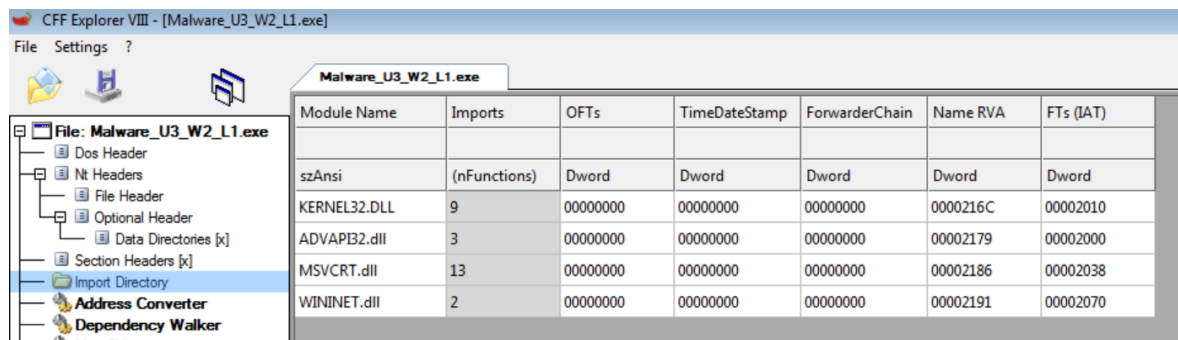


## S10/L1

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

Sulla sezione Import Directory, vediamo le librerie importate dinamicamente:



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	9	00000000	00000000	00000000	0000216C	00002010
ADVAPI32.dll	3	00000000	00000000	00000000	00002179	00002000
MSVCRT.dll	13	00000000	00000000	00000000	00002186	00002038
WININET.dll	2	00000000	00000000	00000000	00002191	00002070

Kernel32.dll → è una libreria di sistema in ambienti operativi Windows. Il suo nome deriva dal fatto che contiene funzioni (DLL, Dynamic Link Library) utilizzate dal kernel del sistema operativo Windows. Questa libreria fornisce una vasta gamma di funzionalità, tra cui gestione dei file, gestione della memoria, gestione dei processi ecc...ed è dunque essenziale per il corretto funzionamento di molti programmi e componenti del sistema operativo Windows.

Advapi32.dll → è un'altra libreria di sistema fondamentale nei sistemi operativi Windows. Questa libreria fornisce una vasta gamma di funzionalità per la gestione della sicurezza e la gestione degli account utente. Alcune delle funzioni principali di Advapi32.dll includono l'accesso al Registro di sistema, la gestione dei servizi di Windows, la crittografia dei dati, l'autenticazione e l'autorizzazione degli utenti, nonché la gestione dei token di sicurezza. È utilizzato da molti programmi e componenti del sistema operativo Windows per garantire la sicurezza e il corretto funzionamento del sistema.

Msvcrt.dll → è una libreria di sistema di Microsoft utilizzata principalmente per fornire funzionalità di runtime della libreria di esecuzione di Microsoft C. Le funzionalità offerte da msvcrt.dll includono operazioni di gestione dei file, gestione della memoria, operazioni matematiche, operazioni di stringa e altro ancora.

Wininet.dll → è una libreria di sistema di Microsoft utilizzata per fornire funzionalità di connettività di rete e accesso a Internet nei sistemi operativi Windows. Questa DLL offre un'ampia gamma di funzioni per l'accesso e la gestione di risorse su Internet, è ampiamente utilizzata da applicazioni Windows che richiedono connettività di rete, come browser web, client di posta elettronica, applicazioni di download e molti altri programmi che interagiscono con risorse su Internet. È una parte fondamentale del supporto di rete nel sistema operativo Windows.

Vediamo ora le sezioni di un file eseguibile, spesso associate ai file eseguibili nei sistemi operativi come Windows (in formato PE, Portable Executable), le quali sono aree di memoria organizzate all'interno del file che contengono diverse tipologie di dati e istruzioni necessarie per il funzionamento del programma.

Vediamo quali vi sono nella sezione "section headers": noteremo che sono in formato UPX (Ultimate Packer for eXecutables), ovvero uno strumento di compressione e decompressione per file eseguibili, progettato per ridurre le dimensioni dei file eseguibili senza compromettere la loro funzionalità.

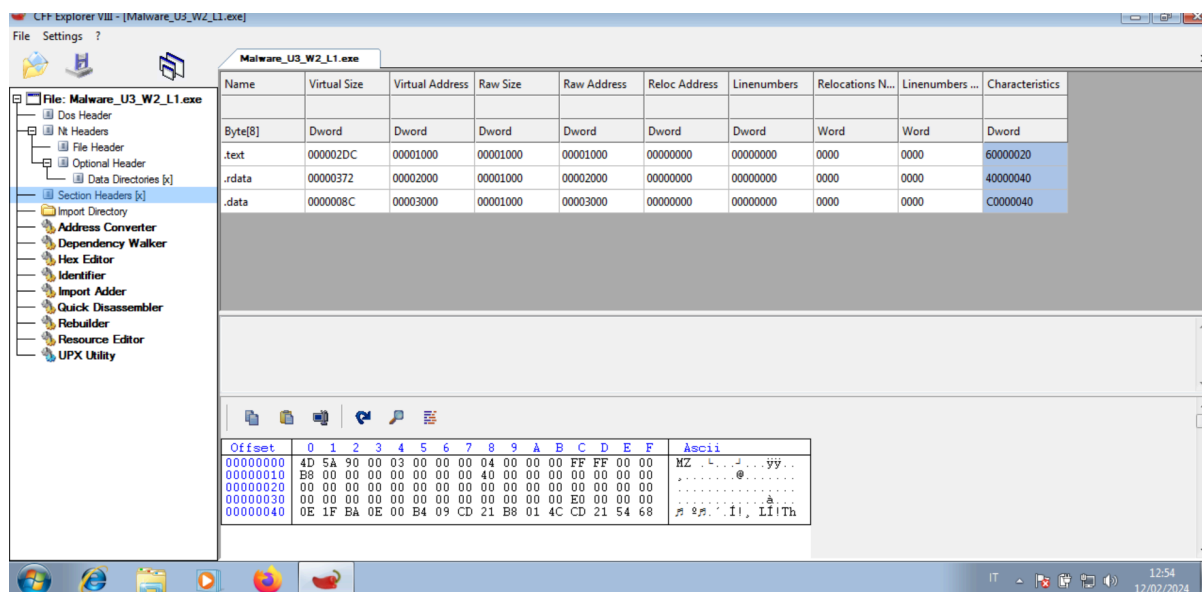
Una volta decompressi vedremo le seguenti sezioni:

```
Directory di C:\Users\user\Desktop\upx-4.2.2-win64
12/02/2024 14:49 <DIR> .
12/02/2024 14:49 <DIR> ..
12/02/2024 14:49      18.092 COPYING
12/02/2024 14:49       5.448 LICENSE
12/02/2024 14:49     24.953 NEWS
12/02/2024 14:49       3.728 README
12/02/2024 14:49       2.230 THANKS.txt
12/02/2024 14:49     38.689 upx-doc.html
12/02/2024 14:49     37.296 upx-doc.txt
12/02/2024 14:49     43.267 upx.1
12/02/2024 14:49     563.712 upx.exe
          9 File      737.415 byte
          2 Directory 22.851.297.280 byte disponibili

C:\Users\user\Desktop\upx-4.2.2-win64>upx -d \Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe
      Ultimate Packer for eXecutables
      Copyright (C) 1996 - 2024
UPX 4.2.2      Markus Oberhumer, Laszlo Molnar & John Reiser      Jan 3rd 2024

-----
File size      Ratio      Format      Name
-----
16384 <-      3072      18.75%      win32/pe      Malware_U3_W2_L1.exe

Unpacked 1 file.
```

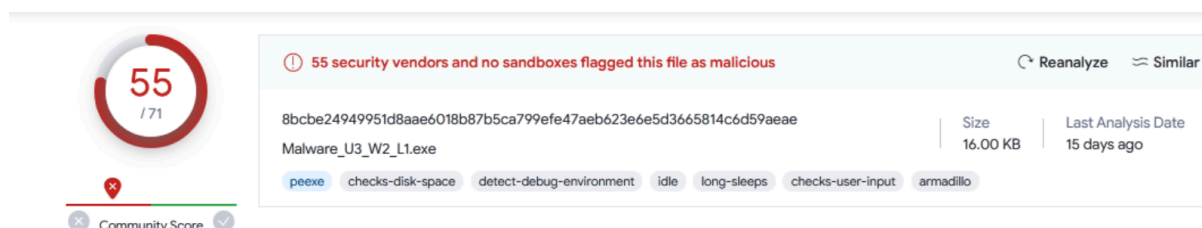


**.TEXT** → La sezione di un file PE (Portable Executable) denominata ".text" è una delle sezioni più importanti e comuni all'interno di un'eseguibile o di una DLL in ambiente Windows. Questa sezione contiene il codice eseguibile del programma, ovvero le istruzioni che vengono eseguite dalla CPU quando il programma viene avviato.

**.RDATA** → La sezione di un file PE (Portable Executable) denominata ".rdata" contiene dati di sola lettura che sono incorporati direttamente nel file eseguibile o nella DLL. Questi dati sono accessibili durante l'esecuzione del programma, ma non possono essere modificati dall'applicazione stessa. I dati presenti nella sezione ".rdata" possono includere costanti, stringhe, tabelle e altre informazioni statiche utilizzate dal programma durante l'esecuzione.

**.DATA** → La sezione di un file PE denominata ".data" contiene dati variabili utilizzati durante l'esecuzione del programma. Questi dati possono essere letti e scritti dall'applicazione durante l'esecuzione, e dunque modificati durante l'esecuzione del programma e accessibili da diverse parti del codice.

Per capire se effettivamente è un malware, carichiamo il file su Virus Total (servizio online che fornisce un'ampia gamma di strumenti per l'analisi dei file e delle URL alla ricerca di malware e altre minacce informatiche), per avviare una scansione antivirus multipla.



Notiamo subito dei parametri quali:

- check-disk-space → verifica dello spazio sul disco
- detect-debug-environment → è una funzione o un'istruzione di programmazione utilizzata per identificare se un programma è in esecuzione all'interno di un ambiente di debug o di un debugger.
- idle → si riferisce allo stato del file una volta che il processo di scansione è stato completato. In altre parole, indica che il file è inattivo o non sta eseguendo alcuna azione particolare all'interno dell'ambiente di analisi di VirusTotal.
- long-sleeps → come indicatore di comportamento all'interno di VirusTotal si riferisce a un comportamento del file analizzato che coinvolge periodi di inattività prolungata durante l'esecuzione. In questo contesto, "sleep" si riferisce a un'istruzione di programmazione che fa sospendere temporaneamente l'esecuzione del processo per un certo periodo di tempo specificato.
- check-user-input → potrebbe riferirsi a una funzionalità del file analizzato che coinvolge il controllo o la manipolazione di input forniti dall'utente. In genere, questa funzionalità potrebbe essere sfruttata da malware per intercettare, modificare o raccogliere informazioni inserite dall'utente all'interno di un'applicazione o di un sistema.

 Trojan/Win32.StartPage.C26214

Possiamo dunque ipotizzare che il malware è un Trojan Horse, un tipo di malware che si presenta come un'applicazione legittima o affidabile, ma che in realtà nasconde funzionalità dannose o malevole all'interno del suo codice causando danni ai dati, al sistema o all'utente.

Considerando le librerie e le sezioni coinvolte, il malware in questo caso potrebbe:

- Rubare informazioni sensibili: Utilizzando le funzionalità di rete (libreria wininet.dll), il Trojan potrebbe essere in grado di inviare dati rubati (come username, password, informazioni bancarie) a un server remoto controllato dall'attaccante.
- Backdoor e accesso remoto: Utilizzando le funzionalità di rete offerte dalle librerie, il Trojan potrebbe stabilire una backdoor nel sistema dell'utente, consentendo agli attaccanti di ottenere accesso remoto al sistema per eseguire ulteriori attività dannose.
- Potrebbe inoltre installare altri malware, sul sistema dell'utente.
- Infine, tramite l'indicatore di comportamento check-user-input, il malware potrebbe intercettare e raccogliere informazioni sensibili inserite dall'utente, come password, dati finanziari ecc...; manipolare le azioni dell'utente, ad esempio reindirizzando a pagine web malevole o inserendo informazioni errate; può iniettare codice malevolo all'interno di input forniti dall'utente, ad esempio per eseguire attacchi di tipo "injection" come SQL injection o cross-site scripting (XSS).