## ESERCIZIO 1 SETTIMANA 10

Dopo aver importaro il malware su CFF Explorer controlliamo quali librerie vengono importate:

| 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 |

In questo caso le librerie che vengono importate sono:

- **Kernel32.dll**: contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.
- **Advapi32.dll**: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo.
- **MSVCRT.dll**: contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C.
- **Wininet.dll**: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Dobbiamo anche capire di quali sezioni è composto il malware. Ci spostiamo quindi nella finestra Section Headers.

| Name | Virtual Size | Virtual Address | Raw Size | Raw Address | Reloc Address | Linenumbers | Relocations N... | Linenumbers ... | Characteristics |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| 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 |

Questo Malware è composto dalle seguenti sezioni:

- .text: contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto.

- .rdata: include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer.
- .data: contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma. Una variabile si dice globale quando non è definita all'interno di un contesto di una funzione, ma bensì è globalmente dichiarata ed è di conseguenza accessibile da qualsiasi funzione all'interno dell'eseguibile.

## Considerazioni finali

Questo malware sembra progettato per interagire direttamente con il sistema operativo e per svolgere varie operazioni come manipolazione dai file, gestione della memoria.