CONSEGNA S10/L1

Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi statica basica.

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

MODULI DEL MALWARE

Dallo screenshot possiamo vedere le **librerie** che il malware importa. Ecco una descrizione di ciascuna di esse:

KERNEL32.dll: Questa è una delle principali librerie di sistema di Windows che gestisce funzioni di basso livello, come la gestione della memoria, operazioni di input/output e creazione di processi. Praticamente ogni programma Windows utilizza questa libreria per le funzioni di base del sistema operativo.

USER32.dll: Una libreria che fornisce funzioni di base per la gestione dell'interfaccia utente, come finestre e messaggi. Consente al malware di interagire con l'interfaccia pag. 2 grafica del sistema e può essere utilizzato per manipolare finestre o rilevare input dell'utente.

ADVAPI32.dll: Fornisce funzionalità relative alla sicurezza, al registro di sistema e ai servizi. Questa libreria è spesso utilizzata per eseguire operazioni che richiedono privilegi elevati, come la modifica delle impostazioni di sicurezza o l'accesso a parti sensibili del registro di sistema.

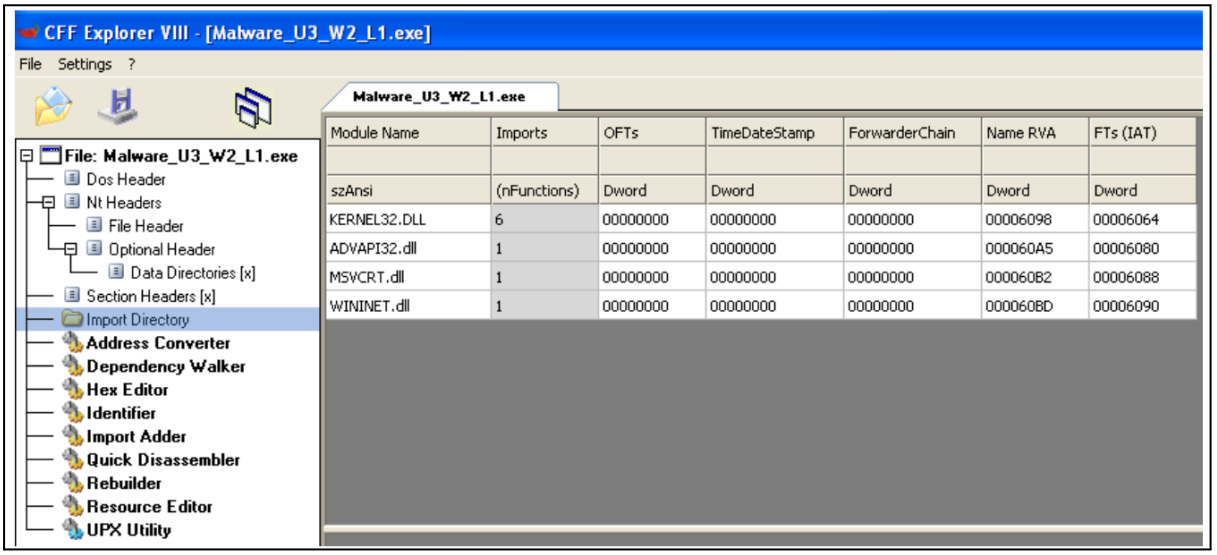
MSVCRT.dll: Il Microsoft Visual C++ Run-Time, che fornisce funzioni standard di C come manipolazione di stringhe, matematica e altre operazioni di base. Viene utilizzata per accedere a funzioni standardizzate senza doverle scrivere da zero.

WININET.dll: Una libreria che fornisce funzioni di alto livello per l'accesso a protocolli Internet come HTTP e FTP. Questa libreria è spesso utilizzata per la comunicazione di rete, inclusa la possibilità di scaricare o caricare dati da e verso Internet.

Queste librerie sono comunemente usate in molti programmi Windows legittimi, ma in un contesto di malware, possono indicare le potenziali capacità del malware, come:

- Modificare o leggere dati sensibili dal sistema
- Interagire con il sistema operativo a livello di rete o di interfaccia utente
- Manipolare servizi e processi

L'uso di queste librerie potrebbe suggerire che il malware ha la capacità di manipolare l'ambiente host, comunicare o scaricare ulteriori payload da Internet e potenzialmente nascondere la sua presenza modificando le impostazioni di sicurezza o di sistema. Per avere una comprensione completa delle capacità del malware basate su queste librerie, dovresti esaminare le specifiche API che importa da queste librerie e come vengono utilizzate nel codice del malware.



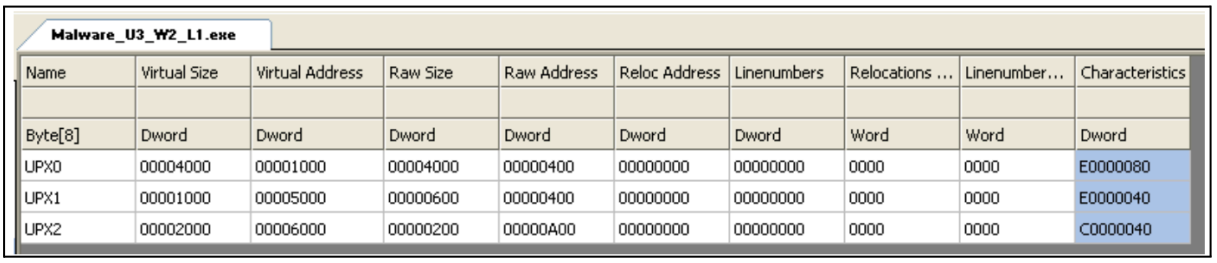
SEZIONI CRIPTATE

Possiamo vedere le sezioni del malware visualizzate in **CFF Explorer**. Le sezioni sono etichettate come **UPX0**, **UPX1** e **UPX2**, che sono indicative di un malware compresso o impacchettato utilizzando **UPX** (*Ultimate Packer for eXecutables*). UPX è un packer eseguibile gratuito e portatile per diversi formati di file eseguibili. Questo può essere usato per comprimere o criptare il codice di un eseguibile per varie ragioni, come ridurre le dimensioni del file o rendere più difficile l'analisi del malware.

UPX0: Questa sezione di solito non ha una dimensione "raw" (dimensione effettiva dei dati nel file) perché è probabile che contenga codice decompresso a runtime. La sua dimensione virtuale è l'ammontare di spazio che occuperà nella memoria quando sarà decompresso. Le caratteristiche E0000060 indicano che la sezione è eseguibile e può essere letta o scritta.

UPX1: Questa sezione sembra essere quella che contiene la maggior parte del codice compresso o criptato, dato dalla sua dimensione "raw" e virtuale. Le caratteristiche E0000040 indicano anch'esse che questa sezione è eseguibile e può essere letta o scritta.

UPX2: È possibile che questa sezione contenga dati o codice aggiuntivi che sono parte del payload compresso. La dimensione sia raw che virtuale è più piccola rispetto a UPX1, e le caratteristiche C0000040 suggeriscono che questa sezione può essere letta o eseguita, ma non scritta.



Malware_U3_W2_L1.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00004000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00002000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

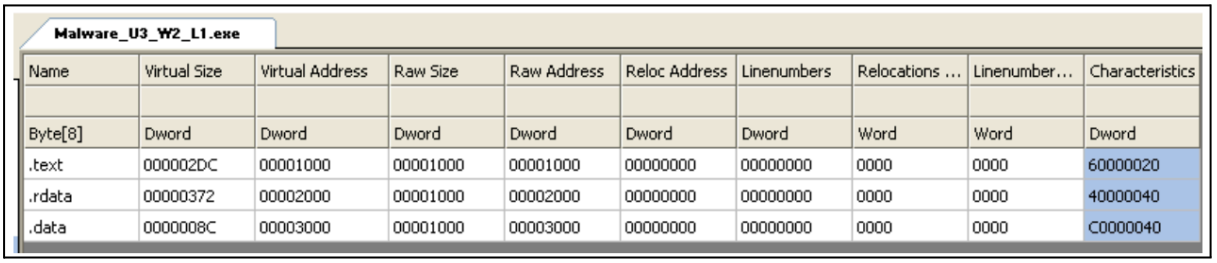
SEZIONI DECRIPTATE

Basandosi sulla nuova schermata una volta fatto "**Unpaking**" del file, ora possiamo analizzare le sezioni del file eseguibile e fornire una descrizione per ciascuna di esse, come richiesto per l'esercizio:

.text: La sezione .text contiene il codice eseguibile del programma. La dimensione virtuale è di 0x2DC e la dimensione raw è di 0x100, con un indirizzo virtuale di partenza di 0x1000. Le caratteristiche 60000020 indicano che questa sezione contiene codice eseguibile (la flag 20000000), è in sola lettura (la flag 40000000), e può essere eseguita nel codice del processo (la flag 00000020).

.rdata: La sezione .rdata contiene dati in sola lettura, come stringhe e costanti. La dimensione virtuale è di 0x372 e la dimensione raw è di 0x100, con un indirizzo virtuale di partenza di 0x2000. Le caratteristiche 40000040 indicano che questa sezione è in sola lettura (la flag 40000000) e che può essere eseguita nel codice del processo (la flag 00000040).

.data: La sezione .data contiene dati inizializzati che possono essere modificati durante l'esecuzione del programma. La dimensione virtuale è di 0x8C e la dimensione raw è di 0x100, con un indirizzo virtuale di partenza di 0x3000. Le caratteristiche C0000040 indicano che questa sezione contiene dati inizializzati (la flag C0000000), può essere letta e scritta (la flag 00000040).



Malware_U3_W2_L1.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	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

CONSIDERAZIONI FINALI

Con le informazioni raccolte dalle sezioni del file eseguibile e dalle librerie importate, possiamo formulare una considerazione finale che analizzi il potenziale comportamento e le capacità del malware.

L'analisi statica del file eseguibile del malware suggerisce che è stato progettato con la capacità di interagire ampiamente con il sistema operativo Windows. La presenza di librerie di sistema fondamentali come KERNEL32.dll e USER32.dll indica che il malware può eseguire funzioni di base, come manipolazione di processi e interazioni con l'interfaccia utente. L'importazione di ADVAPI32.dll implica la potenziale capacità di modificare le impostazioni di sicurezza o di accedere a parti sensibili del registro di sistema, il che potrebbe essere utilizzato per ottenere elevati privilegi o per effettuare modifiche persistenti nel sistema infetto. La libreria MSVCRT.dll è un indicatore di operazioni standard di programmazione, mentre l'uso di WININET.dll suggerisce che il malware può avere la capacità di connettersi a Internet, che potrebbe essere utilizzata per scaricare ulteriori payload malevoli o inviare dati a un attaccante.

Le sezioni standard del file eseguibile, osservate dopo la decompressione da UPX, non mostrano tecniche di occultamento particolari a livello di struttura del file, ma ciò non esclude la presenza di codice malevolo. Il fatto che il malware sia stato inizialmente impacchettato con UPX potrebbe indicare un tentativo di nascondere il suo vero contenuto da un'analisi superficiale e da meccanismi di rilevamento semplici.

In conclusione, sulla base di questa analisi statica preliminare, il malware appare essere sofisticato abbastanza da interagire con il sistema a diversi livelli, possedendo meccanismi di evasione iniziali e la capacità di comunicare o alterare il sistema. Tuttavia, per comprendere appieno il suo comportamento e le intenzioni, sarà necessario eseguire un'analisi dinamica, monitorando l'esecuzione del malware in un ambiente controllato e analizzando il suo comportamento runtime, le modifiche al sistema, le chiamate di rete e qualsiasi altra attività sospetta. Questo passo è cruciale per determinare la vera natura del malware, le sue strategie di attacco e per sviluppare misure di mitigazione efficaci.