2024

EPICODE

CS0124

REPORT

Week 10 Lesson 1

PREPARED BY : Bruno Falconi

Report sull'Analisi del Malware - Esercizio_Pratico_U3_W2_L1

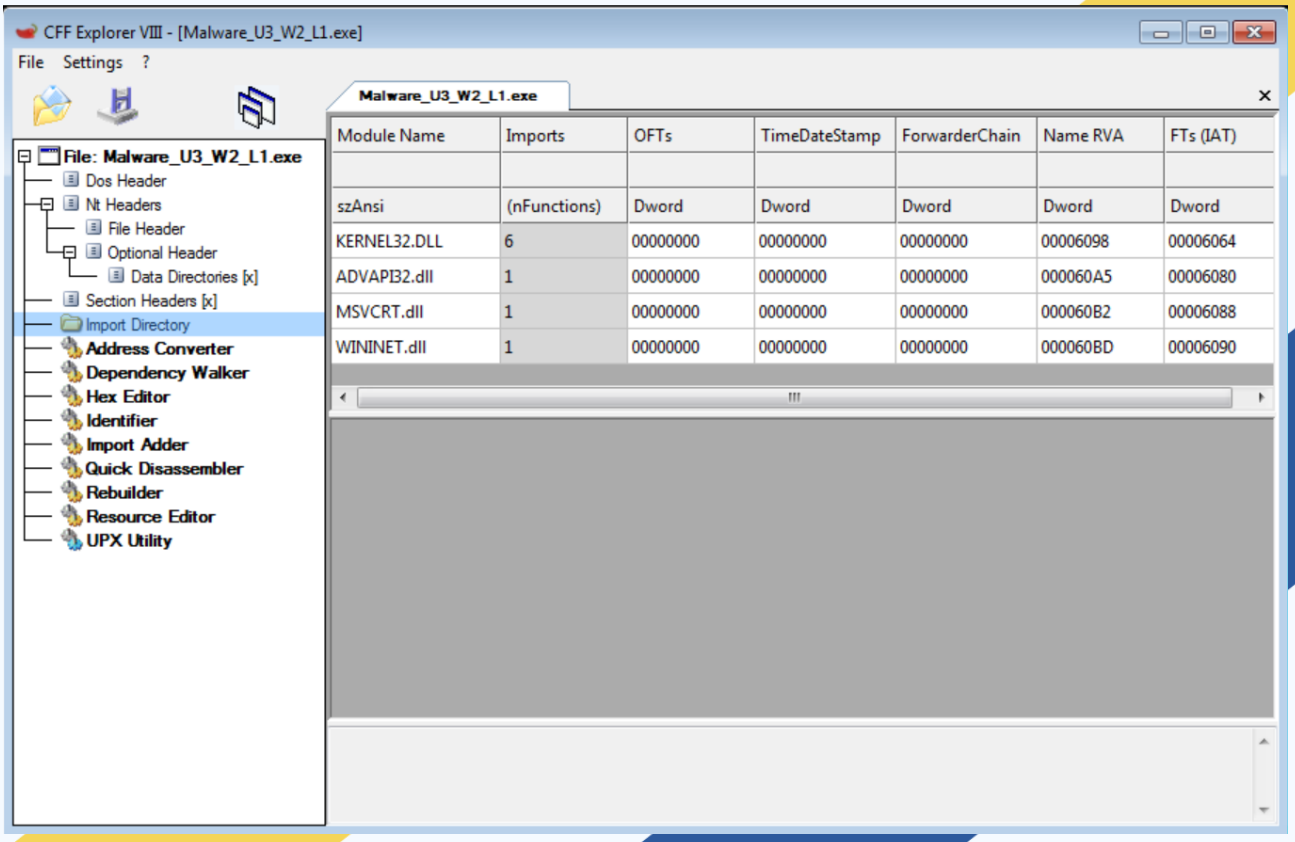
Introduzione

Il presente report descrive l'analisi del file eseguibile "Esercizio_Pratico_U3_W2_L1" trovato nella cartella omonima sul Desktop della macchina virtuale dedicata all'analisi dei malware. Il file è stato sottoposto a varie analisi utilizzando CFF Explorer VIII, compresa la verifica MD5 tramite Ash, e successivamente è stato caricato su VirusTotal per una scansione antivirus e un'ulteriore analisi. Lo scopo di queste analisi è identificare le librerie importate, le sezioni e le potenziali minacce del malware.

Analisi delle Librerie Importate e Sezioni del Malware:

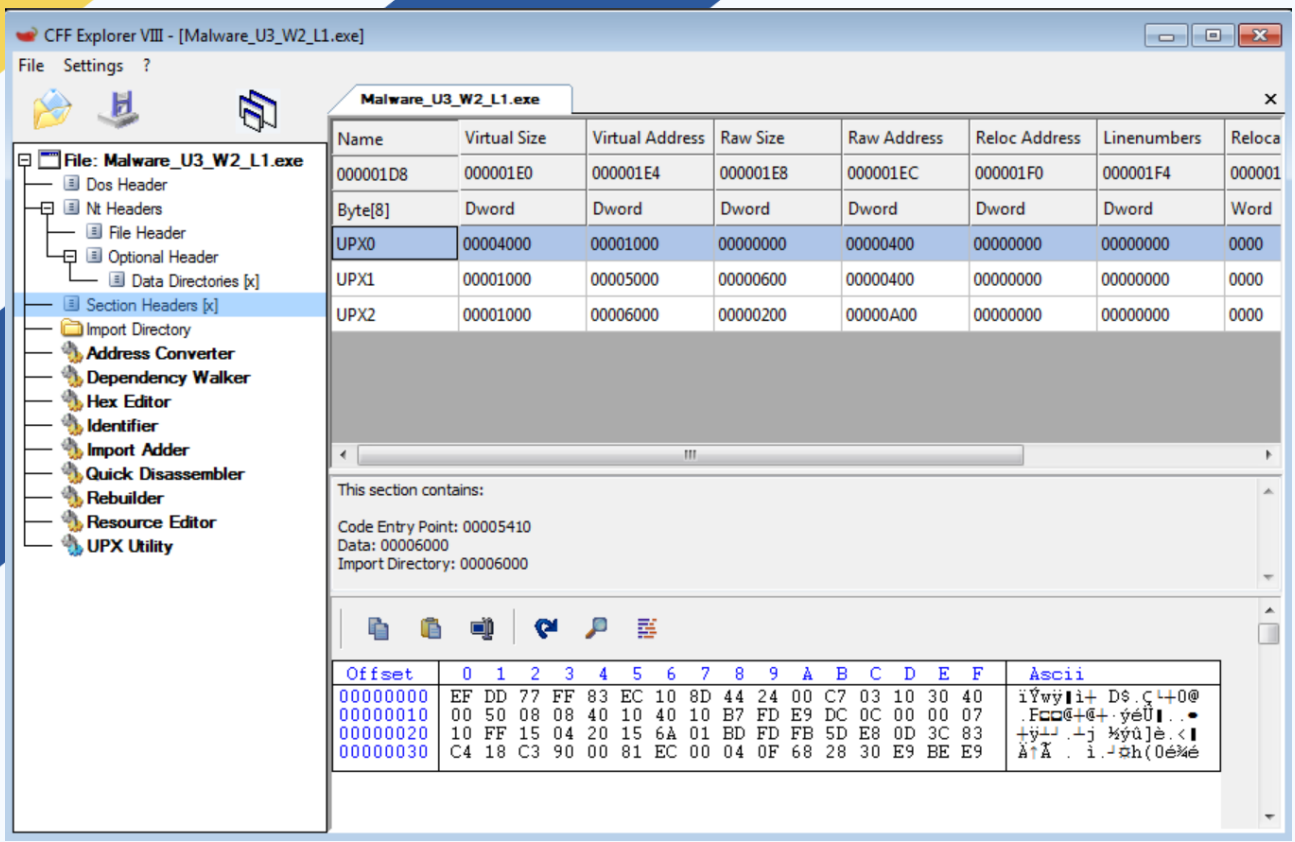
Dopo un'attenta analisi con CFF Explorer VIII, sono state individuate le seguenti librerie importate e funzioni del malware:

1. **Librerie Importate:**
    - **KERNEL32.dll:**
        - LoadLibraryA
        - GetProcAddress
        - VirtualProtect
        - VirtualAlloc
        - VirtualFree
        - ExitProcess
    - **ADVAPI32.dll:**
        - CreateServiceA
    - **MSVCRT.dll:**
        - exit
    - **WININET.dll:**
        - InternetOpenA



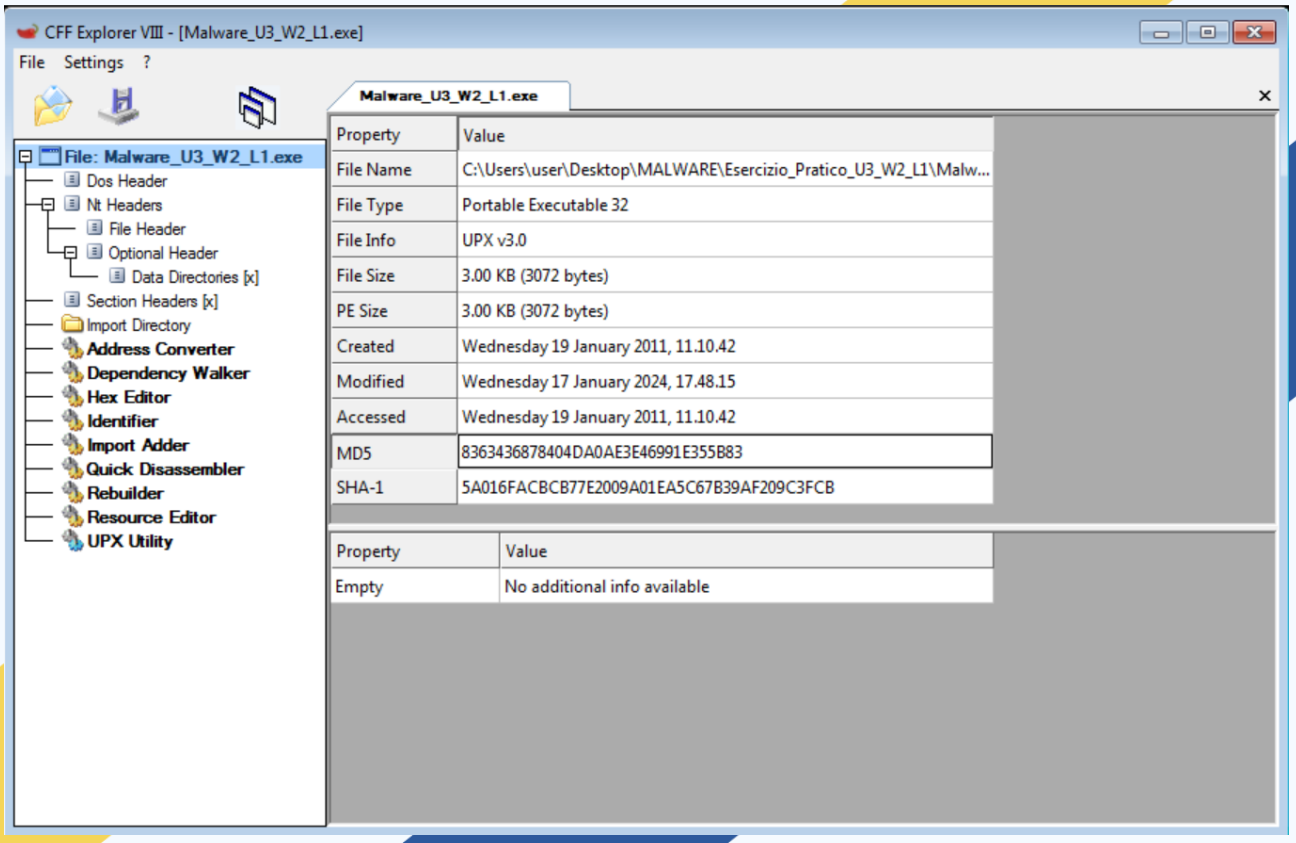
2. **Sezioni del Malware:**

   - Sezioni Codificate: All'interno del malware sono presenti tre sezioni il cui contenuto è codificato e non immediatamente leggibile. Queste sezioni potrebbero contenere dati crittografati o codificati utilizzati per scopi non rivelati.



Analisi con VirusTotal:

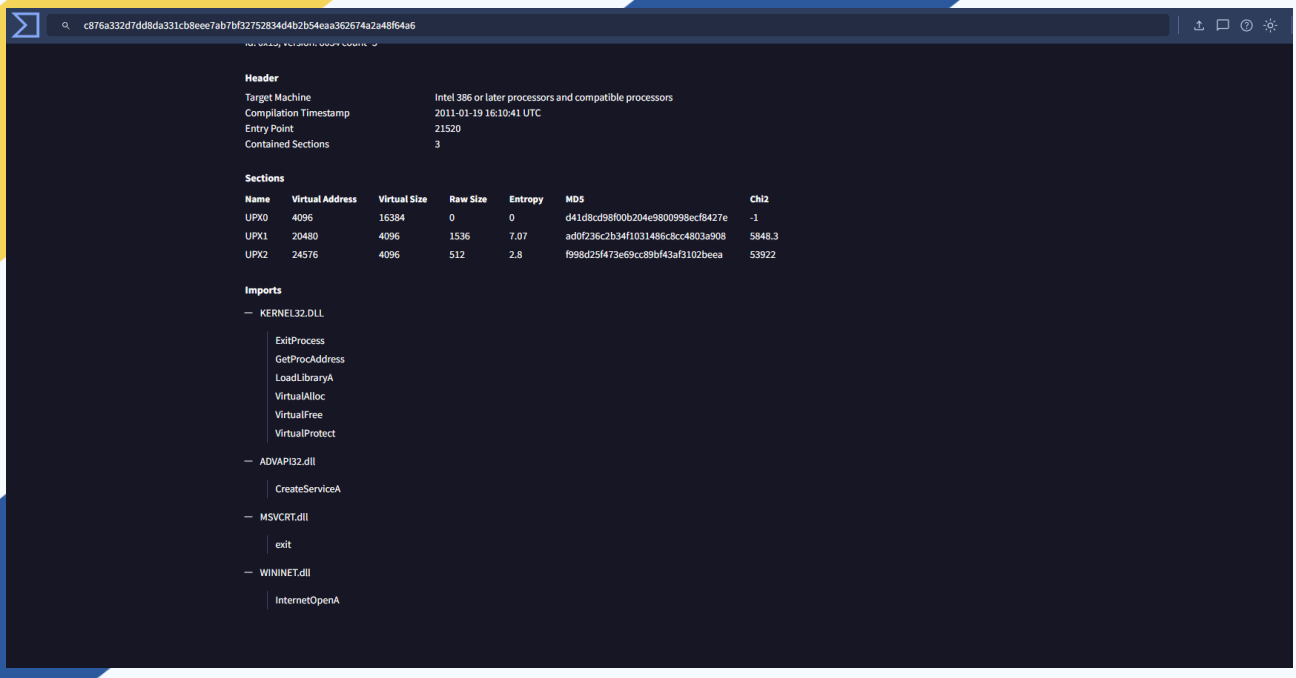
Dopo aver ottenuto il checksum MD5 del file tramite Ash, lo abbiamo caricato su VirusTotal per eseguire una scansione antivirus e un'ulteriore analisi. Abbiamo confrontato le informazioni fornite da VirusTotal con quelle ottenute da CFF Explorer per identificare eventuali discrepanze.



Risultati dell'Analisi:

- Le informazioni sulle librerie importate segnalate da CFF Explorer corrispondono a quelle segnalate da VirusTotal, confermando la coerenza delle informazioni fornite da entrambi gli strumenti.

- Non sono state identificate discrepanze tra le librerie segnalate da CFF Explorer e quelle segnalate da VirusTotal.



Ipotesi di Funzionamento del Malware:

Basandoci sulle informazioni fornite dalle analisi, possiamo ipotizzare il seguente funzionamento del malware:

1. **Caricamento Dinamico di Librerie**: Il malware potrebbe caricare dinamicamente altre librerie utilizzando le funzioni di caricamento come **LoadLibraryA** e **GetProcAddress**. Questo potrebbe consentire al malware di estendere le sue funzionalità o di caricare moduli aggiuntivi per eseguire operazioni specifiche.
2. **Manipolazione della Memoria**: Le funzioni come **VirtualProtect**, **VirtualAlloc**, e **VirtualFree** potrebbero consentire al malware di manipolare la memoria del processo

corrente. Questo potrebbe essere utilizzato per eseguire tecniche di evasione delle protezioni o per nascondere parti del malware dalla rilevazione.

3. **Comunicazione su Internet**: La presenza della funzione **InternetOpenA** indica che il malware è in grado di inizializzare una sessione di comunicazione su Internet. Questo potrebbe consentire al malware di inviare o ricevere dati da server remoti, potenzialmente per scopi dannosi come il furto di informazioni o l'esecuzione di comandi remoti.
4. **Creazione di Servizi di Sistema**: La funzione **CreateServiceA** potrebbe consentire al malware di creare un nuovo servizio di sistema o aprire un servizio esistente. Questo potrebbe essere utilizzato per persistere nel sistema, eseguendo il malware automaticamente all'avvio del sistema o con privilegi elevati.
5. **Terminazione del Processo**: La funzione **ExitProcess** potrebbe consentire al malware di terminare il processo corrente e tutti i suoi thread in esecuzione. Questo potrebbe essere utilizzato per interrompere l'esecuzione di processi critici o per nascondere le tracce del malware dopo aver completato le sue attività.

Considerazioni Finali:

L'analisi del malware ha rivelato l'utilizzo di librerie importate comuni per operazioni di sistema, comunicazione su Internet e altro ancora. La presenza di sezioni codificate indica la presenza di dati o istruzioni non immediatamente leggibili, che richiedono ulteriori analisi per comprenderne appieno il contenuto e le potenziali minacce. Nonostante le informazioni fornite da CFF Explorer e VirusTotal siano