

A decorative graphic on the left side of the slide. It consists of a blue parallelogram and a light green parallelogram, both tilted at an angle. The blue shape is in the foreground, and the green shape is partially behind it. They are set against a dark blue background with faint, lighter blue diagonal stripes.

# Esercizio S10 L1



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:

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



# Librerie del malware

Per affrontare l'esercizio di oggi e quelli dei prossimi giorni è necessario scaricare il pacchetto .ova fornito che contiene tutti gli strumenti da utilizzare per i prossimi esercizi oltre ad i malware che andremo ad analizzare.

Dopo aver scaricato il file .ova lo andremo ad aprire all'interno di Oracle VM Virtualbox, così facendo creiamo una nuova macchina virtuale.

Apriamo la nuova macchina virtuale appena creata ed andiamo all'interno della cartella MALWARE ed apriamo il file malware U3\_W2\_L1.exe con CFF Explorer.

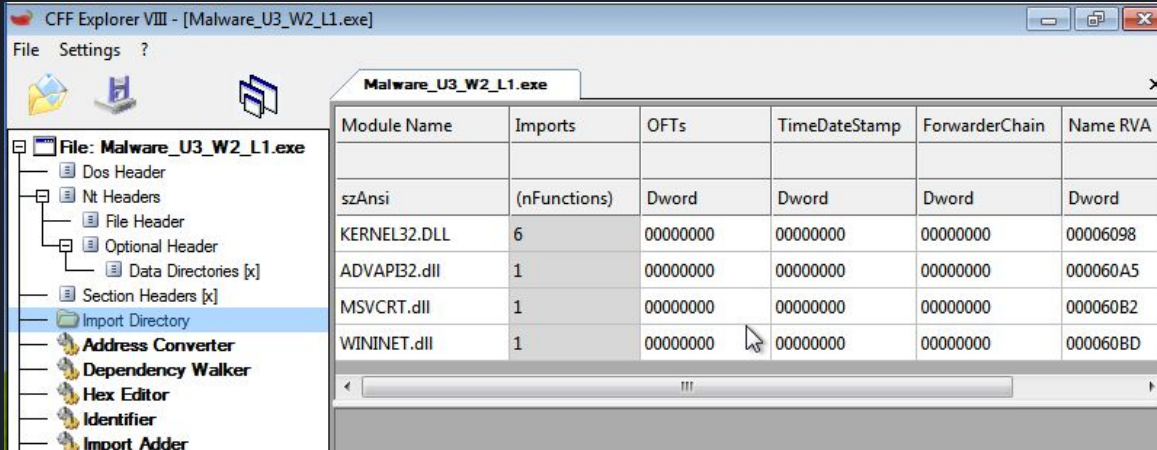
CFF Explorer è un PE editor e process viewer gratuito creato da Erik Pistelli che noi andiamo ad utilizzare per fare analisi statica basica del malware.

# Librerie del malware

Per osservare le librerie importate dal malware ci spostiamo all'interno della sezione Import Directory ed osserviamo che il malware che stiamo analizzando importa 4 diverse librerie:

Kernel32.dll , Advapi32.dll , Msvcrt.dll , Wininet.dll

Cerchiamo di capire adesso queste librerie cosa fanno.



CFF Explorer VIII - [Malware\_U3\_W2\_L1.exe]

File Settings ?

Malware\_U3\_W2\_L1.exe

| Module Name  | Imports      | OFTs     | TimeDateStamp | ForwarderChain | Name RVA |
|--------------|--------------|----------|---------------|----------------|----------|
| szAnsi       | (nFunctions) | Dword    | Dword         | Dword          | Dword    |
| KERNEL32.DLL | 6            | 00000000 | 00000000      | 00000000       | 00006098 |
| ADVAPI32.dll | 1            | 00000000 | 00000000      | 00000000       | 000060A5 |
| MSVCRT.dll   | 1            | 00000000 | 00000000      | 00000000       | 000060B2 |
| WININET.dll  | 1            | 00000000 | 00000000      | 00000000       | 000060BD |



# Librerie del malware

- **Kernel32.dll** è un modulo del kernel di Windows. È una libreria di collegamento dinamico a 32 bit utilizzata nei sistemi operativi Windows. All'avvio del sistema, kernel32.dll viene caricato in una memoria protetta in modo che non venga danneggiato da altri processi del sistema o dell'utente. Funziona come processo in background e svolge funzioni importanti come la gestione della memoria, operazioni di input/output e interruzioni.
- **Advapi32.dll** fa parte della libreria di servizi API avanzati. Fornisce l'accesso a funzionalità avanzate che vengono fornite in aggiunta al kernel. È responsabile di cose come il registro di Windows, il riavvio e l'arresto del sistema, l'avvio/arresto e la creazione di servizi Windows e la gestione degli account utente.



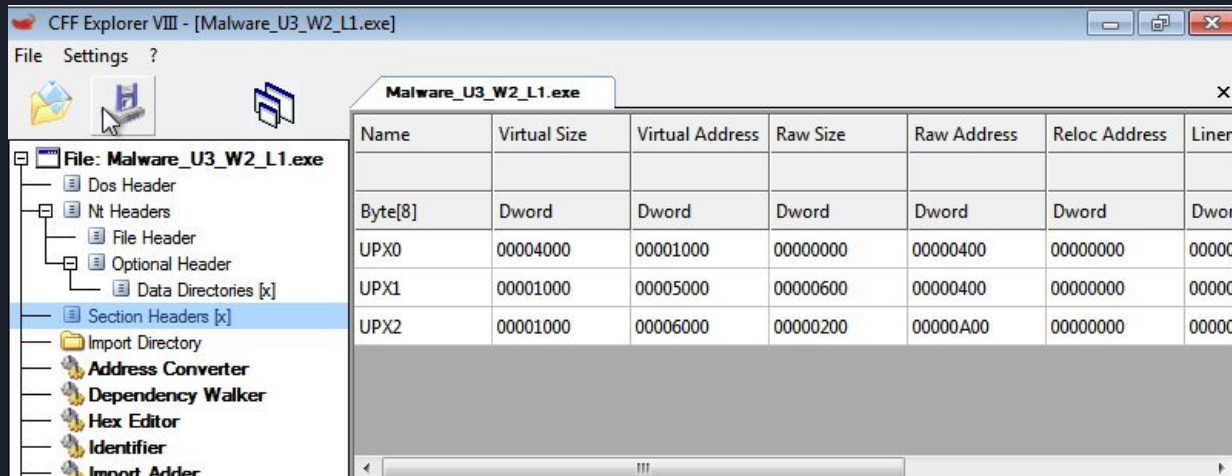
# Librerie del malware

- Il file **Msvcrt.dll**, noto anche come Microsoft C Runtime Library, è un componente cruciale del sistema operativo Windows. Contiene una raccolta di funzioni e risorse utilizzate da vari programmi per eseguire attività comuni, come l'allocazione della memoria, le operazioni di input/output di file e la gestione delle eccezioni.
- **Wininet.dll** è un componente cruciale del sistema operativo Windows che svolge un ruolo significativo nello stabilire e mantenere le connessioni Internet. È responsabile della gestione di varie funzioni relative a Internet, come i protocolli HTTP, FTP e HTTPS, nonché della gestione dei cookie e della memorizzazione nella cache.

# Sezioni del malware

Per visualizzare le varie sezioni di cui è composto il malware ci spostiamo adesso nella sezione Section Headers [x] del programma e vediamo che il malware ha 3 diverse sezioni.

Sembra che il malware abbia camuffato il vero nome delle sezioni con le scritte UPX0-1-2 che non ci permettono di risalire al vero nome delle sezioni e pertanto non è possibile analizzare più approfonditamente le sezioni.



| Name    | Virtual Size | Virtual Address | Raw Size | Raw Address | Reloc Address | Linen |
|---------|--------------|-----------------|----------|-------------|---------------|-------|
| Byte[8] | Dword        | Dword           | Dword    | Dword       | Dword         | Dwor  |
| UPX0    | 00004000     | 00001000        | 00000000 | 00000400    | 00000000      | 00000 |
| UPX1    | 00001000     | 00005000        | 00000600 | 00000400    | 00000000      | 00000 |
| UPX2    | 00001000     | 00006000        | 00000200 | 00000A00    | 00000000      | 00000 |



## Considerazioni finali:

Dai dati delle analisi appena svolte è possibile evincere che il malware sia in grado di camuffarsi per nascondere le proprie sezioni, di conseguenza deve trattarsi di un malware abbastanza avanzato in termini di capacità che sfrutta le librerie chiamate durante il Runtime e che rende difficile una analisi dettagliata sfruttando tecniche di analisi basica statica.