## Malware analysis

Richiesta: Dato il malware nella VM windows 7, analizzate il contenuto attraverso CFF explorer.

Rispondere ai seguenti quesiti:

- 1. Indicare le librerie importate dal malware, descrivendole.
- 2. Indicare le sezioni di cui si compone il malware, descrivendole.
- 3. Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte.

## Librerie

Utilizzando CFF explorer, ho riscontrato le seguenti librerie:

Malware_U3_W2_L1.exe X					
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5
MSVCRT.dll	1	00000000	00000000	00000000	000060B2
WININET.dll	1	00000000	00000000	00000000	000060BD
1					

KERNEL32.DLL: Una delle librerie fondamentali di Windows. Fornisce funzioni di base per la gestione della memoria, la creazione e la gestione dei processi e dei thread, e altre funzioni del sistema operativo.

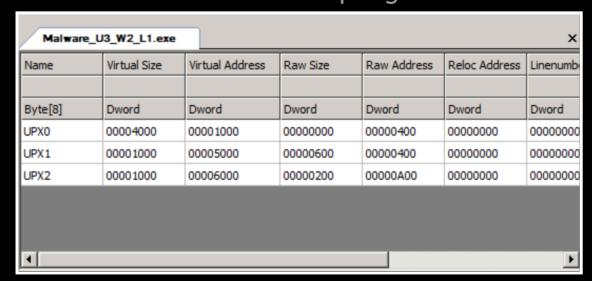
ADVAPI32.dll: Contiene API avanzate di windows, importati per interagire con i servizi e i registri del sistema operativo.

MSVCRT.dll: Microsoft Visual C Runtime Library, una libreria che fornisce funzioni standard di C come la gestione delle stringhe, matematica, input/output di file, etc.

WININET.dll: Libreria che gestisce funzioni relative ad internet, Fornisce API per la comunicazione con protocolli FTP, HTTP, NTP.

## Sezioni

Individuiamo le sezioni compongono il malware:



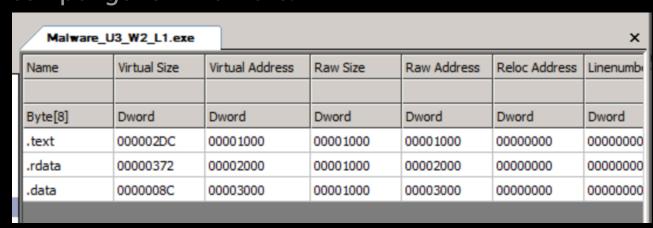
Definiamo UPX: Ultimate Packer for eXecutables, si tratta di un packer (strumento che comprime/cripta un file.exe) utilizzato per alleggerire il peso del file attraverso la compressione. Questa tecnica è utilizzata per renderne più difficile l'analisi e bypassare un possibile antivirus.

Le sezioni riportate da CFF explorer sono:

- 1. UPX0: Potrebbe essere una sezione che è stata svuotata e non contiene dati (come indicato dalla dimensione raw di 0), riservata per l'espansione durante la decompressione in memoria.
- 2. UPX1: Questa sezione potrebbe contenere il codice compresso del programma.
- 3. UPX2: Potrebbe contenere dati o codice aggiuntivo necessario per il funzionamento del programma una volta decompresso.

Queste sezioni vengono solitamente create automaticamente dal packer UPX quando comprime l'eseguibile e non sono tipicamente presenti in file non compressi.

Una volta decompresso il file, possiamo osservare le reali sezioni che compongono il malware:



.text: Questa sezione contiene il codice eseguibile del programma. Qui risiedono le istruzioni che eseguirà la CPU al momento dell'esecuzione.

.rdata: La sezione "Read Data", contiene informazioni riguardanti le librerie e le funzioni importate ed esportate dall'exe.

.data: Questa sezione contiene dati inizializzati, il che significa variabili globali e statiche che sono inizializzate dal programmatore.

Queste riportate sono le reali sezioni che compongono l'eseguibile.

## **Considerazione finale**

Sulla base delle informazioni ricavate attraverso il tool CFF explorer, riporto le seguenti deduzioni:

- 1. Comportamento all'Esecuzione: Dato che il malware era compresso con UPX, l'intento potrebbe essere stato quello di nascondere il vero scopo del codice e ridurre la dimensione del file per facilitarne la distribuzione.
- 2. Sezioni Standard: Le sezioni .text, .rdata e .data suggeriscono che il malware ha una struttura convenzionale, con codice eseguibile, dati di sola lettura e dati modificabili.
- 3. Obiettivi del Malware: Basandoci sulle librerie importate, il malware sembra avere la capacità di interfacciarsi con funzioni di sistema essenziali, modificare il registro di sistema, eseguire operazioni di rete, e possibilmente manipolare processi e thread.

I malware possono utilizzare i thread per eseguire compiti in background, come connessioni di rete, senza interrompere il flusso principale del programma, rendendo l'attività malevola meno rilevabile.