

Analisi Statica Basica

Traccia

Analizzando il file Malware_U3_W2_L1 facciamo le seguenti considerazioni:

- 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

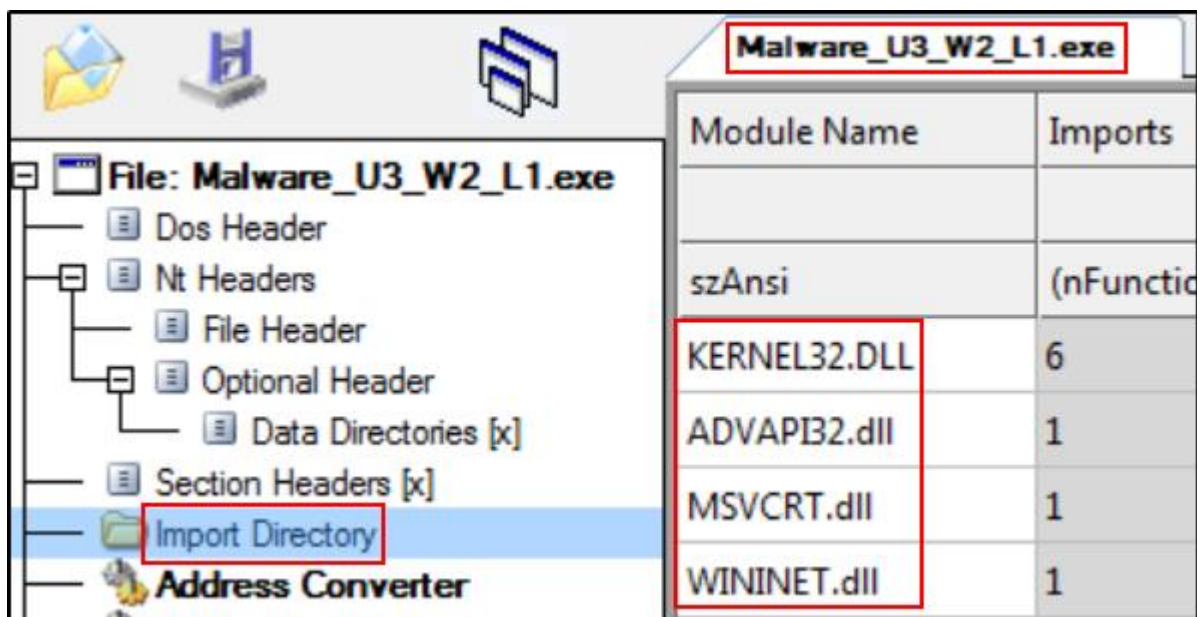
Le librerie importate dal Malware sono le seguenti:

KERNEL32.DLL Contiene funzioni per interagire col sistema operativo, come gestione dei file, memoria, processi, thread e errori.

ADVAPI32.dll Contiene funzioni per interagire con servizi, registri di sistema, account utente, e crittografia.

MSVCRT.dll Contiene funzioni per la gestione delle stringhe, allocazione memoria, Input/Output e conversione di tipi di dati.

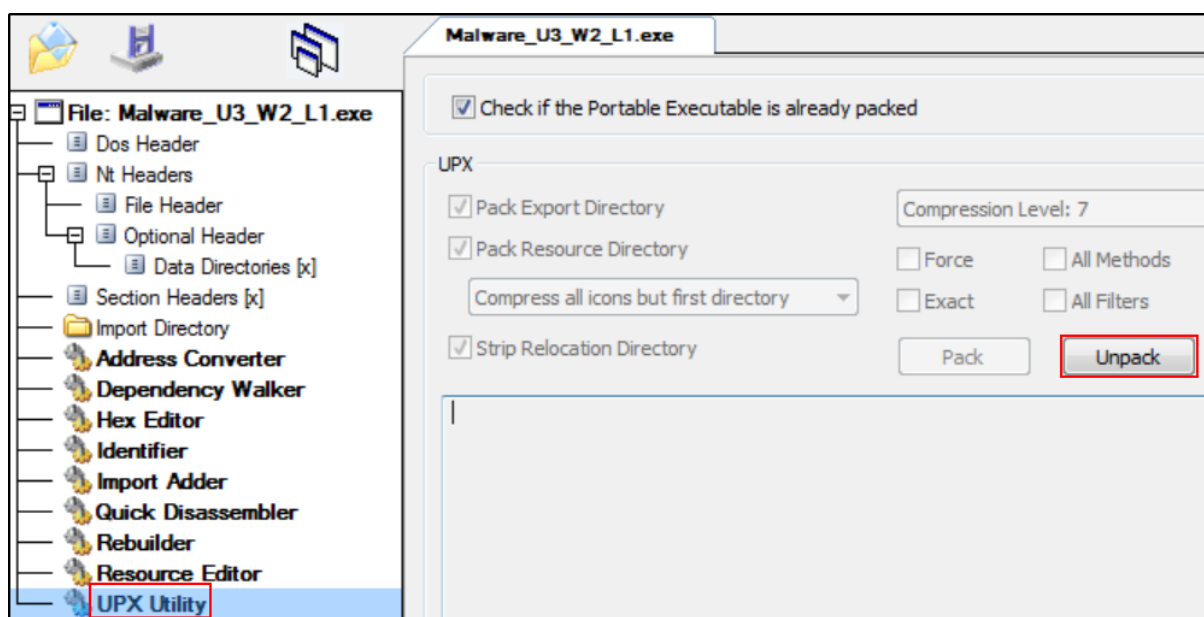
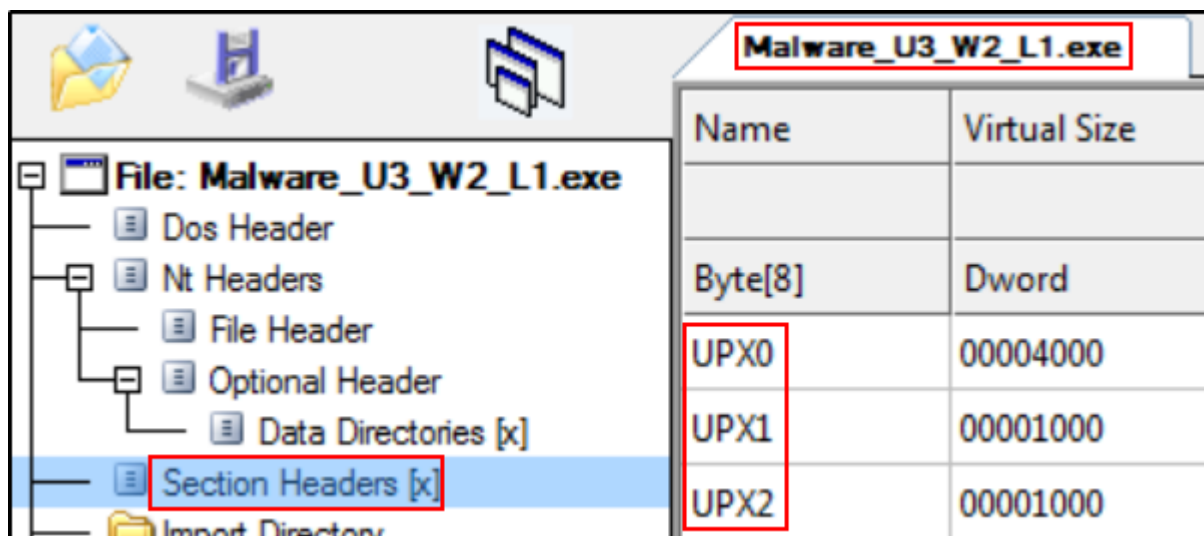
WININET.dll Contiene funzioni per l'accesso a internet, protocolli di rete, cookie e certificati di sicurezza.



Module Name	Imports
szAnsi	(nFunction
KERNEL32.DLL	6
ADVAPI32.dll	1
MSVCRT.dll	1
WININET.dll	1

Sezioni

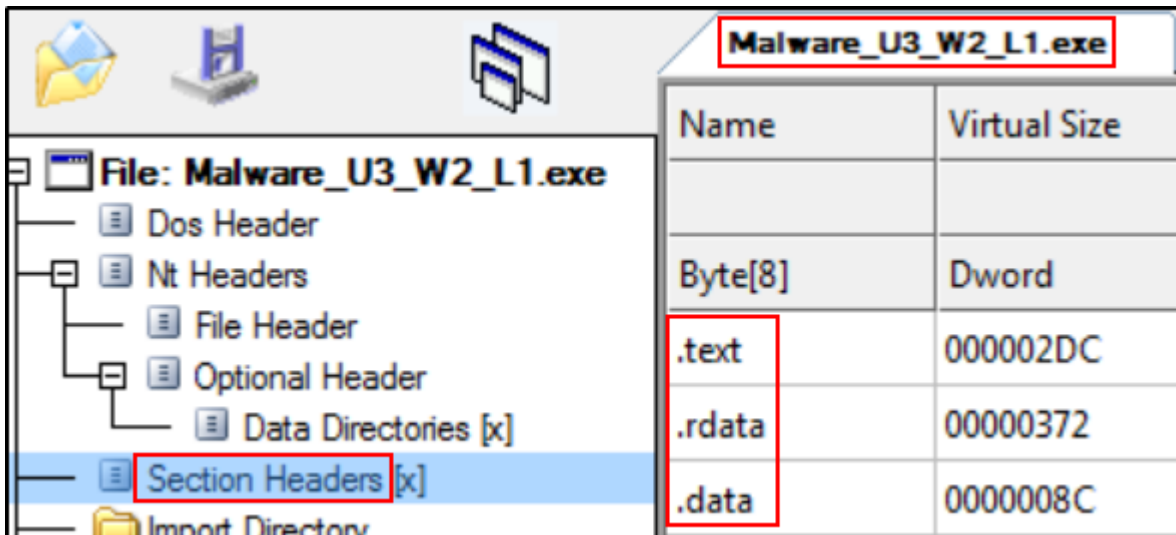
Inizialmente le sezioni sono comprese in formato UPX (Ultimate Packer for eXecutables), andiamo quindi a decompprimerle con l'opzione Unpack dell'UPX Utility



.text E' una sezione critica perchè contiene informazioni fondamentali sulle azioni del codice eseguibile in questione ed è l'unica che viene eseguita dalla CPU mentre le altre sezioni contengono dati o informazioni a supporto

.rdata Sta per Read-Only Data e svolge un ruolo simile a .data ma a differenza di quest'ultima contiene dati costanti o destinati alla sola lettura

.data Contiene dati/variabili globali e viene usata per capire meglio come un programma gestisce le informazioni dinamiche



Name	Virtual Size
Byte[8]	Dword
.text	000002DC
.rdata	00000372
.data	0000008C

Considerazione Finale

Avendo librerie che lavorano a livello Kernel, che possono manipolare account utente, che coinvolgono operazioni di input/output ed effettuato operazioni di rete possiamo ipotizzare che il Malware in questione cerca di stabilirsi in maniera persistente nel sistema operativo, cerca di ottenere privilegi utente elevati, ruba o modifica informazioni presenti nel dispositivo e cerca di stabilire una connessione con l'esterno, possibilmente una shell per permettere all'attaccante di eseguire comandi da remoto.

Potrebbe quindi trattarsi di un Trojan.