S10-L1

Intro

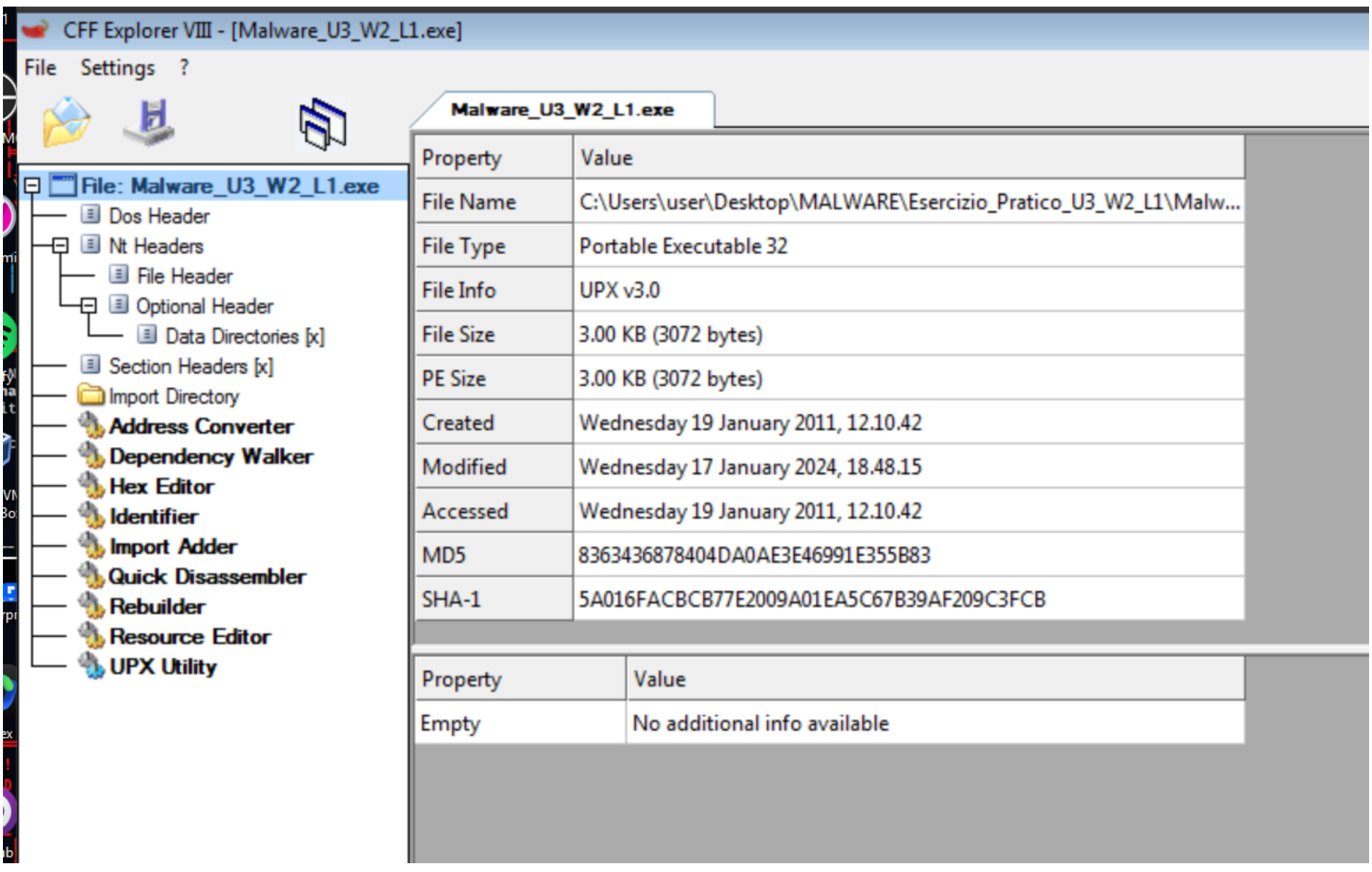
In questo report, presentiamo un'analisi dettagliata del file eseguibile "Malware_U3_W2_L1.exe" utilizzando il programma CFF Explorer.
L'obiettivo di questa analisi è identificare le caratteristiche strutturali e funzionali del file.

Il software CFF Explorer è stato scelto per la sua capacità di fornire una visione approfondita della composizione interna degli eseguibili di Windows.
La nostra analisi si concentra su due aspetti principali: le "Section Headers", che descrivono le varie sezioni del file, e le “Import Directory", che elenca le librerie esterne utilizzate dal programma.

La comprensione di questi elementi è fondamentale per determinare il comportamento potenziale del file eseguibile e le sue possibili intenzioni malevole.

Estratto di Report sull'Analisi di un File Eseguibile con CFF Explorer

Generalità sul malware:

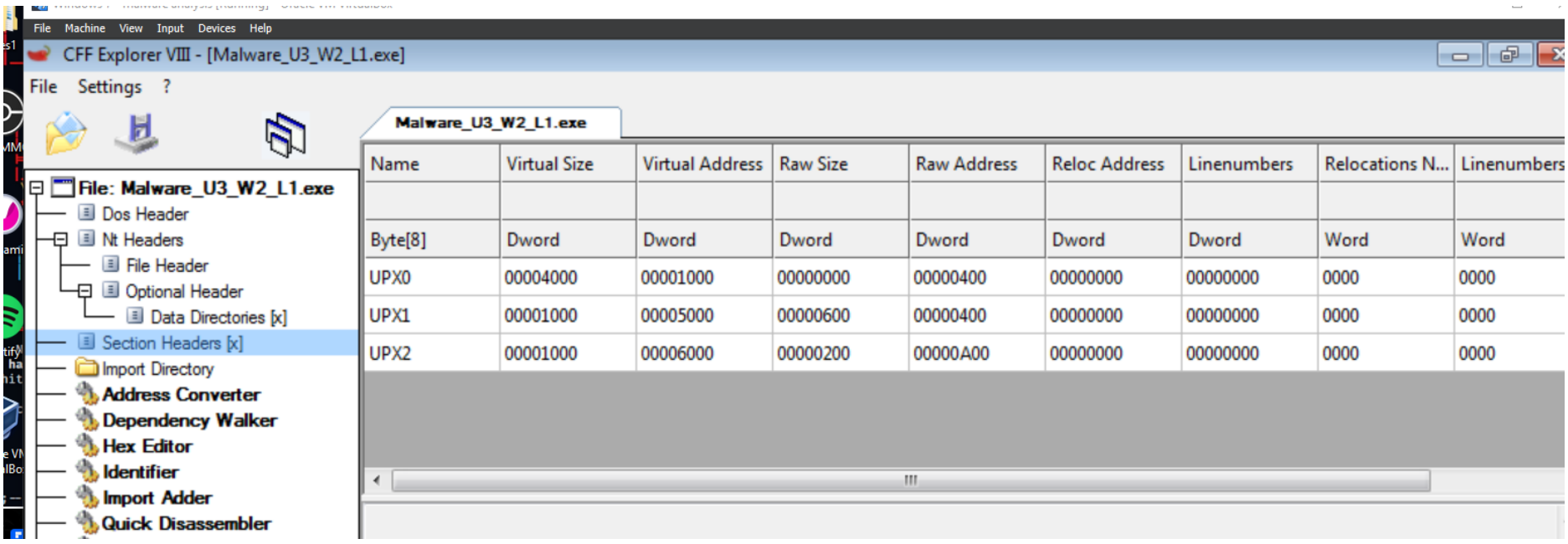


Section Headers

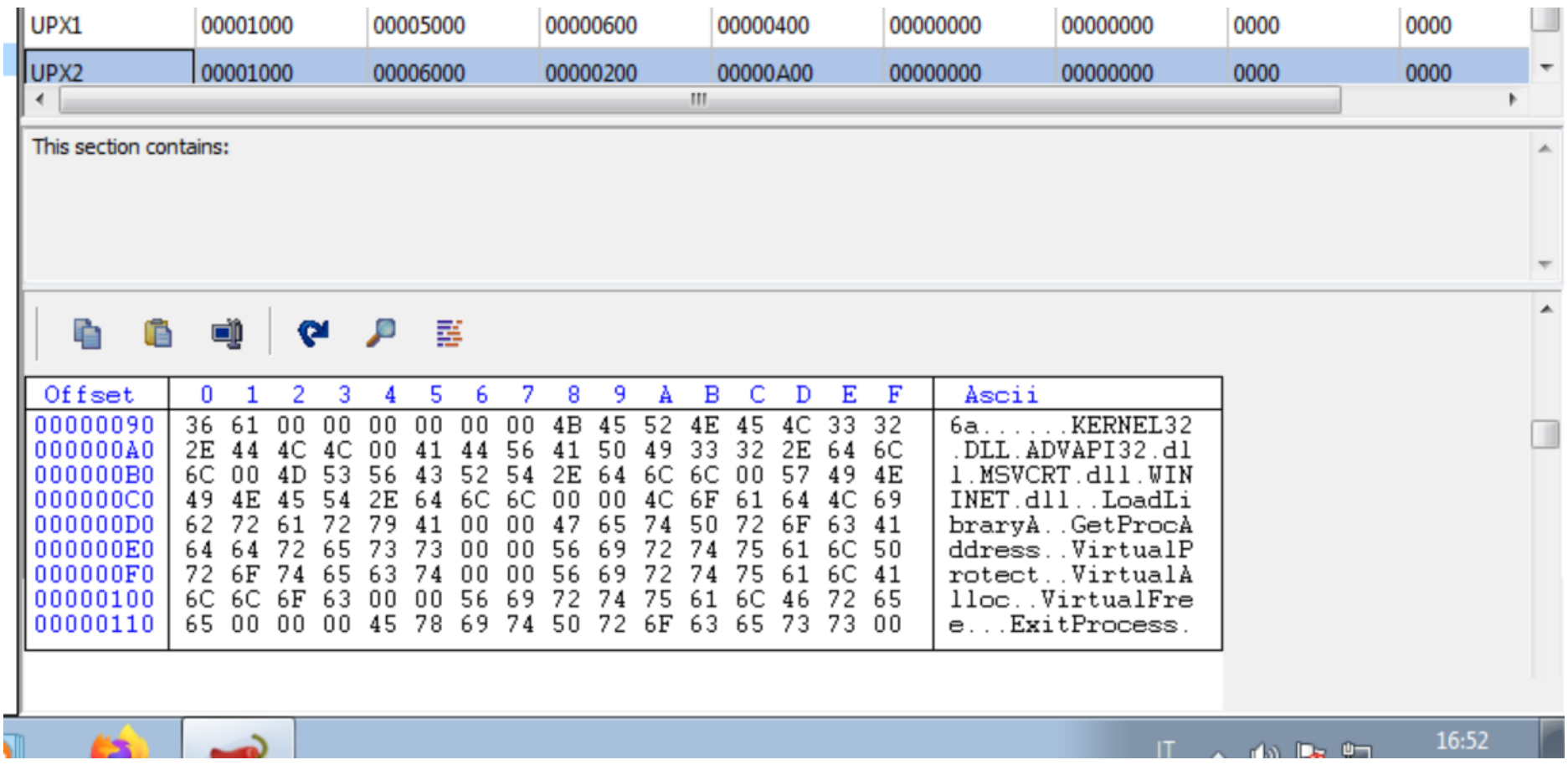
Sezioni UPX

Le sezioni indicate come "UPX0", "UPX1" e "UPX2" (In Section Headers) stanno ad indicare che il file .exe è stato compresso utilizzando UPX (Ultimate Packer for eXecutables).
UPX è un compressore di eseguibili che riduce le dimensioni del file, complicandone l'analisi senza una decompressione preliminare.

- **UPX0**: di solito contiene il codice compresso del programma.
- **UPX1**: di solito ospita il codice originale non compresso del programma.
- **UPX2**: potrebbe contenere dati o codice aggiuntivi.



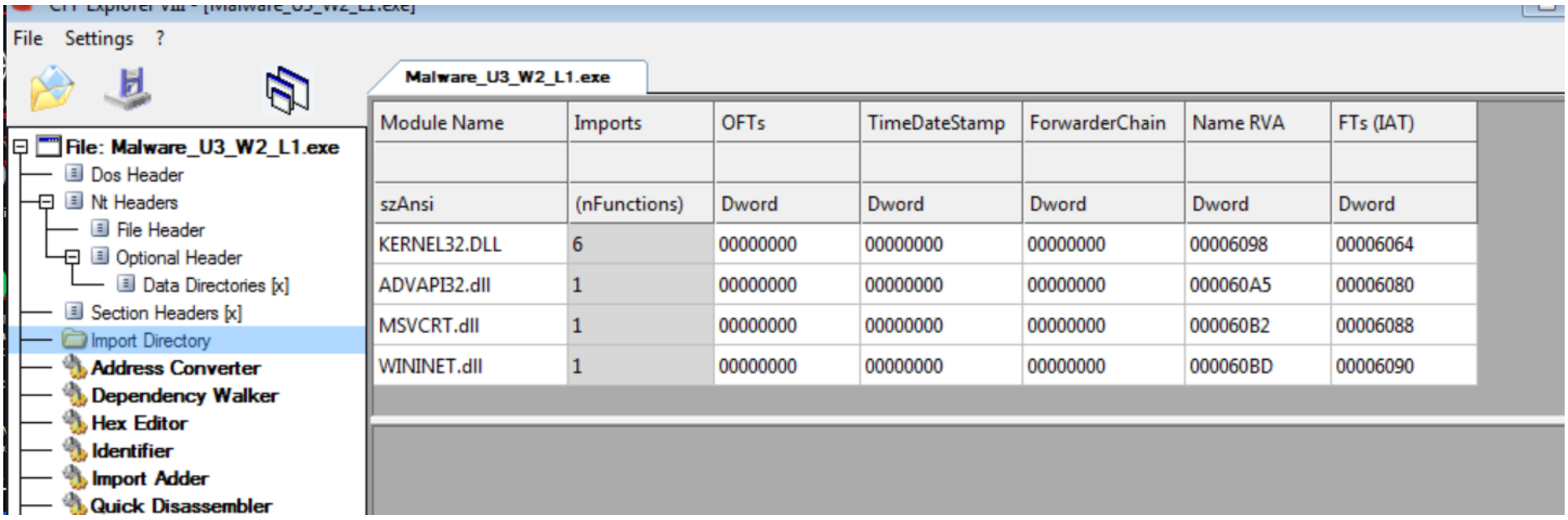
Zoom su UPX2



Import Directory

La tabella delle importazioni del file eseguibile evidenzia le librerie DLL (Dynamic Link Library) che il malware carica e utilizza.

Librerie Importate



- **KERNEL32.DLL**: Contiene funzioni fondamentali di Windows per la gestione della memoria, dei file, dei processi e dei thread, tra le altre funzioni di sistema di basso livello.
  Il malware che importa funzioni da questa libreria potrebbe voler manipolare file, gestire processi o eseguire altre operazioni di sistema.
- **ADVAPI32.DLL**: Include funzioni avanzate API di Windows, molte delle quali legate alla gestione della sicurezza e delle operazioni del registro.
  Importare funzioni da questa libreria può indicare che il malware tenta di accedere o modificare voci del registro di sistema o gestire i privilegi e le autorizzazioni degli utenti.
- **MSVCRT.DLL**: Parte del Microsoft Visual C++ Runtime, contiene funzioni di base per la gestione di input/output, stringhe, gestione della memoria e altre operazioni standard in C.
  Il malware potrebbe usare queste funzioni per operazioni di calcolo e gestione dei dati.
- **WININET.DLL**: Fornisce funzioni per l'accesso a Internet, inclusi protocolli come HTTP e FTP. L'importazione di questa libreria può indicare che il malware tenta di comunicare con server remoti, scaricare o caricare dati, o svolgere altre attività di rete.

L'uso di queste librerie suggerisce che il malware potrebbe essere progettato per eseguire una varietà di operazioni (ovvero quelle consentite utilizzando le libreria sopra citate), tra cui:

- **Manipolazione di file e processi**: tramite KERNEL32.DLL.
- **Modifiche al registro di sistema o gestione delle autorizzazioni**: attraverso ADVAPI32.DLL.
- **Comunicazioni di rete**: sfruttando WININET.DLL.
- **Operazioni generali di calcolo e gestione dei dati**: utilizzando MSVCRT.DLL.