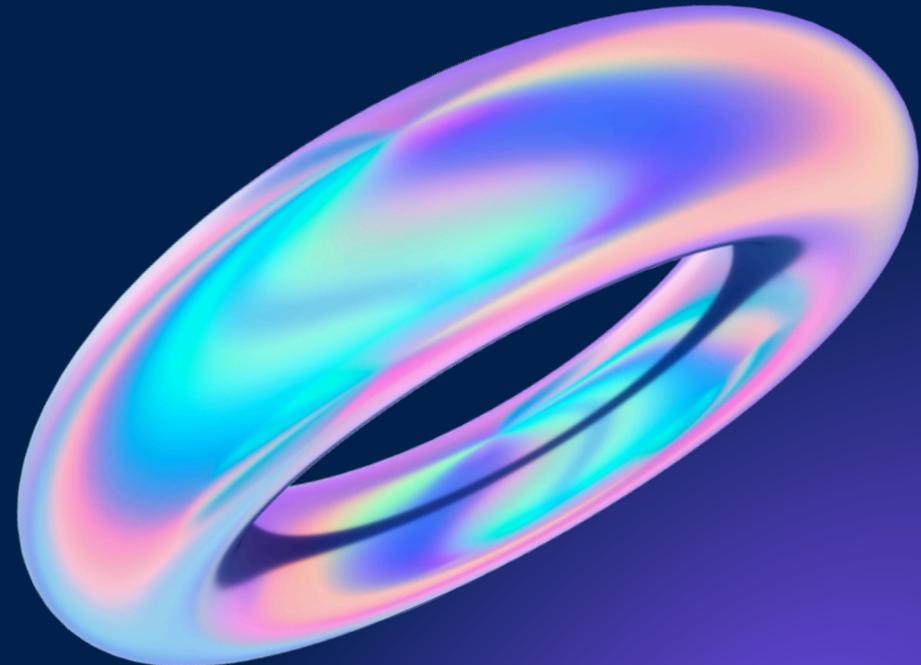




# S10L1

Antonio Perna  
Fabio Nobili



# S10L1

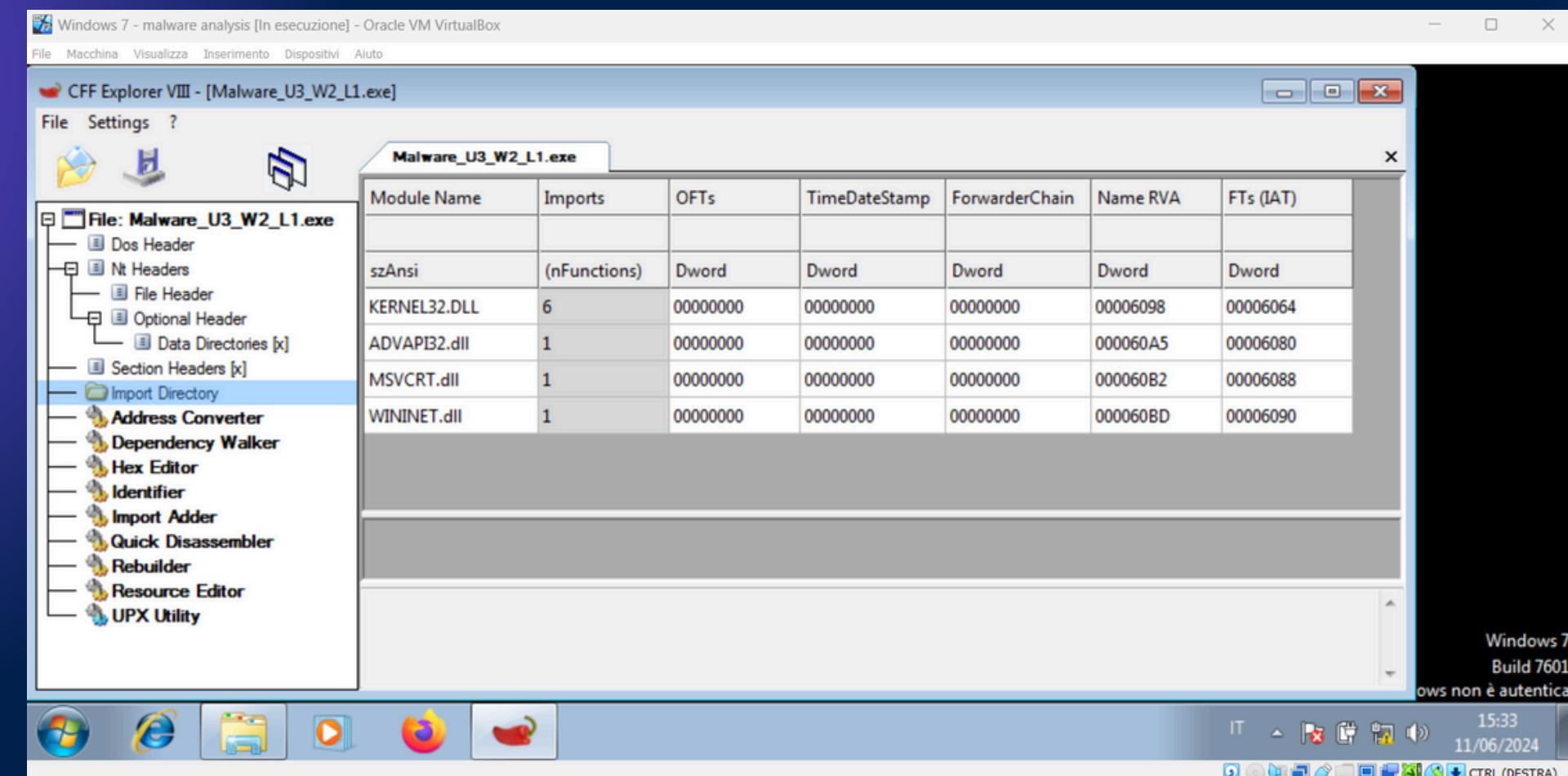
Malware analysis: analisi basica statica

# Cosa fare

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 importate dal malware



Dopo aver aperto il malware dal tool di CFF EXPLORER, dalla sezione “import directory”, vediamo che utilizza 4 librerie:

- KERNEL32.DLL: Creazione di processi per eseguire payload dannosi.
- ADVAPI32.dll: Modifica delle impostazioni di sicurezza o registrazione delle chiavi di registro per la persistenza.
- MSVCRT.dll: Utilizzo delle funzioni di runtime per eseguire codice maligno.
- WININET.dll: Comunicazione con server di comando e controllo (C&C) per scaricare ulteriori componenti del malware o esfiltrare dati.

# Descrizione dettagliata delle librerie

1. **KERNEL32.dll**: Questa libreria contiene funzioni di base del sistema operativo Windows, come la gestione della memoria, operazioni sui file e sui processi, e altre operazioni fondamentali del sistema.

Funzioni comuni includono:

- Creazione e gestione di file e directory.
- Allocazione e gestione della memoria.
- Creazione e terminazione di processi e thread.

2. **ADVAPI32.dll**: Questa libreria fornisce funzioni avanzate per la gestione delle API di Windows, in particolare per la sicurezza e la gestione dei servizi.

Funzioni comuni includono:

- Gestione della sicurezza e dei permessi.
- Manipolazione del registro di sistema.
- Gestione dei servizi di sistema.

3. **MSVCRT.dll**: Questa è la libreria runtime di Microsoft Visual C++, che fornisce le funzioni del runtime del C e del C++. Funzioni comuni includono:

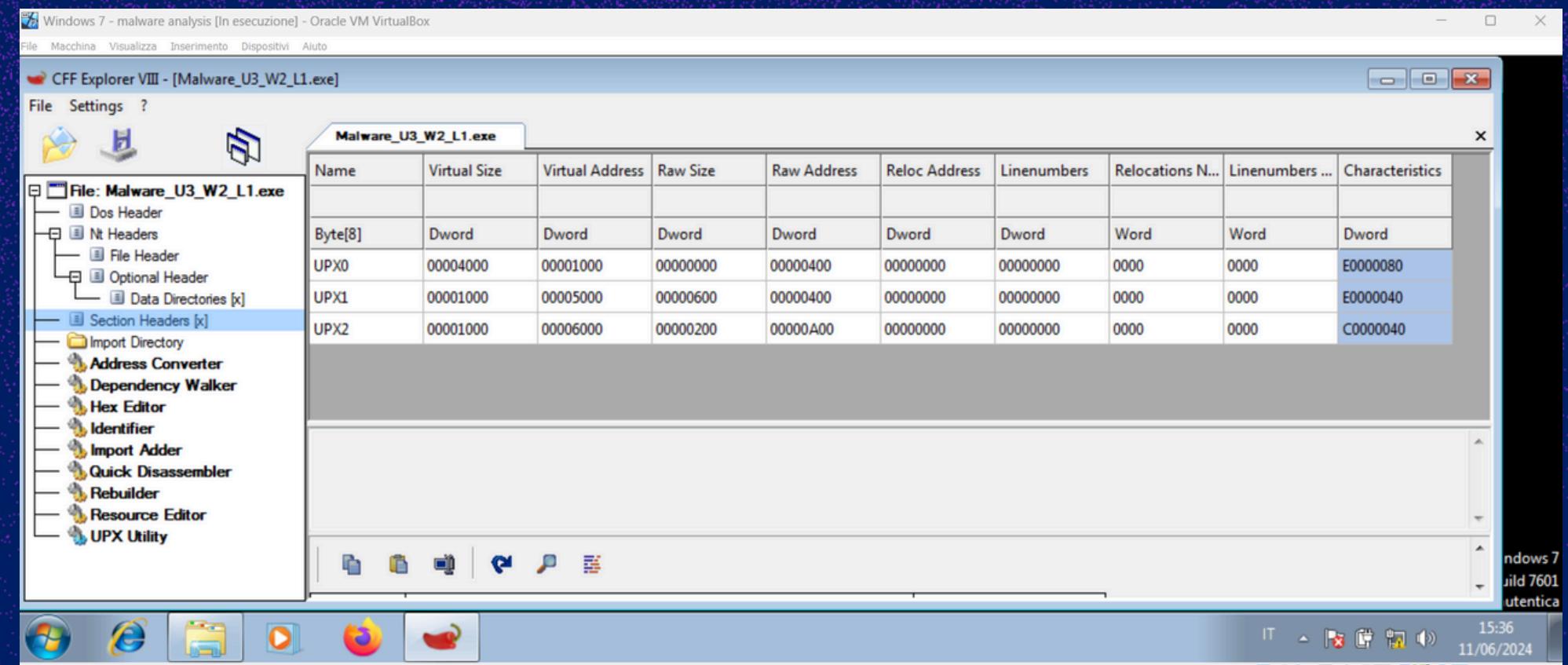
- Funzioni per la gestione delle stringhe.
- Funzioni di input/output (I/O).
- Gestione della memoria dinamica (malloc, free).

4. **WININET.dll**: Questa libreria fornisce funzioni per l'accesso a Internet e per la gestione delle comunicazioni di rete tramite protocolli come HTTP e FTP.

Funzioni comuni includono:

- Connessione a server web.
- Download e upload di file tramite HTTP/FTP.
- Gestione delle sessioni di rete.

# Sezioni malware



L'immagine mostra le intestazioni delle sezioni (Section Headers) di un file eseguibile, specificatamente per "Malware\_U3\_W2\_L1.exe", utilizzando CFF Explorer.

1. UPX0
2. UPX1
3. UPX2

# UPX0

Questa sezione spesso contiene il codice o i dati originali compressi. In questo caso, sembra essere vuota nel file, ma occupa spazio in memoria.

- Virtual Size: 0x00004000 (16 KB) - Dimensione che questa sezione occupa in memoria.
- Virtual Address: 0x00001000 - Indirizzo virtuale dove questa sezione viene caricata in memoria.
- Raw Size: 0x00000000 - Dimensione della sezione nel file sul disco. Valore zero indica che non ha dati nel file.
- Raw Address: 0x00000400 - Offset nel file dove inizia la sezione. In questo caso, non contiene dati, quindi l'offset è irrilevante.
- Characteristics: 0xE0000080 - Attributi della sezione, in questo caso, denota una sezione eseguibile e leggibile.

# UPX1

Questa sezione contiene i dati compressi e l'header UPX, che è responsabile della decompressione in memoria.

- Virtual Size: 0x00001000 (4 KB) - Dimensione in memoria.
- Virtual Address: 0x00005000 - Indirizzo virtuale in memoria.
- Raw Size: 0x00000600 - Dimensione della sezione nel file (1.5 KB).
- Raw Address: 0x00000400 - Offset nel file.
- Characteristics: 0xE0000040 - Attributi della sezione, in questo caso, denota una sezione eseguibile e leggibile.

# UPX2

Questa sezione contiene i dati compressi e l'header UPX, che è responsabile della decompressione in memoria.

- Virtual Size: 0x00001000 (4 KB) - Dimensione in memoria.
- Virtual Address: 0x00006000 - Indirizzo virtuale in memoria.
- Raw Size: 0x00000200 - Dimensione della sezione nel file (512 bytes).
- Raw Address: 0x00000A00 - Offset nel file.
- Characteristics: 0xC0000040 - Attributi della sezione, in questo caso, denota una sezione eseguibile e leggibile.

# Conclusioni

L'analisi preliminare del file "Malware\_U3\_W2\_L1.exe" ha rivelato l'uso di librerie di sistema critiche e la compressione tramite UPX, caratteristiche comuni nei malware. Per comprendere appieno il comportamento e l'intento di questo eseguibile, è fondamentale decomprimere il file e condurre sia analisi statica che dinamica in un ambiente sicuro e controllato. Tuttavia, il malware nasconde il contenuto delle librerie e i nomi dei processi presenti quindi, non è possibile identificare cosa fa di preciso il malware dato che, le librerie verranno eseguite man mano dal processo quando è in esecuzione.