# Esercizio S10 L1

## 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 descrizioneper ognuna di esse

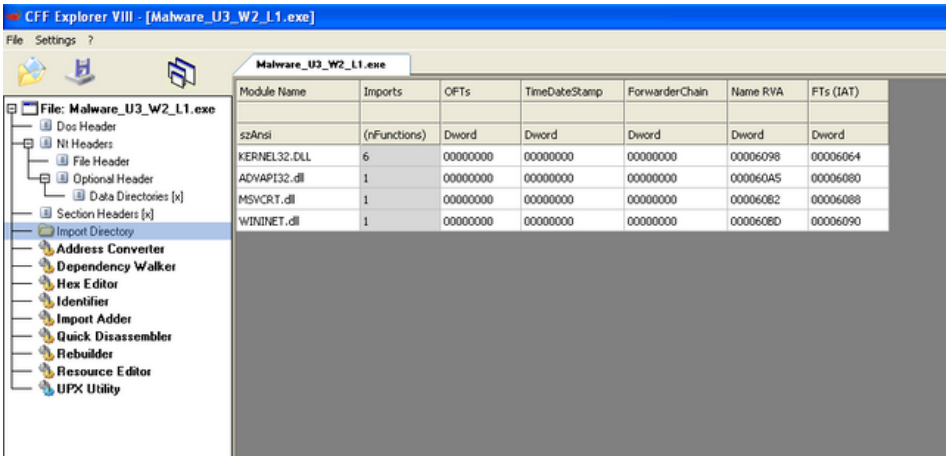
• Indicare le sezioni di cui si compone il malware, fornendo una descrizioneper ognuna di essa

• Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

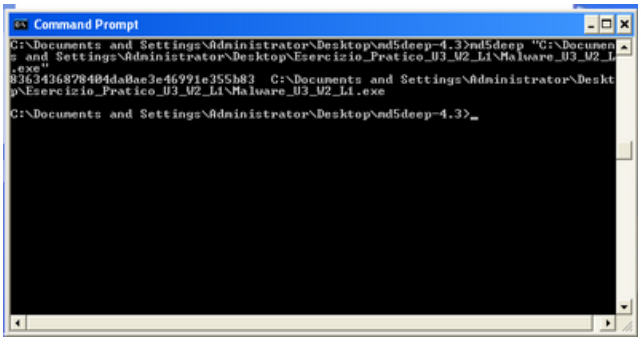
Le librerie importate dal malware sono state individuate con tre metodi:

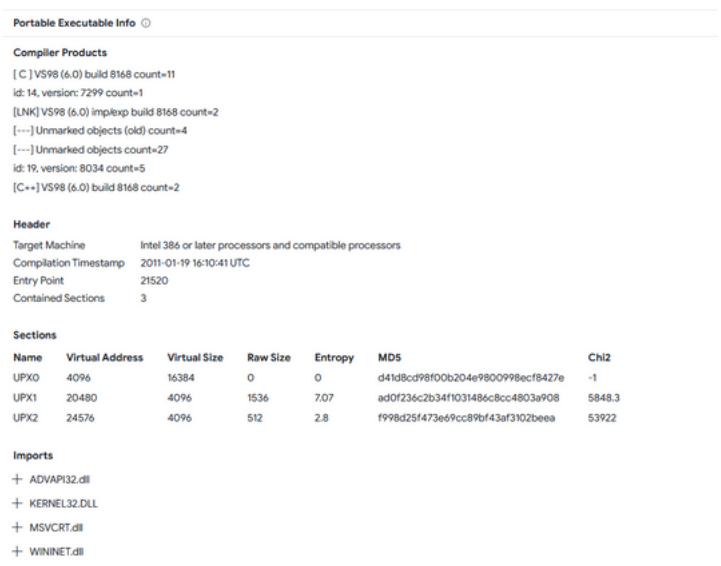
- Tramite l'utilizzo del programma strings che mostra le stringhe all'interno di un file .exe


- Tramite l'utilizzo del software CFF Explorer:




- Sono presenti su Virus Total inserendo l'Hash del malware ricavato tramite Md5deep:



Le librerie individuate sono:

**Kernel32.dll**
Contiene le funzioni principali per interagire con il sistema operativo.
Nello specifico le funzioni utilizzare sono:

- LoadLibraryA: Carica il modulo specificato nello spazio indirizzi del processo chiamante.
- GetProcAddress: Recupera l'indirizzo di una funzione esportata (nota anche come routine) o variabile dalla libreria di collegamento dinamico (DLL) specificata.
- VirtualProtect: Modifica la protezione in un'area di pagine di commit nello spazio indirizzi virtuale del processo di chiamata.
- VirtualAlloc: Riserva, impegna o modifica lo stato di una regione di pagine nello spazio degli indirizzi virtuali del processo chiamante.
- VirtualFree: Rilascia, decommits o rilascia e decommette un'area di pagine all'interno dello spazio indirizzi virtuale del processo chiamante.
- ExitProcess: Termina il processo chiamante e tutti i relativi thread.

**Advapi32.dll**
Contiene le funzioni per interagire con i servizi ed i registri del sistema operativo.
Funzioni utilizzate:

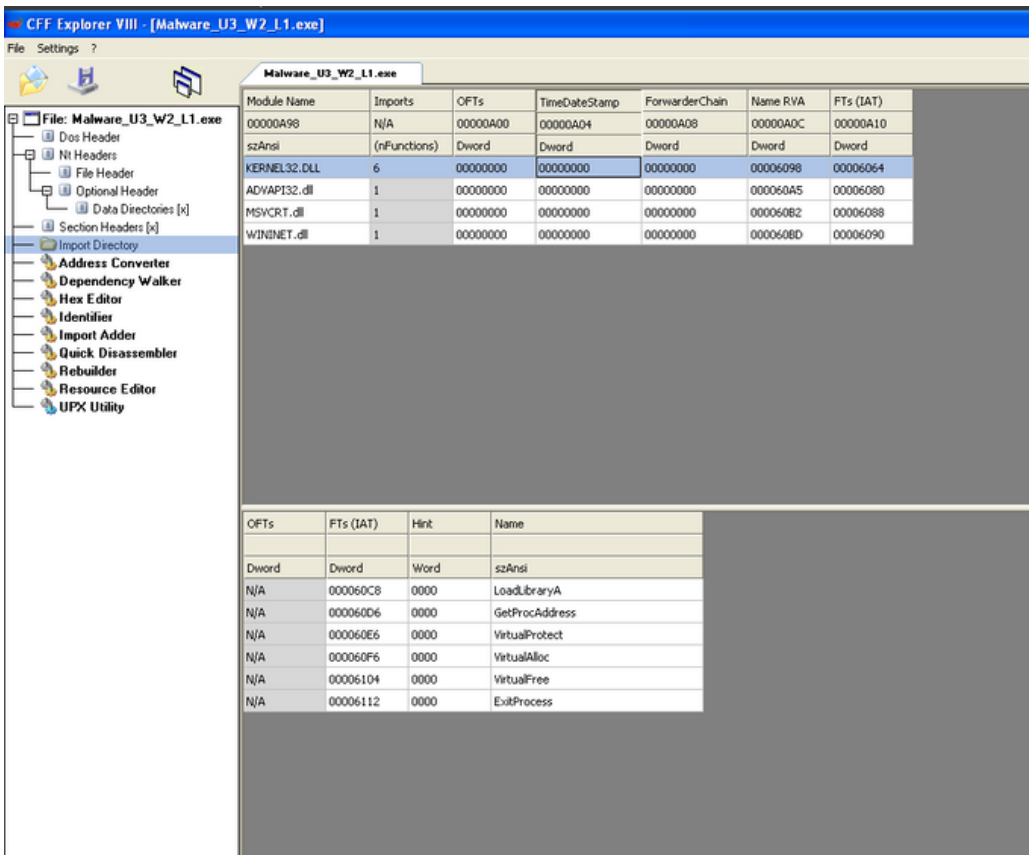
- CreateServiceA: Crea un oggetto di servizio e lo aggiunge al database del gestore di controllo dei servizi specificato.

**MSVCRT.dll**
Contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C.
Funzioni utilizzate:

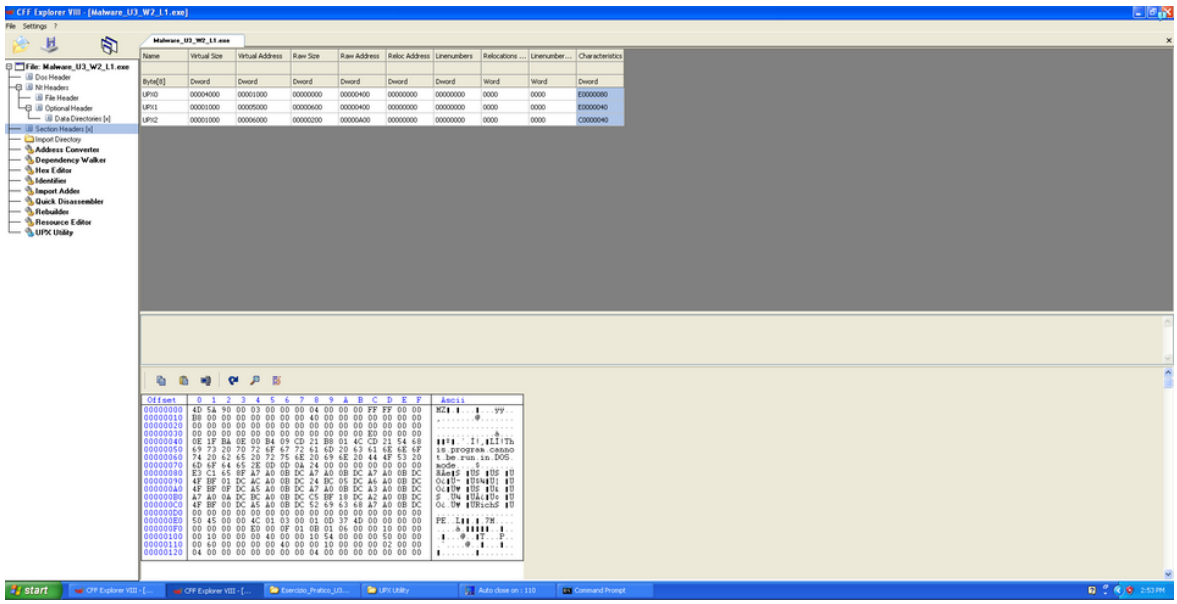
- exit: Termina il processo chiamante.

**Wininet.dll**
Contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.
Funzioni utilizzate:

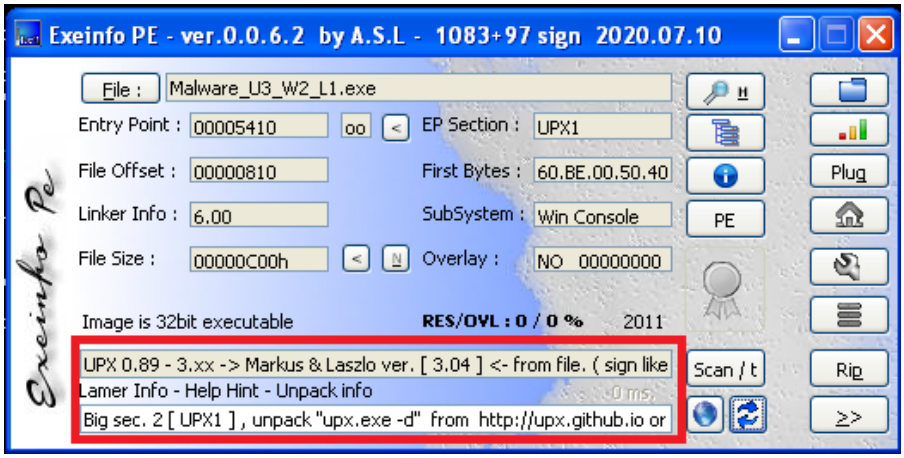
- InternetOpenA: Inizializza l'uso di un'applicazione delle funzioni WinINet.



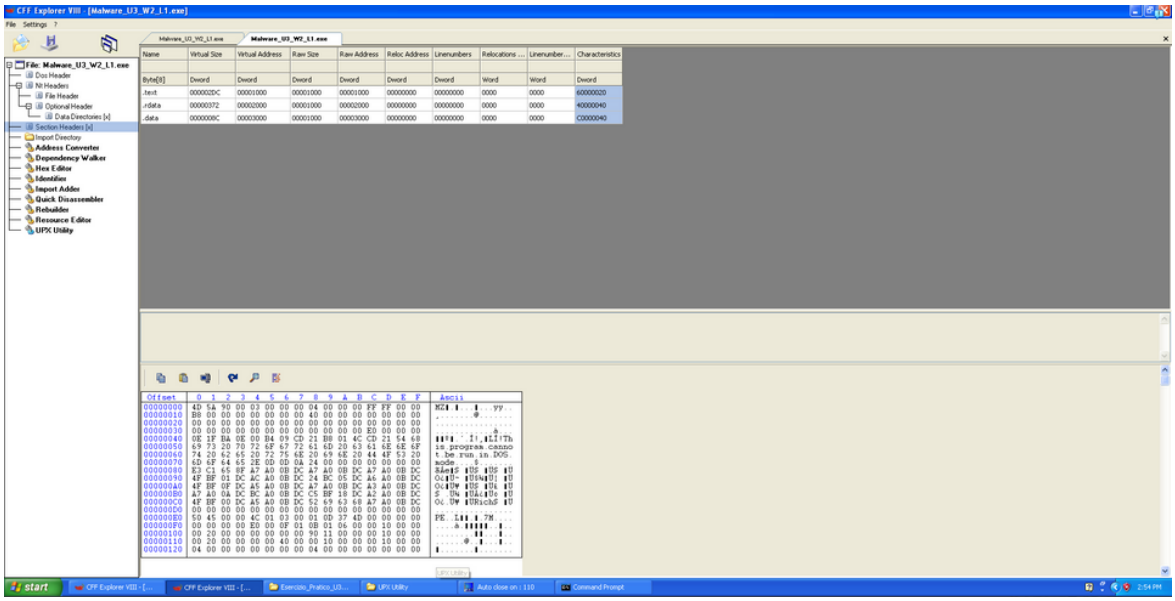
Le sezioni di cui si compone il malware sono state individuate tramite CFF Explorer.



Come possiamo notare sono compresse con UPX, per decomprimerle prima ho utilizzato EXE Info PE.




Ho individuato il metodo per decomprimere il file del malware.
Utilizzando UPX con il comando upx.exe -d “file” ho decompresso, possiamo notare riutilizzando CFF Explorer che le sezioni sono in chiaro adesso.



Le sezioni sono:

- **.text**: Contiene le istruzioni, ovvero le righe di codice, che la CPU eseguirà una volta che il software sarà avviato.
- **.rdata**: Include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile.
- **.data**: contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

Le informarzioni raccolte suggeriscono che il malware potrebbe coinvolgere la manipolazione della memoria virtuale, il caricamento dinamico di librerie, la gestione dei servizi di Windows e l'accesso a Internet.
Potrebbe trattarsi di un **downloader** che  è solitamente progettato per scaricare e installare un ulteriore malware sul sistema compromesso. Le funzioni come “LoadLibraryA” e “GetProcessAddress” potrebbero essere coinvolte nell'aggiornamento dinamico di funzionalità del malware attraverso il caricamento di librerie dinamiche.

Oppure potrebbe trattarsi di una **backdoor** che è progettata per aprire un canale segreto di comunicazione tra il sistema compromesso e un server remoto, consentendo agli attaccanti di eseguire comandi a distanza o di svolgere altre attività dannose. Funzioni come “CreateServiceA” e l'accesso a Internet tramite “InternetOpenA” potrebbero essere utilizzate in una backdoor per installarsi come servizio di sistema o per comunicare con un server di comando e controllo.

Analizzando comunque le informazioni presenti su virus total è chiaro si tratti di un **trojan downloader**.