S10 L1

Report esercizio “Malware analysis”

GiuliaSalani

INDICE

TRACCIA

Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'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:

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;

REPORT

1. PREMESSA: MALWARE ANALYSIS

1.1 DEFINIZIONE DI ANALISI STATICA BASICA

L'analisi statica è una **tecnica di esame del software senza eseguirlo**. In ambito di malware analysis, coinvolge l'analisi del codice sorgente o binario senza attuare l'esecuzione del programma.

Durante questa analisi, **gli analisti esaminano la struttura del codice, rilevano pattern di comportamento sospetti e identificano potenziali indicatori di compromissione**.

L'obiettivo è ottenere una comprensione preliminare del malware senza esporsi a rischi operativi. L'analisi statica può rivelare informazioni sulle funzionalità, sulla presenza di tecniche di evasione, e sull'utilizzo di risorse del sistema.

1.2 CFF EXPLORER

CFF Explorer è un **software di analisi e modifica di file eseguibili su piattaforma Windows**.

Fornisce un'interfaccia grafica per esplorare la struttura interna dei file PE (Portable Executable), consentendo agli analisti di visualizzare informazioni dettagliate sulle sezioni, le risorse, e i riferimenti a funzioni.

È spesso utilizzato in ambito di reverse engineering e analisi malware per esaminare e comprendere la composizione di eseguibili Windows. CFF Explorer supporta anche funzionalità avanzate come la modifica di attributi e l'estrazione di risorse dai file PE.

1.3 EXEINFO PE

Exeinfo PE è un **tool leggero e intuitivo utilizzato per analizzare file eseguibili PE** (Portable Executable) **su piattaforma Windows**.

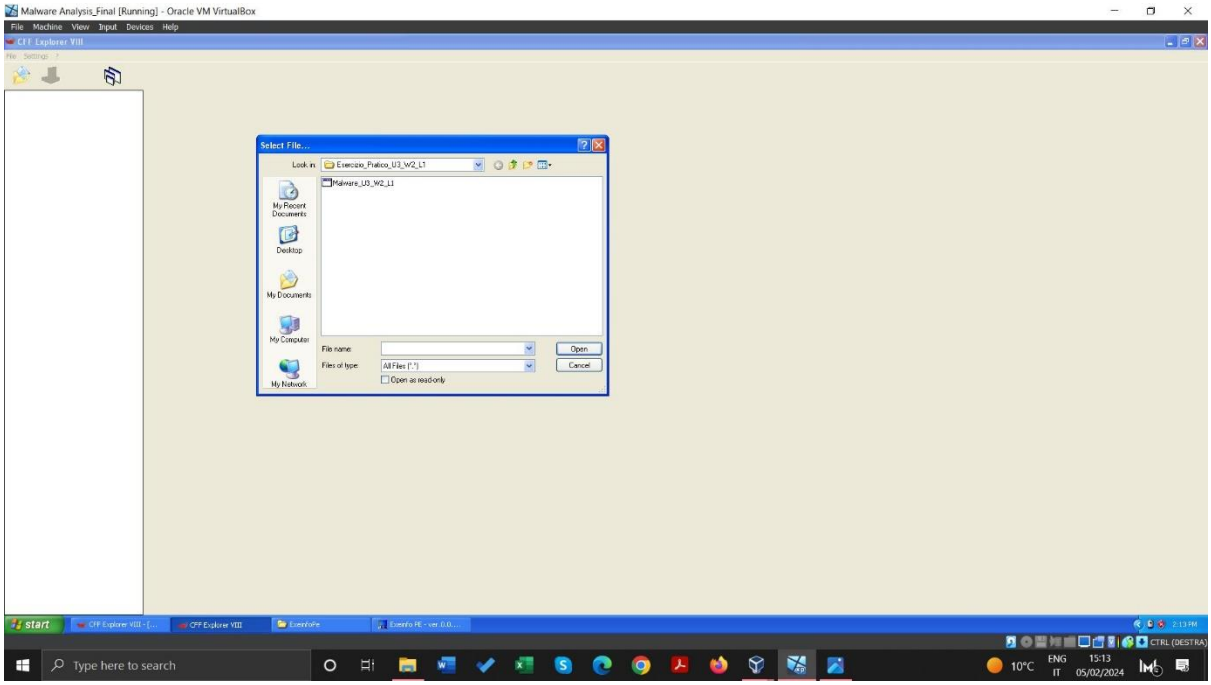
Questo strumento fornisce informazioni dettagliate sul tipo di file, l'architettura, le firme digitali, e altro ancora. È comunemente utilizzato nell'ambito di reverse engineering, analisi di malware e durante la fase di identificazione delle caratteristiche di un file eseguibile.

Exeinfo PE **offre una rapida panoramica della struttura interna del file**, aiutando gli utenti a comprendere la natura e le caratteristiche di un'**eseguibile senza doverlo eseguire** direttamente.

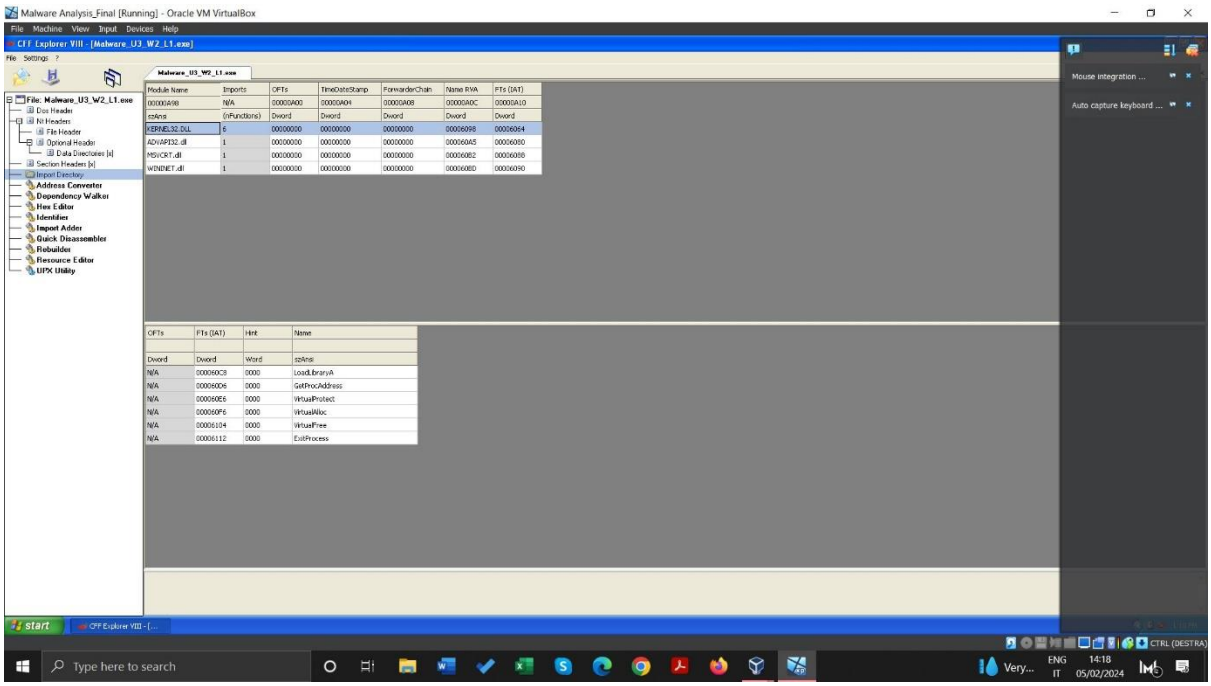
2. LIBRERIE

2.1 ISTRUZIONI PASSO A PASSO

Iniziamo aprendo CFF Explorer e cliccando sulla prima icona sulla sinistra, quella che rappresenta una cartella. Potremo a questo punto selezionare il file oggetto dell'esercizio di oggi:

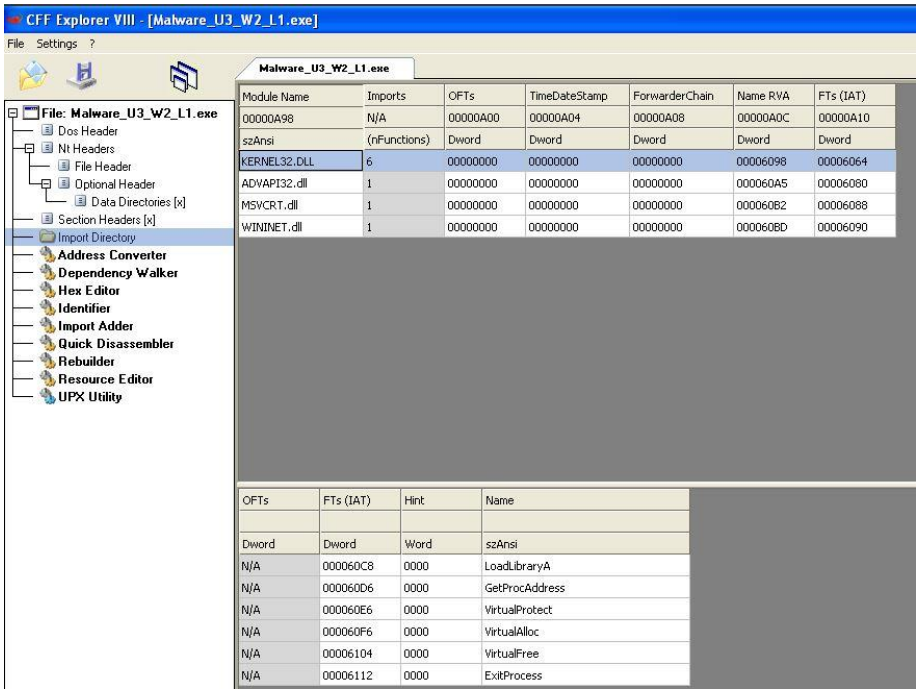


Una volta aperto il file, dall'elenco a sinistra selezioniamo Import Directory. A questo percorso potremo vedere tutte le librerie importate dal malware, che sono quattro. Nella sezione che segue le analizzeremo una ad una.



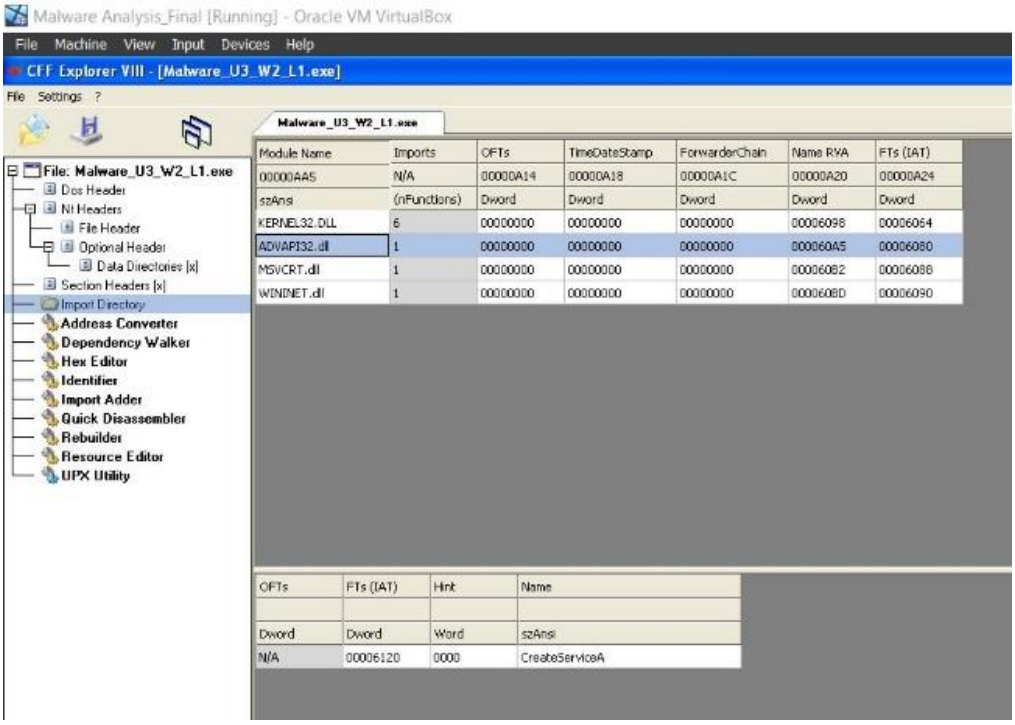
2.2 KERNEL32.DLL

La prima libreria caricata è "Kernel32.dll", una libreria piuttosto comune che contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.



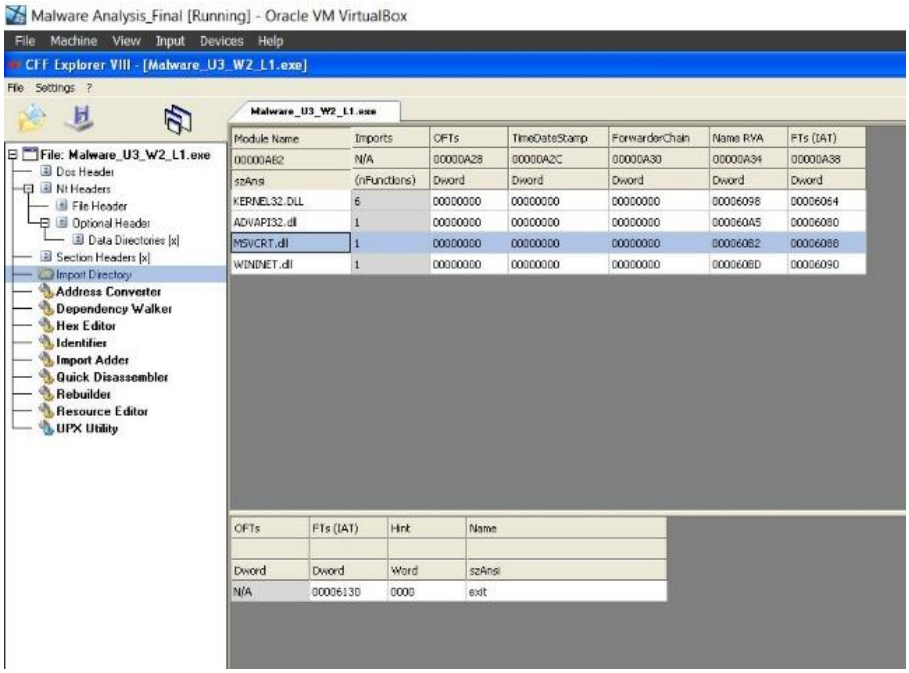
2.3 ADVAPI32.DLL

La seconda è "Advapi32.dll", libreria che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft:



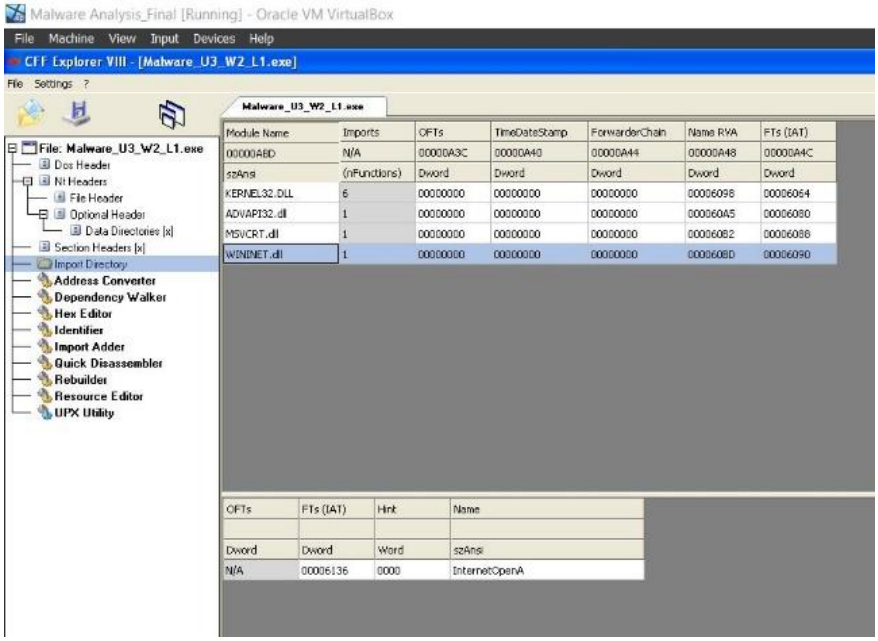
2.4 MSVCRT.DLL

La terza è "Msvcrt.dll", libreria che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro, come ad esempio chiamate per input/output in stile linguaggio C:



2.5 WININET.DLL

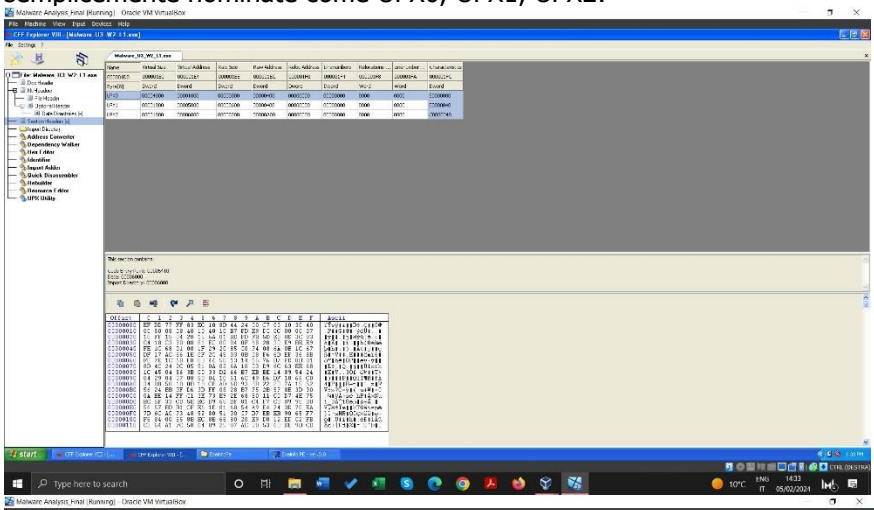
Infine Wininet.dll, libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP:

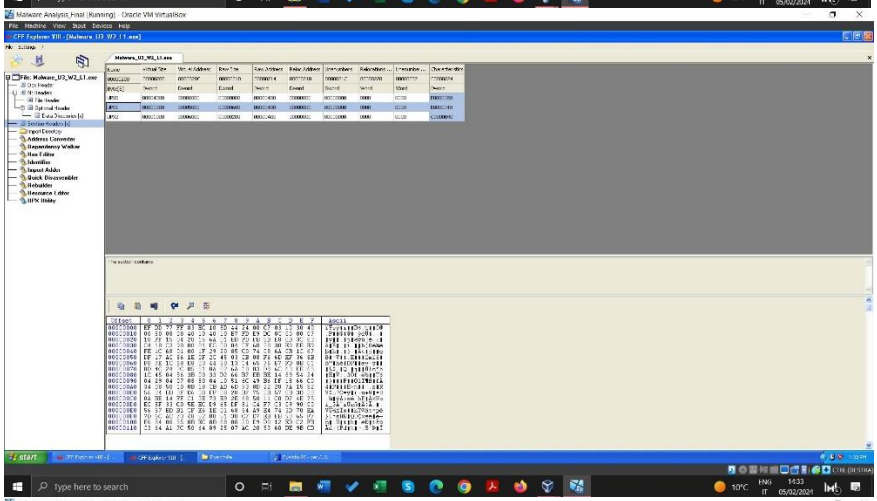


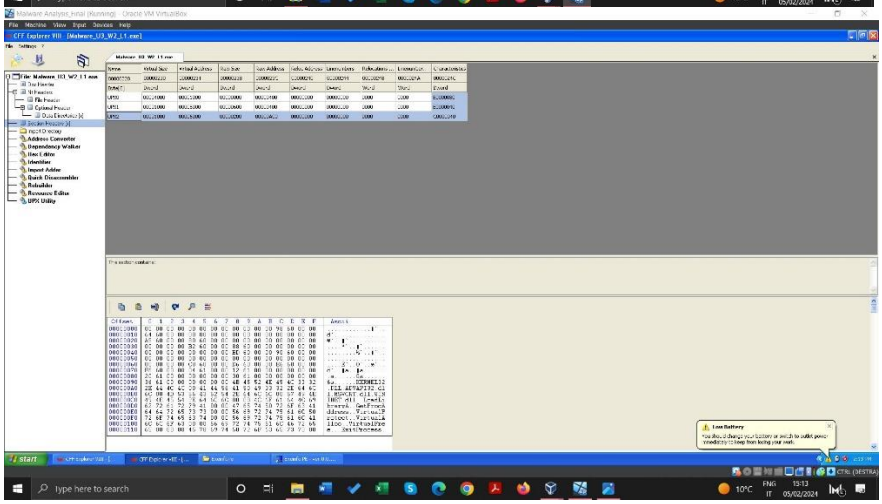
3. SEZIONI

3.1 ISTRUZIONI PASSO A PASSO

All'interno di CFF Explorer, è possibile studiare le varie sezioni del malware dalla riga Section Headers. Cliccandoci sopra scopriamo che le sezioni sono 3, ma non hanno un nome intellegibile: sono semplicemente nominate come UPX0, UPX1, UPX2:







CONSIDERAZIONE FINALI

Durante l'analisi statica basica del malware, è stato possibile raccogliere alcune informazioni e da queste fare alcune deduzioni.

Il malware carica quattro librerie, che abbiamo già elencato. La presenza delle librerie di sistema come KERNEL32.DLL, USER32.DLL, ADVAPI32.DLL, e GDI32.DLL all'interno di un malware è comune, poiché queste DLL forniscono molte delle funzionalità di base necessarie per l'interazione con il sistema operativo Windows.

Il malware si compone di tre sezioni i cui nomi non sono "parlanti", ma a sigla numerata: questo fa pensare che il file sia crittato o compresso.

Possiamo dedurre che si tratti di un malware fra quelli più avanzati, per il fatto che oscura il nome delle sezioni, inoltre carica le librerie durante l'esecuzione (runtime import) nascondendo di fatto all'analisi statica le funzioni e le librerie importate. Questi malware sono riconoscibili in quanto hanno generalmente poche entry nella sezione import, e tra esse figurano le funzioni «LoadLibrary e GetProcAddress» che vengono appunto utilizzate per caricare funzioni addizionali durante l'esecuzione.

Con l'aiuto di VirusTotal, è stato possibile dedurre che il file malware è un Trojan.