EPICODE

Esercizio S10 – L1

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:  
• 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.

SOLUZIONE

Per svolgere l’esercizio si è scelto di utilizzare CFF Explorer, un programma di analisi file eseguibili Windows.

Una volta aperto è possibile caricare il malware che si vuole analizzare.

Nell’immagine sottostante è possibile vedere le librerie utilizzate dal malware. È sufficiente cliccare su “Import Directory”. Nell’immagine si può notare che il malware ha importato 4 librerie comuni. Nell’immagine è possibile notare anche il numero di funzioni per ogni libreria.

Immagine che contiene testo, schermata, software, schermo

Descrizione generata automaticamente

Spiegazione librerie:

- KERNEL32.DLL è un componente essenziale del sistema operativo Windows. Gioca un ruolo fondamentale nella gestione della memoria.

- ADVAPI32.dll sta per Advanced Windows 32 Base API. Fa parte delle API Windows 32, che include anche KERNEL32.DLL. ADVAPI32.dll fornisce una libreria di servizi API che supporta chiamate di sicurezza e del registro.

- MSVCRT.dll è la Microsoft Visual C++ Runtime Library. Fornisce funzioni essenziali per programmi in C e C++.

- WIWINET.dll (Windows Internet Extensions for Win32) è una libreria di sistema di Windows. Consente alle applicazioni di interagire con i protocolli FTP e HTTP per accedere alle risorse Internet. È utilizzato per la gestione delle connessioni di rete, il download di file e altre operazioni di rete.

Nell’immagine sottostante è possibile vedere le sezioni in cui è diviso il malware. In questo caso sono tutte UPX (Ultimate Packer for eXecutables). Si tratta di un compressore eseguibile gratuito e open source. In sostanza, UPX riduce le dimensioni dei file eseguibili, consentendo loro di essere eseguiti senza dover essere esplicitamente decompressi in anticipo. Tuttavia, è importante notare che l’uso di UPX nei malware è abbastanza raro, poiché è un packer relativamente semplice e ben documentato. Di solito, i creatori di malware preferiscono tecniche più sofisticate per rendere più difficile l’analisi.

Immagine che contiene testo, schermata, software, schermo

Descrizione generata automaticamente

UPX0: Questa sezione contiene il caricatore UPX. È responsabile di decomprimere il resto del file in memoria durante l’esecuzione. Quando il malware viene avviato, il caricatore UPX estrae il payload compresso e lo rende disponibile per l’esecuzione.

UPX1: Questa sezione contiene il payload UPX decompresso. Dopo che UPX0 ha fatto il suo lavoro, il payload viene estratto e posizionato nella sezione UPX1. Questo è il codice effettivo del malware, pronto per essere eseguito.

UPX2: Questa sezione potrebbe contenere dati o risorse aggiuntive utilizzate dal malware. Ad esempio, potrebbe contenere stringhe, tabelle di lookup o altre informazioni necessarie per il funzionamento del malware.

In CFF Explorer è possibile cliccare “UPX Utility” e “Unpack” per decomprimere le sezioni del malware.

Immagine che contiene testo, schermata, software, Icona del computer

Descrizione generata automaticamente

Segue

Di seguito è possibile vedere le sezioni decompresse.

Immagine che contiene testo, schermata, software, schermo

Descrizione generata automaticamente

Il malware in questione è un Trojan. Nell’immagine di seguito (scorrendo in basso a destra) è possibile leggere tutto ciò che fa il malware per ogni sezione (.rdata contiene il payload e .data contiene l’url).

Immagine che contiene testo, schermata, software, Icona del computer

Descrizione generata automaticamente