene le informazioni riguardanti le librerie importate ed esportate dall’eseguibile;

La sezione .data contiene le variabili globali del programma, che vuol dire che tali variabili dovranno essere eseguibili da ogni parte del programma.

Successivamente, procederemo all’analisi della “import directory”.



Da questa schermata, possiamo notare che sono presenti 4 librerie diverse:

Kernel32: è una delle librerie più comuni e contiene le funzioni principali per l’interazione con il sistema operativo come quelle per la manipolazione dei file e la gestione della memoria;

Advapi32: è una libreria che contiene funzioni con i servizi ed i registri di Microsoft;

Msvcrt: contiene funzioni per la manipolazione delle stringhe e chiamate in input/output;

Winnet: libreria che contiene le funzioni per l’implementazione per alcuni protocolli di rete (http, HTTPS).

Andando poi su virustotal, possiamo notare che questo malware sembra essere un Trojan.