

REPORT

23/09/2022

In questo report andremo ad effettuare un'analisi statica basica e un'analisi statica avanzata su un malware.

INTRODUZIONE

Un **Malware (Malicious Software)** è un programma informatico creato per arrecare danno ai sistemi informatici, spesso usato a scopo di lucro.

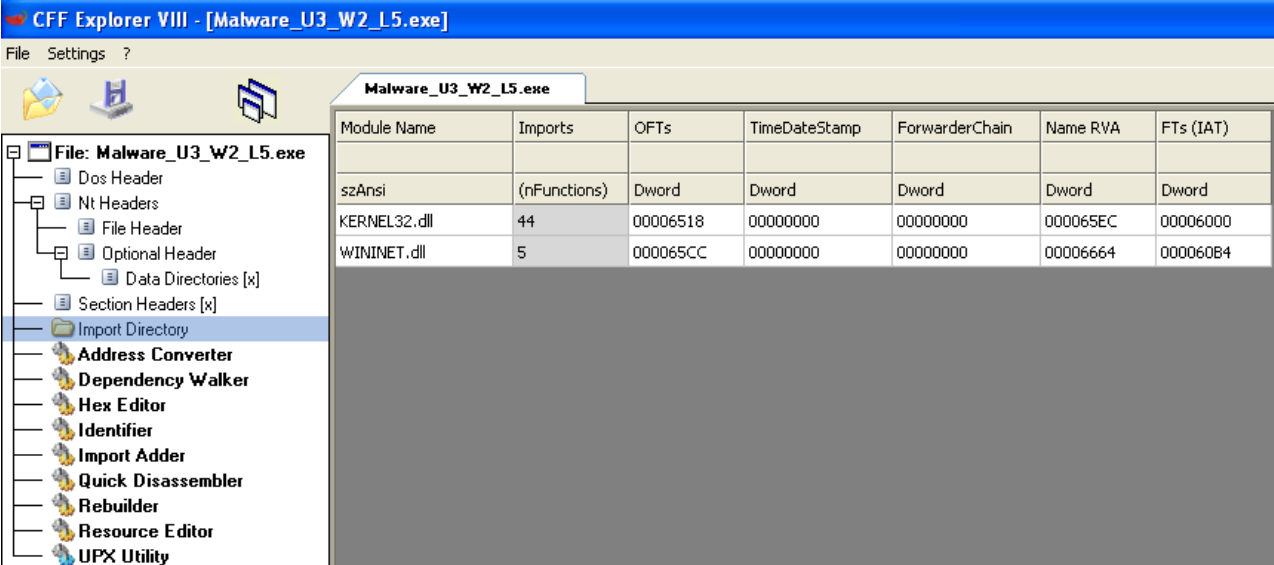
Esistono diverse **tipologie** di Malware ed è compito di un **Malware Analyst** capire con quale tipologia si ha a che fare, attraverso tecniche di **analisi statica** (basica e avanzata) e **analisi dinamica** (basica e avanzata).

LIBRERIE IMPORTATE

Attraverso l'utilizzo del tool **CFF Explorer VIII** ho identificato le librerie di funzione utilizzate dal malware.

Le librerie trovate sono:

- **KERNEL32.dll**: contiene funzioni principali per interagire con il sistema operativo, con la manipolazione dei file e con la gestione della memoria.
- **WININET.dll**: contiene funzioni per l'implementazione di alcuni protocolli come http e ftp.



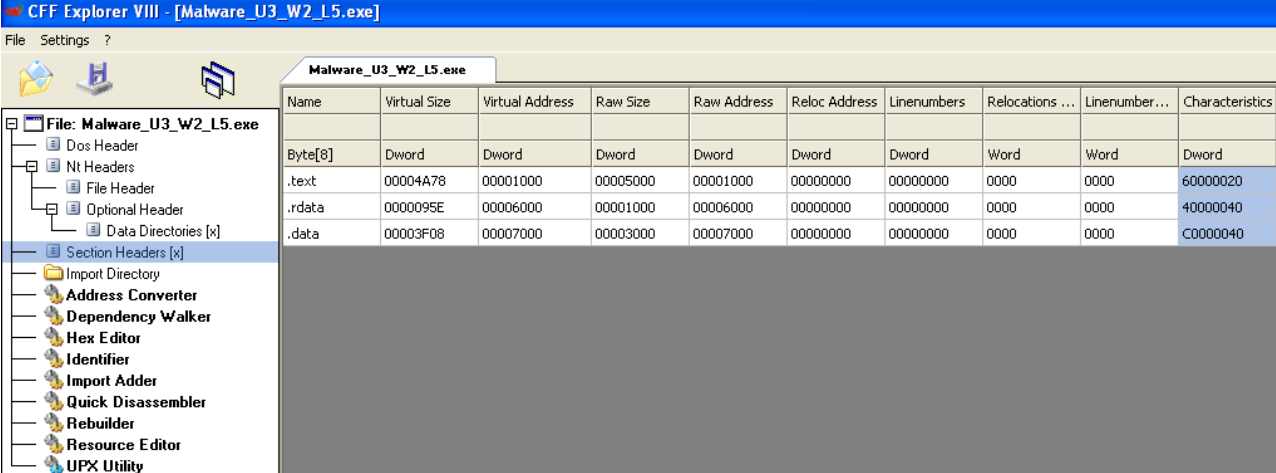
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

SEZIONI DEL FILE ESEGUIBILE

Sempre attraverso l'utilizzo del tool **CFF Explorer VIII** ho trovato le sezioni di cui si compone il file eseguibile del Malware.

Le sezioni trovate sono:

- **.text**: contiene le righe di codice che la CPU (Central Processing Unit) eseguirà una volta avviato il Malware.
- **.rdata**: contiene le informazioni riguardo le librerie e le funzioni importate ed esportate dall'eseguibile.
- **.data**: contiene le variabili globali del programma.



CFF Explorer VIII - [Malware_U3_W2_L5.exe]

File Settings ?

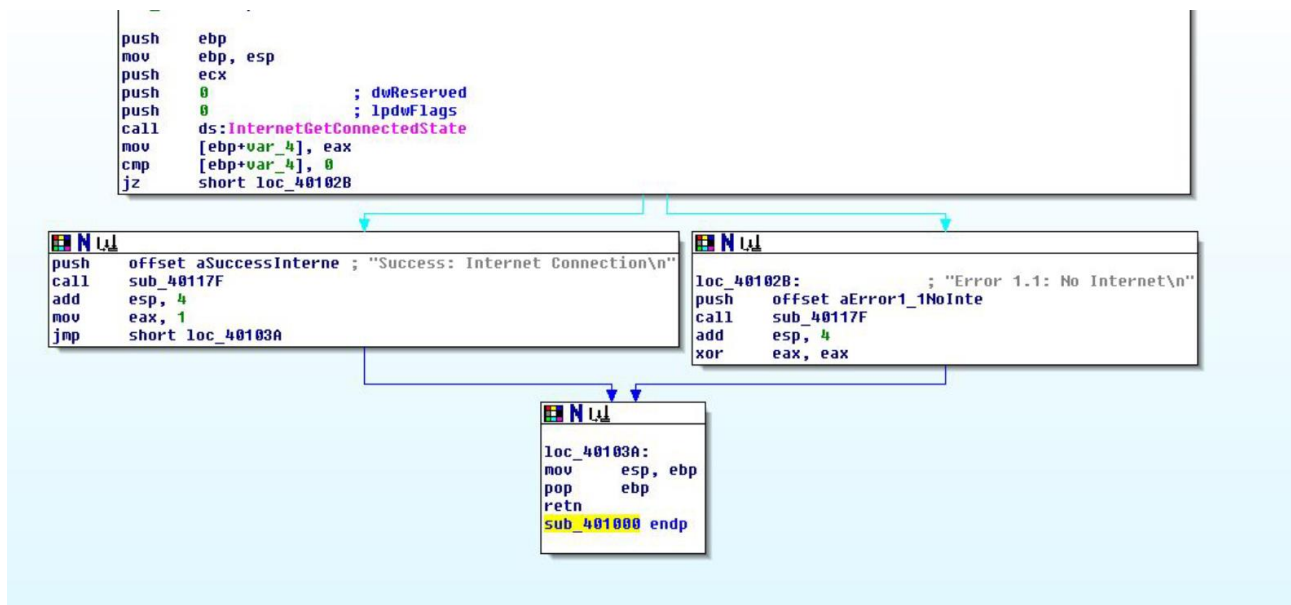
Malware_U3_W2_L5.exe

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	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000	40000040
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000	C0000040

File: Malware_U3_W2_L5.exe

- Dos Header
- Nt Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Addr
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

IDENTIFICAZIONE DEI COSTRUTTI



- **Creazione Stack:** partendo dal primo rettangolo più grande, possiamo notare le prime due righe di assembly che creano lo Stack.
- **Inizializzazione delle variabili:** continuando sul rettangolo più grande, troviamo le successive tre istruzioni (push), che inizializzano le variabili locali.
- **Chiamata alla funzione:** proseguendo avviene la chiamata alla funzione (call) per ottenere lo stato della connessione verso Internet.
- **Inizio del ciclo IF:** le ultime tre righe di codice del rettangolo più grande identificano l'inizio di un ciclo IF, determinato dalla presenza del comando cmp (compare) e subito dopo del comando jz (jump if zero). I successivi due rettangoli, a sinistra e a destra, fanno parte del ciclo IF, e viene **eseguito uno solo di loro** a seconda del risultato della condizione. Più precisamente, viene eseguito il rettangolo **di sinistra se lo zero flag è impostato a zero**; diversamente viene eseguito il rettangolo **di destra se lo zero flag è impostato a uno**. Nel primo caso la connessione a Internet ha successo e viene eseguita una jmp (jump) alle istruzioni finali nel quadrato in basso; nel secondo caso la connessione a Internet non ha successo e si continua con le istruzioni al quadrato in basso.
- **Pulizia dello Stack:** nell'ultimo quadrato in basso, con le prime due istruzioni avviene la pulizia dello Stack.
- **Conclusione:** le ultime due istruzioni del quadrato in basso eseguono un retn (return) alla funzione chiamante.

IPOTESI DEL COMPORTAMENTO

Basandomi sulla funzionalità implementata posso dedurre con **certezza** che il Malware effettui un tentativo di connessione a Internet.

Questo mi fa **ipotizzare** due casistiche:

- **Backdoor:** un Malware molto difficile da identificare una volta che riesce a nascondersi nel computer vittima. Esegue un tentativo di connessione verso Internet ogni volta che il computer vittima si avvia, permettendo al **Black Hat** di controllare la macchina della vittima da remoto.
- **Downloader:** un Malware che una volta avviato tenta la connessione verso Internet, in particolare su un server o un sito specifico, dal quale **scaricare altri Malware** per continuare ad infettare il pc della vittima.