S10_L1
Unit 3 - CS0424

MATTEO BELTRAMI MARZOLINI
CYBEREAGLES

Giorno 1 – Analisi Statica Dinamica

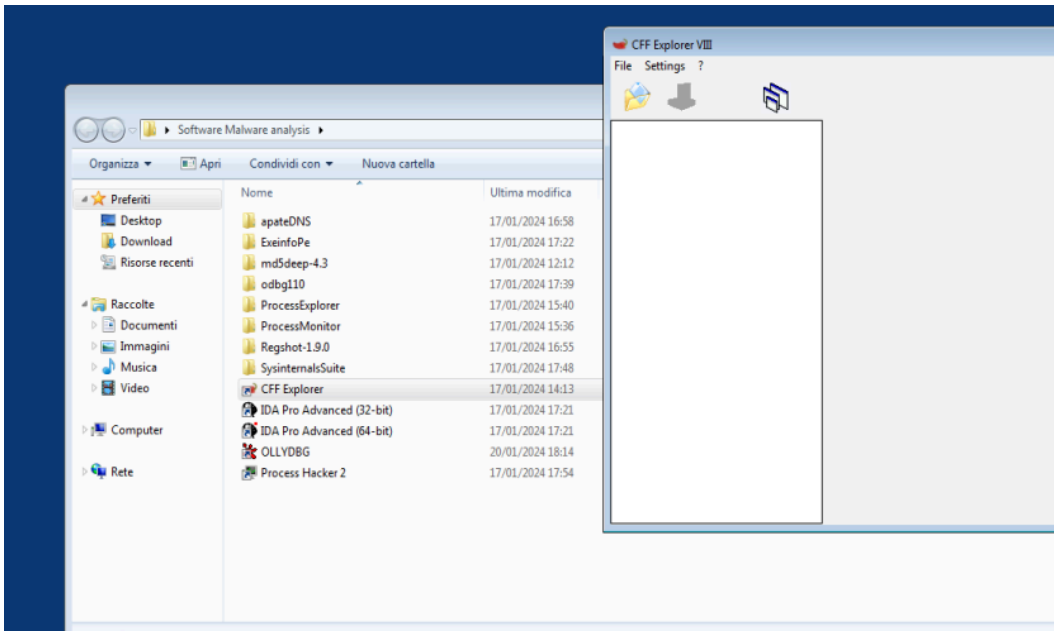
TRACCIA

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:

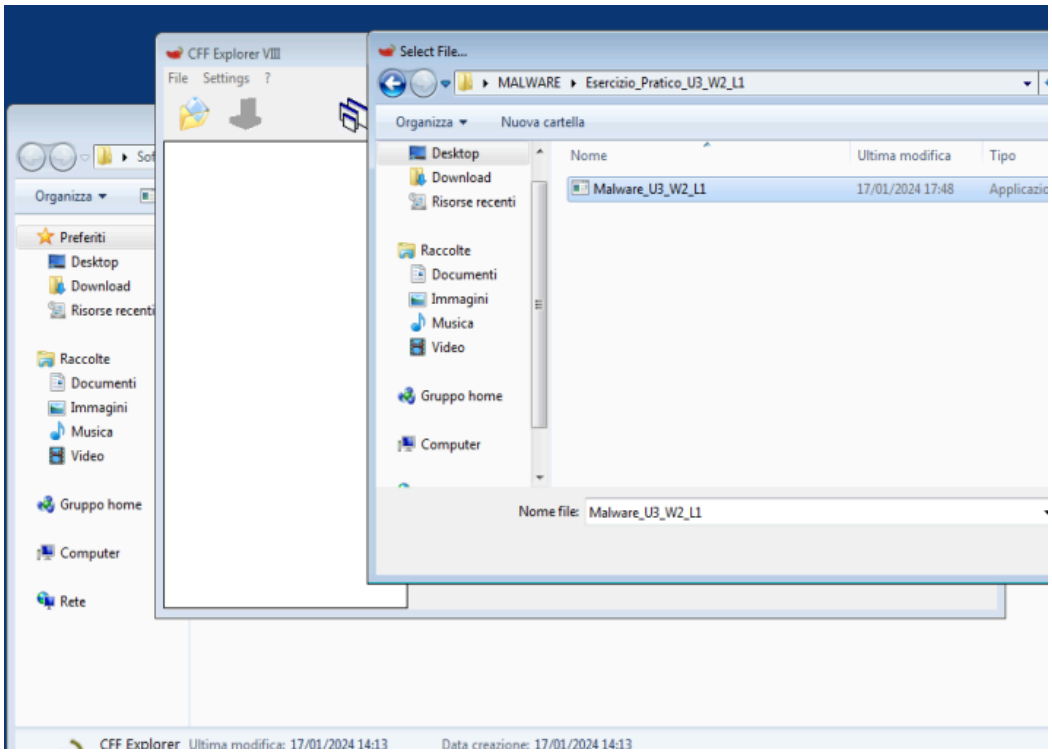
- Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse
- Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

SVOLGIMENTO

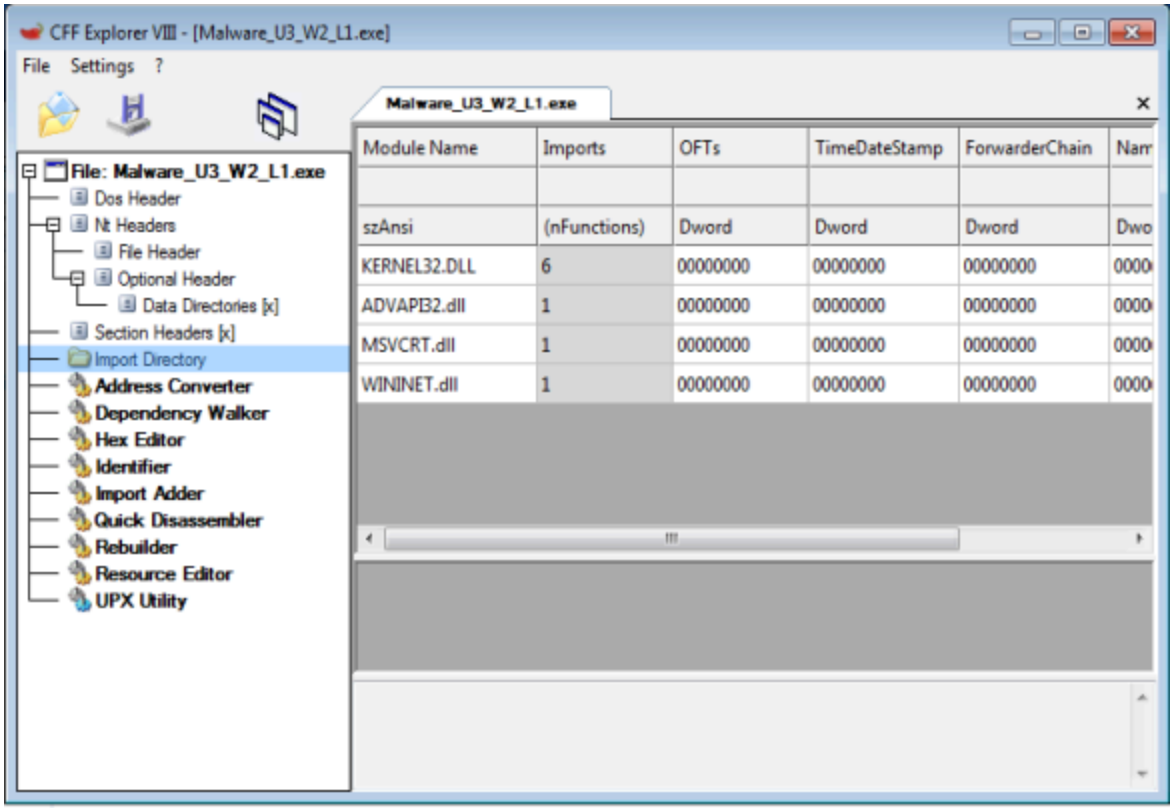
Per procedere all’esercizio, avvio CFF Explorer.



Dopo aver selezionato il malware U3_W2_L1



si procede selezionando la Import Directory in quanto la traccia richiede di indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse.



Come si può notare saranno presenti 4 librerie importate:

1. Kernel32.dll

`Kernel32.dll` è una delle librerie più importanti di Windows. Fornisce l'accesso a una vasta gamma di funzioni di sistema a livello di kernel, che sono essenziali per la gestione delle risorse di sistema e l'esecuzione di applicazioni. Alcune delle principali funzionalità offerte da questa libreria includono:

- **Gestione della memoria:** Funzioni per allocare e liberare memoria.
- **Gestione dei file:** Funzioni per aprire, leggere, scrivere e chiudere file.
- **Thread e processi:** Funzioni per la gestione di thread e processi.
- **Temporizzazione:** Funzioni per la gestione del tempo e dei timer.

2. Advapi32.dll

`Advapi32.dll` (Advanced Windows 32 Base API) contiene funzioni avanzate per la gestione della sicurezza e altre funzionalità di sistema avanzate. Include:

- **Gestione della sicurezza:** Funzioni per gestire l'accesso e le autorizzazioni, come la gestione dei token di sicurezza e delle ACL (Access Control List).
- **Registro di sistema:** Funzioni per leggere e scrivere chiavi nel registro di sistema di Windows.
- **Servizi di sistema:** Funzioni per avviare, fermare e configurare servizi di sistema.

3. MSVCRT.dll

`MSVCRT.dll` (Microsoft Visual C Runtime) è una libreria runtime del C fornita con Microsoft Visual C++. Fornisce implementazioni delle funzioni della libreria standard del C, come:

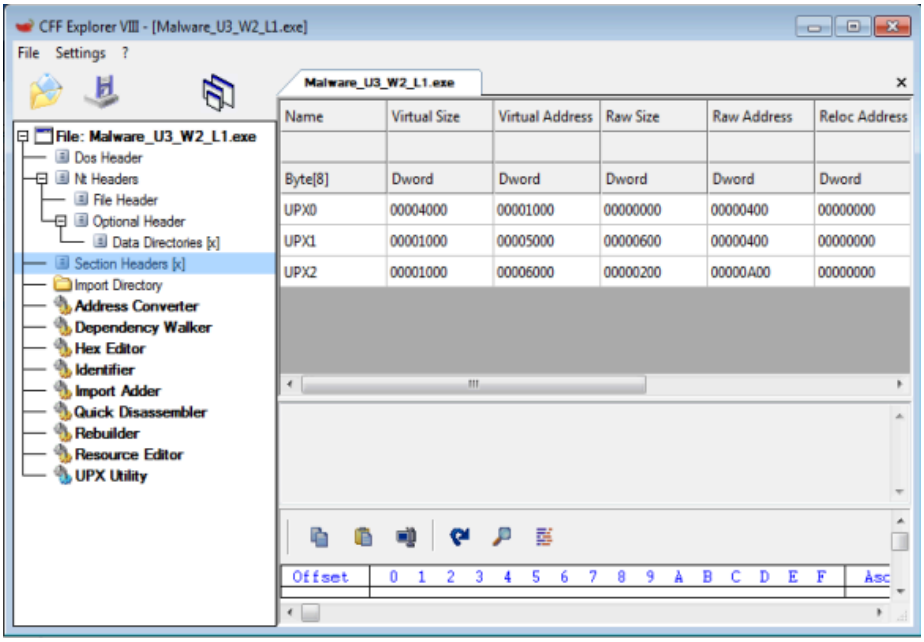
- **Gestione delle stringhe:** Funzioni per manipolare stringhe.
- **Input/output:** Funzioni per la gestione dell'input e dell'output.
- **Operazioni matematiche:** Funzioni matematiche comuni.
- **Gestione della memoria:** Funzioni per l'allocazione e la liberazione della memoria.

4. Wininet.dll

`Wininet.dll` (Windows Internet API) fornisce un insieme di funzioni per l'accesso a internet e alle reti. Include:

- **HTTP/FTP:** Funzioni per gestire richieste e risposte HTTP e trasferimenti FTP.
- **Cache:** Funzioni per gestire la cache dei contenuti web.
- **Autenticazione:** Funzioni per gestire l'autenticazione su siti web.

Successivamente la traccia richiede di indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa



Si può notare la presenza di 3 sezioni, però non siamo in grado di capire che tipo di sezioni sono perchè il malware sembra abbia nascosto il vero nome delle sezioni.

Per le considerazioni finali, il malware non ci consente di recuperare molte informazioni sul suo comportamento con l'analisi statica base.

Ciò è supportato dal fatto che tra le funzioni importate troviamo «LoadLibrary e GetProcAddress», che ci fanno pensare ad un malware che importa le librerie a tempo di esecuzione (runtime) nascondendo di fatto le informazioni circa le librerie importate a monte.