**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.

Prima di tutto è importante fare alcune considerazioni per comprendere meglio l’esecuzione dell’esercizio che stiamo andando a svolgere.

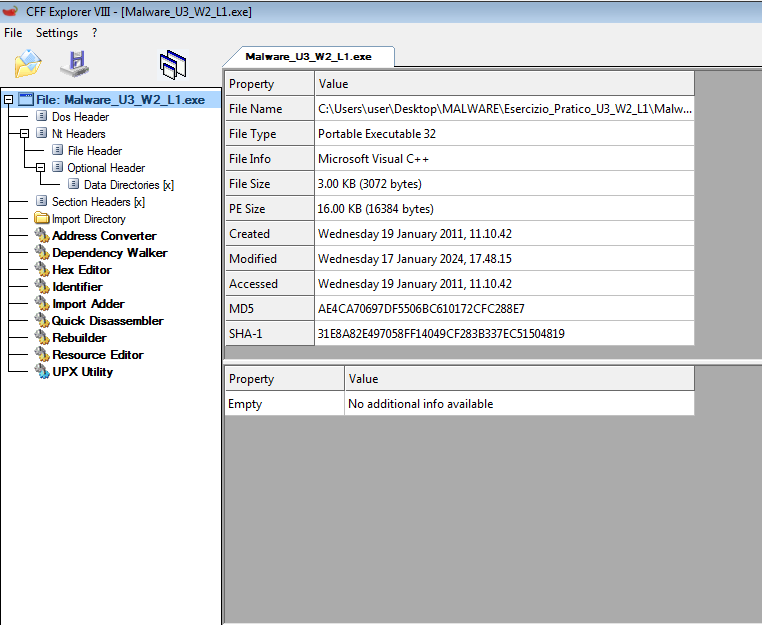
In informatica per **PE** si intende un formato di file eseguibile utilizzato principalmente dal sistema operativo Windows. Questi file sono strutturati in sezioni, ciascuna delle quali contiene dati specifici necessari per l'esecuzione del programma.

Il formato PE è stato progettato per essere "*portabile*", da qui il nome *Portable Executable*, il che significa che i file PE possono essere eseguiti su diverse versioni di Windows senza dover essere ricompilati. Questa portabilità è essenziale per garantire la compatibilità delle applicazioni su diverse versioni del sistema operativo Windows.

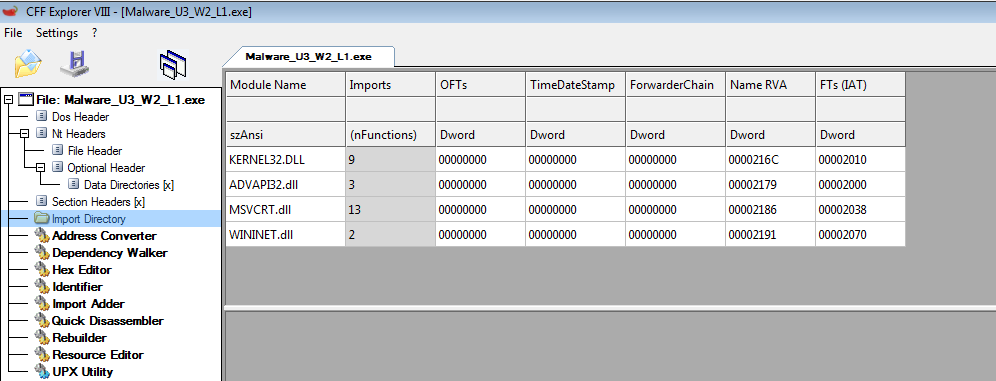
La parte iniziale di un file eseguibile PE viene detto **Header,** ed è proprio qui che sono contenute informazioni essenziali sulla sua struttura e sui dati contenuti al suo interno. Ed è proprio questa parte che sarà utile per il corretto svolgimento del nostro esercizio.

Infatti, attraverso l’applicazione **CFF Explorer,** utilizzata per esplorare e analizzare i file eseguibili di Windows, come file EXE, DLL e altri, potremmo andare ad esaminare la struttura interna dei file binari e comprendere i dettagli di come sono strutturati e come funzionano.

Quindi andiamo sulla nostra macchina Windows 7 su Virtual Box, e apriamo il nostro file con CFF Explorer:



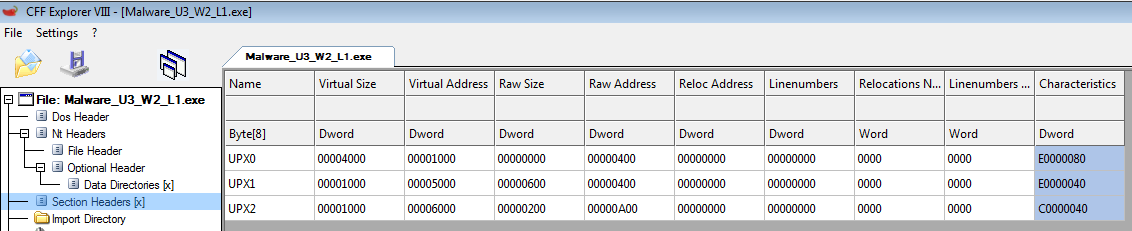
E, andando nella sezione Import Directory del menu a sinistra, rispondiamo alla prima domanda che ci pone l’esercizio, ovvero che tipo di librerie sono importate dal Malware:



Nella tabella risultante possiamo vedere quattro tipi di librerie, analizziamole:

* **KERNEL32.DLL** 🡪 è una delle librerie di sistema principali di Microsoft Windows, fornisce le *funzioni di base necessarie per molte operazioni di sistema e per l'interazione delle applicazioni utente con il sistema operativo*. Le funzioni contenute in questa libreria coprono una vasta gamma di operazioni di sistema, tra cui gestione della memoria, gestione dei file e delle directory, operazioni di input/output, gestione dei processi e dei thread, sincronizzazione, gestione degli errori, e altro ancora;
* **ADVAPI32.dll 🡪** fornisce funzionalità essenziali per la *gestione dei servizi di sistema, la sicurezza, la crittografia e l'accesso al Registro di sistema* su Microsoft Windows;
* **MSVCRT.dll 🡪** contiene funzioni per la *manipolazione stringhe, allocazione memoria e altro come chiamate per input/output*, come nel linguaggio C;
* **WININET.dll 🡪** fornisce *funzionalità per la comunicazione in rete e l'accesso a risorse Internet*. Questa libreria è fondamentale per le applicazioni che necessitano di connettersi a Internet, inviare richieste HTTP, scaricare file da server remoti e altre operazioni di rete.

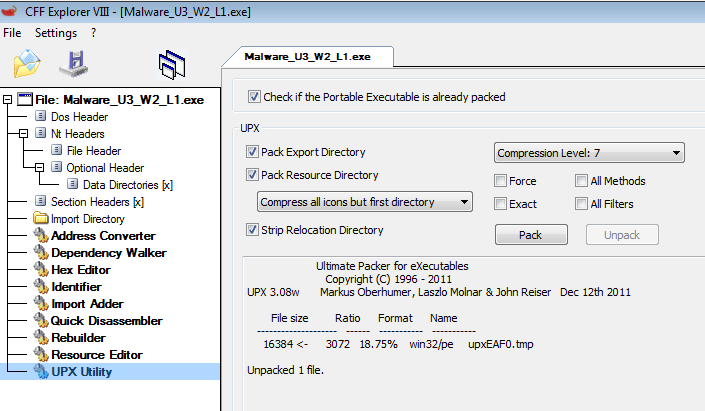
Per rispondere invece al secondo quesito dell’esercizio, dobbiamo andare nella **Section Header** del nostro menu su CFF per vedere le sezioni di cui si compone il malware in analisi:

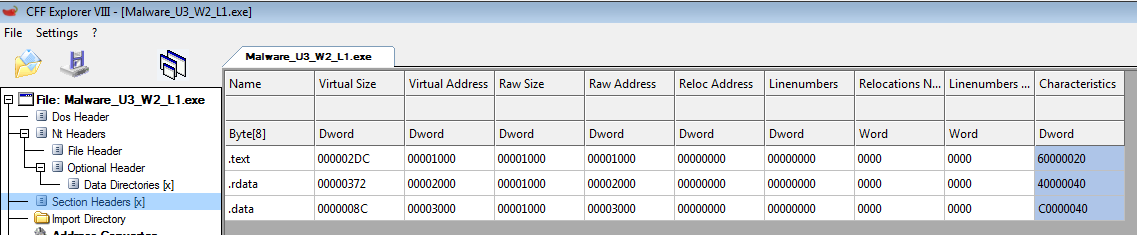


Quando si vede una sezione chiamata "UPX0/1/2", è probabile che il file eseguibile sia stato *compresso* utilizzando UPX (Ultimate Packer for eXecutables), uno strumento di compressione e decompressione per file eseguibili, comunemente utilizzato per ridurre le dimensioni dei file binari senza comprometterne la funzionalità.

Per decomprimere i file torniamo nel nostro menu, selezioniamo **UPX utility** e clicchiamo su *Unpack* e, tornando alla tabella precedente potremmo vedere in chiaro le nostre sezioni del malware

:



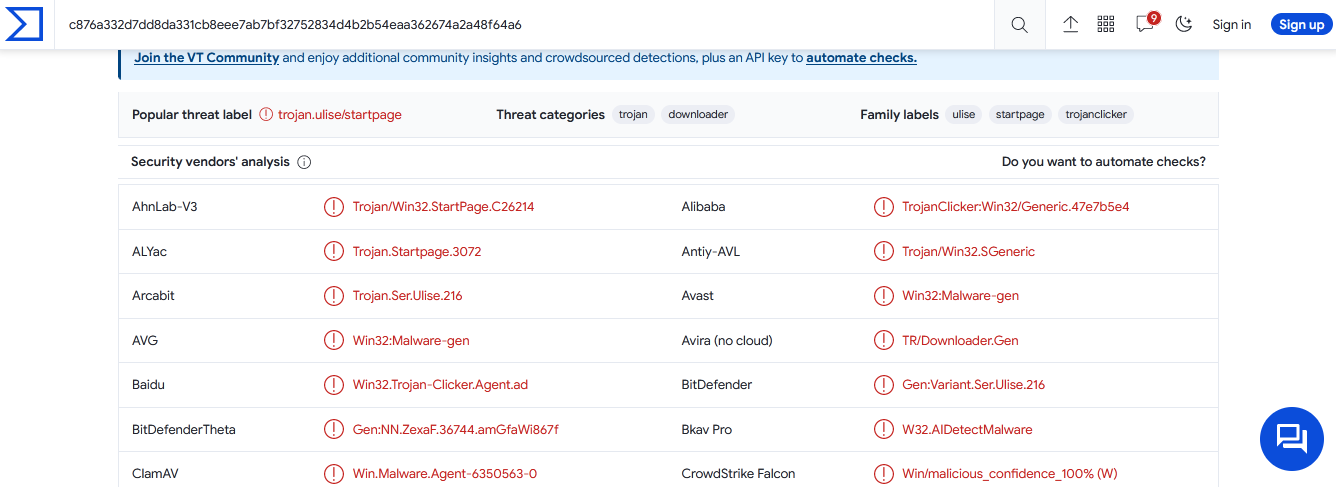


Tre quindi le sezioni di cui si compone il nostro malware. Analiziamole:

1. **.text** 🡪 questa sezione contiene il codice eseguibile del programma, ovvero le istruzioni macchina che vengono eseguite dal processore quando il programma viene avviato;
2. **.rdata** 🡪 include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall’eseguibile; questa sezione contiene principalmente dati "read-only" (sola lettura) per proteggere i dati contenuti al suo interno dall'essere modificati accidentalmente durante l'esecuzione del programma;
3. **.data** 🡪 contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma. Questa sezione contiene variabili globali e dati che possono essere modificati durante l'esecuzione del programma.

In conclusione di tale analisi, per farci un’idea più chiara di che tipo di malware abbiamo tra le mani, possiamo utilizzare uno strumento molto utile che è **VirusTotal,** un servizio online gratuito che fornisce un'analisi antivirus multipla di file e URL per individuare malware e altre minacce informatiche. È utilizzato principalmente da utenti, esperti di sicurezza e ricercatori per verificare la sicurezza di file sospetti o URL potenzialmente dannosi.

Proviamo ad avviare la scansione del nostro file:



A seguito della scansione possiamo renderci conto che abbiamo a che fare con un **Trojan,** un tipo di software malevolo che si presenta come legittimo ma in realtà nasconde funzionalità dannose. I trojan prendono il nome dal cavallo di Troia nella mitologia greca, poiché ingannano gli utenti facendoli apparire come applicazioni o file affidabili, ma in realtà contengono codice malevolo.

Caratteristica subdola dei trojan è che possono assumere molte forme diverse e possono essere utilizzati per una vasta gamma di attacchi informatici. Gli utenti devono essere consapevoli dei rischi associati ai trojan e prendere misure per proteggere i propri dispositivi e dati da tali minacce.

Ciò include l'utilizzo di software antivirus e antimalware aggiornato, l'evitare di scaricare software da fonti non attendibili e l'essere vigili nei confronti di messaggi e-mail o link sospetti.