

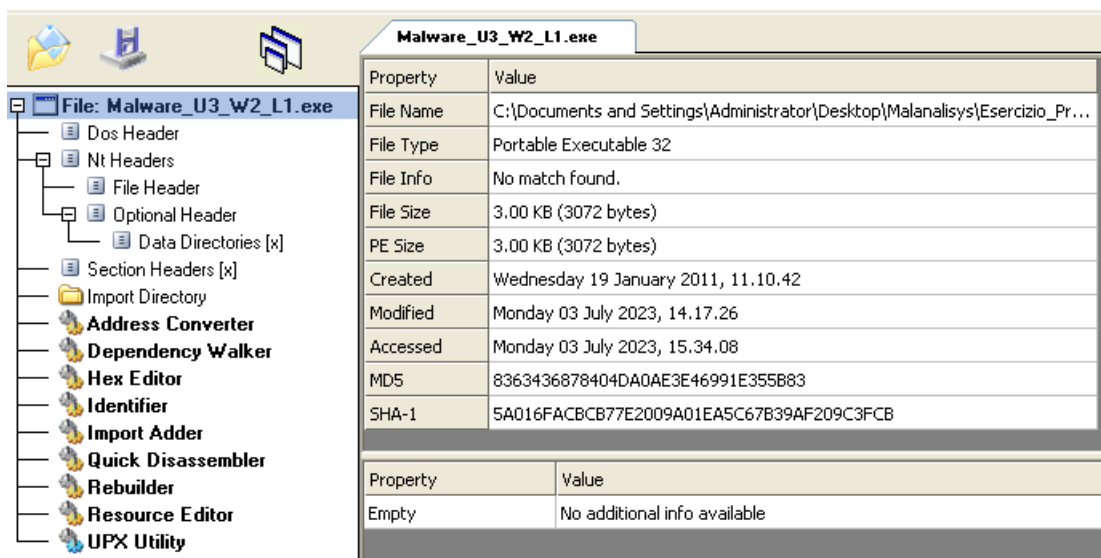
Malware Analysis

Per raccogliere informazioni sul malware: **Malware_U3_W2_L1.exe**, eseguo il programma **CFF Explorer**. CFF Explorer è un software utilizzato per l'analisi e la modifica di file eseguibili, ed è utile per gli sviluppatori e gli appassionati di reverse engineering. Permette di esaminare la struttura interna del file, modificare sezioni, risorse e importazioni/esportazioni.

L'esercizio è svolto su macchina virtuale xp.

Avvio il programma ed eseguo la scansione del file: **Malware_U3_W2_L1.exe**:

la schermata principale ci restituisce le info del file, come grandezza, data di creazione, data modifica ed accessi, hash MD5 e SHA-1, oltre al tipo del file.



Nel menù a sinistra troviamo varie opzioni tra cui:

Dos Header: L'intestazione DOS è la prima parte di un file eseguibile che contiene informazioni specifiche per il sistema operativo DOS. Contiene, ad esempio, l'indirizzo di avvio del programma e altre informazioni legate alla compatibilità con il sistema operativo DOS.

Nt Headers: L'intestazione NT fa parte della struttura di file eseguibile PE (Portable Executable) utilizzata dai sistemi operativi Windows. Contiene informazioni come la versione del sistema operativo di destinazione, le caratteristiche del file, l'entry point del programma e altre informazioni necessarie per l'esecuzione del file.

Section Headers: Le sezioni sono divisioni logiche di un file eseguibile. Gli header delle sezioni contengono informazioni su ciascuna sezione del file, come il nome della sezione, la posizione in memoria, le dimensioni, gli attributi di protezione e altre informazioni correlate. Le sezioni possono contenere codice eseguibile, dati, risorse, tabelle di importazione/esportazione e altro ancora.

Import Directory: La directory delle importazioni indica quali funzioni o librerie esterne sono utilizzate dal file eseguibile. Contiene informazioni su quali librerie dinamiche (DLL) o funzioni specifiche devono essere caricate durante l'esecuzione del programma. Questa directory elenca i nomi delle librerie e delle funzioni importate, nonché i puntatori alle posizioni di memoria corrispondenti.

Le librerie presenti nel file exe sono:

Malware_U3_W2_L1.exe						
Module Name	Imports	OFs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

Kernel32.DLL: contiene le funzioni principali per interagire con il sistema operativo come la manipolazione dei file, gestione di memoria. In questo caso vengono importate sei funzioni:

LoadLibraryA: Carica una libreria dinamica nel processo corrente.

GetProcAddress: Restituisce l'indirizzo di una funzione in una libreria dinamica.

VirtualProtect: Modifica i permessi di accesso di una pagina di memoria.

VirtualAlloc: Alloca memoria virtuale per un processo.

VirtualFree: Libera la memoria virtuale allocata da VirtualAlloc.

ExitProcess: Termina il processo corrente.

ADvapi32.dll: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft. In questo caso viene importata una funzione:

CreateServiceA: Crea un nuovo servizio nel sistema operativo Windows.

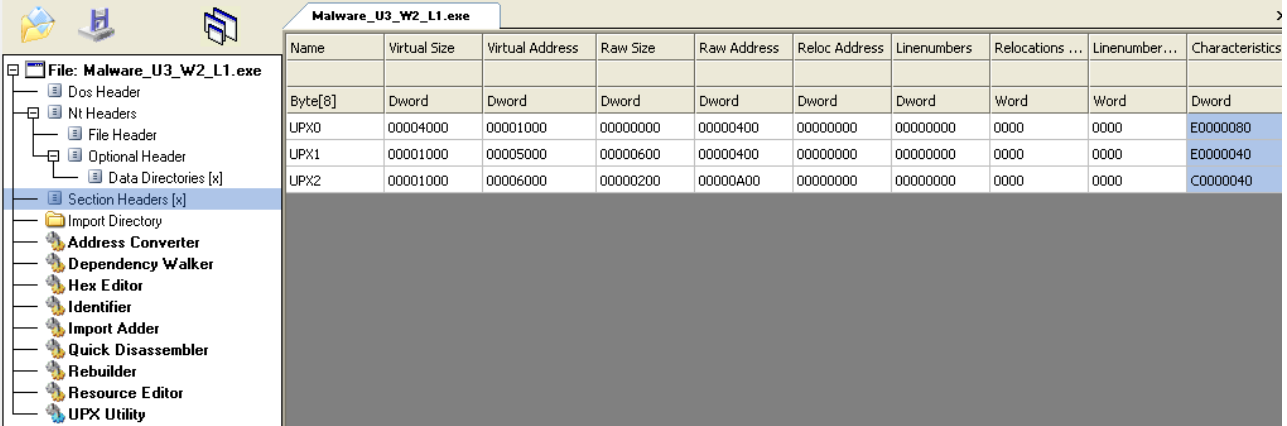
MSVCRT.DLL: contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C. In questo caso viene importata una funzione:

exit: termina il programma corrente.

Winnet.DLL: fornisce funzioni e servizi di rete per il sistema operativo Windows, come la gestione della connessione di rete, l'accesso ai protocolli di rete e la gestione dei socket. In questo caso viene importata una funzione:

InternetOpenA: Apre una nuova connessione.

Ora vado a vedere le sezioni in “section Headers”, vado a fare una ricerca sugli UPX e vedo che è un sistema che comprime i file. Mi dirigo su UPX Utility e spacchetto.



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

Così facendo mi compaiono i nomi delle sezioni.

Malware_U3_W2_L1.exe									
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
000001D8	000001E0	000001E4	000001E8	000001EC	000001F0	000001F4	000001F8	000001FA	000001FC
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000002DC	00001000	00001000	00001000	00000000	00000000	0000	0000	60000020
.rdata	00000372	00002000	00001000	00002000	00000000	00000000	0000	0000	40000040
.data	0000008C	00003000	00001000	00003000	00000000	00000000	0000	0000	C0000040

.text: contiene le istruzioni (righe di codice) che la CPU eseguirà una volta che il software sarà avviato.

.rdata: include le informazioni circa le librerie e le funzioni importate ed esportate dall’eseguibile, informazioni che abbiamo appena visto.

.data: contiene tipicamente i dati /le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

Dalle info ottenute, posso ipotizzare che l’eseguibile è un trojan (come suggerito anche da Virustotal), e visto che c’è l’importazione della libreria Winnet.dll posso ipotizzare che c’è un server in ascolto che fa da connessione remota, quindi possibile backdoor o spyware.