ANALISI STATICA BASICA

I **Malware**(malicious software) includono una vasta gamma di programmi scritti per arrecare danno a sistemi informativi, spesso a scopo di lucro.

**L’analisi statica** è lo studio di malware senza eseguirli(controllo le componenti di “com’è fatto”)

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

Per analizzare il malware all’interno della sua cartella è stato utilizzato il programma CFF explorer che consente di analizzare il malware in maniera passiva. Come vediamo successivamente una volta scelto il file da importare andiamo sulla voce import directory, e ci mostrerà le librerie utilizzate dal programma

A screenshot of a computer

Description automatically generated

Le librerie utilizzate dal malware sono le seguenti:

**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.

Accanto a ogni libreria abbiamo un numero, che equivale alle funzioni che possiede tale libreria

**SECTION HEADERS** (una parte del file che fornisce informazioni su ciascuna sezione all’interno del file)

**Virtual size** = dimensione sezione in memoria virtuale (ram)

**Raw size** = dimensione sezione file eseguibile (hard disk)

A screenshot of a computer

Description automatically generated

Per ottenere altre info all’interno del file è necessario spacchettare il file che eseguirà in ordine sequenziale (esempi di file trovati .tex .data .rsc)

**.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

**.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.

**.rsrc**: include le risorse utilizzate dall’eseguibile come ad esempio icone, immagini, menu e stringhe che non sono parte dell’eseguibile stesso.

Considerazioni finali:

Queste informazioni indicano che il file è un'applicazione Windows a 32 bit con un'estensione .exe. Le dimensioni virtuali e raw del file sono relativamente piccole, il che suggerisce che il malware è relativamente semplice. L'assenza di linee di codice indica che il malware è stato compresso