**Report S10 L1**

**Analisi Statica Basica**

**Traccia:**

Con riferimento al file eseguibile contenuto nella cartella «Esercizio\_Pratico\_U3\_W2\_L1» presente sul desktop della vostra macchina virtuale dedicata all’analisi dei malware, rispondere ai seguenti quesiti:

1. Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse
2. Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa
3. Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

Come richiesto dall’esercizio, andiamo ad analizzare le librerie e le funzioni che vengono importate con questo Malware, per fare ciò utilizziamo CFF Explorer, un tool che ci permette di controllare librerie e funzioni che ogni malware o programma importa quando eseguito:

Immagine che contiene testo, schermata, schermo, software

Descrizione generata automaticamente

Le librerie che vengono importate quindi sono:

Kernel32.dll : Libreria piuttosto comune che contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.

Advapi32.dll : Libreria che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft.

Wininet.dll: Libreria che contiene le funzioni per l’implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

MSVCRT.dll: Libreria che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output in stile linguaggio C.

A questo punto, utilizzando lo stesso tool possiamo procedere con l’analisi delle sezioni di cui si compone il malware.

Immagine che contiene testo, elettronica, schermata, schermo

Descrizione generata automaticamente

Le sezioni riportate sono state compresse utilizzando il tool UPX, tale tool comprime gli eseguibili rendendo inaccessibile il formato PE della sezione.   
Per decomprimere il formato PE, possiamo recarci dal menù a sinistra nella scheda “UPX Utility” e clicchiamo su “Unpack”.  
Immagine che contiene testo, schermata, software, Icona del computer

Descrizione generata automaticamente

Successivamente dovrebbe apparire una schermata del genere.

Immagine che contiene testo, schermata, software, schermo

Descrizione generata automaticamente

A questo punto, recandoci nuovamente sulla scheda “Section Headers” possiamo analizzare ogni singola sezione.

Immagine che contiene testo, schermata, software, numero

Descrizione generata automaticamente

I formati che abbiamo rilevato sono:

.text: La sezione «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: La sezione «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. (modificato)

.data: La sezione «data» contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma. Ricordate che 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 dell’eseguibile.

A questo punto, analizzando singolarmente ogni sezione, ci rendiamo conto che la sezione .text e .rdata sono crittate e indecifrabili senza l’ausilio di altri tool, tuttavia abbiamo scoperto tramite l’analisi della sezione .data che il malware si connette, dopo aver creato un servizio “MalService HGL345”, all’url http://www.malwareanalysisbook.com utilizzando internet explorer alla versione 8.0 come tramite.

Immagine che contiene testo, elettronica, schermata, schermo

Descrizione generata automaticamente

Immagine che contiene testo, elettronica, schermata, schermo

Descrizione generata automaticamente

Con le nostre conoscenze attuali non ci è possibile analizzare cosa il servizio creato fa.