

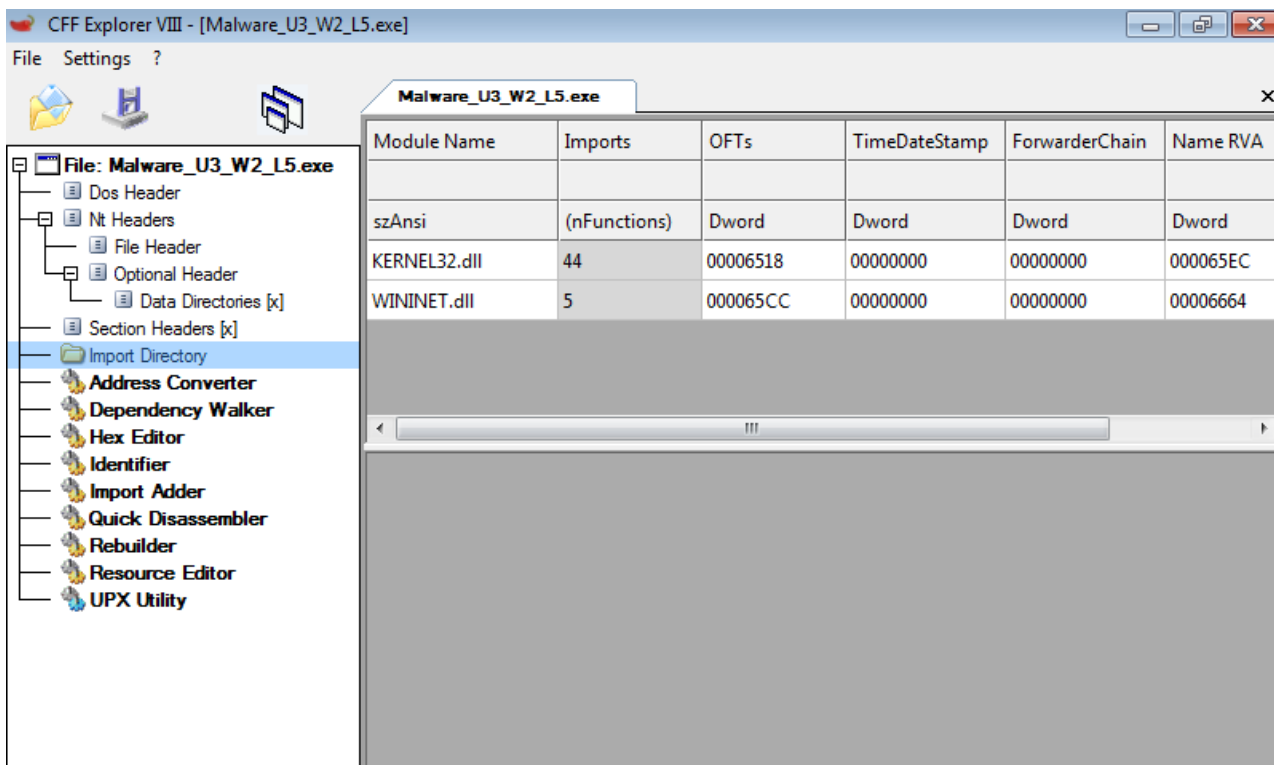
# PROGETTO S10 L5

*Malware\_U3\_W2\_L5*

1. LIBRERIE IMPORTATE DAL MALWARE
2. SEZIONI DEL MALWARE
3. COSTRUTTI NOTI PRESENTI NEL CODICE
4. COMPORTAMENTO DEL CODICE

## 1. LIBRERIE IMPORTATE DAL MALWARE

Utilizzando il tool CFF Explorer possiamo analizzare alcuni dettagli del malware *Malware\_U3\_W2\_L5*, senza la necessità di eseguirlo.



Possiamo notare che ci sono solo due sezioni:

- KERNEL32.dll
- WININET.dll

## KERNEL32.dll

È una delle librerie di sistema fondamentali presenti nei sistemi operativi Windows. Si tratta di una dynamic link library (DLL) che fornisce funzionalità di base al kernel del sistema operativo Windows.

La DLL contiene una vasta gamma di funzioni che possono essere utilizzate da applicazioni utente e da altri componenti di sistema.

Alcune delle funzioni principali fornite da kernel32.dll includono:

- **Gestione dei Processi e dei Thread:** Funzioni per la creazione, la gestione e la terminazione di processi e thread.
- **Gestione della Memoria:** Funzioni per l'allocazione e il deallocazione della memoria, la protezione della memoria e la manipolazione di blocchi di memoria.
- **Gestione dei File e delle Directory:** Funzioni per la creazione, la lettura, la scrittura e la gestione di file e directory.
- **Gestione degli Errori:** Funzioni per la gestione degli errori e la manipolazione delle eccezioni.
- **Tempo e Data:** Funzioni per ottenere informazioni sul tempo e la data di sistema.
- **Gestione delle Risorse:** Funzioni per la gestione delle risorse, come la gestione delle librerie di collegamento dinamico (DLL) e l'accesso a risorse all'interno di file eseguibili.

kernel32.dll è una parte essenziale del sistema operativo Windows e svolge un ruolo fondamentale nel fornire le funzionalità di base necessarie per l'esecuzione delle applicazioni e la gestione del sistema.

Le applicazioni Windows spesso fanno ampio uso delle funzioni fornite da questa DLL per interagire con il sistema operativo.

## WININET.dll

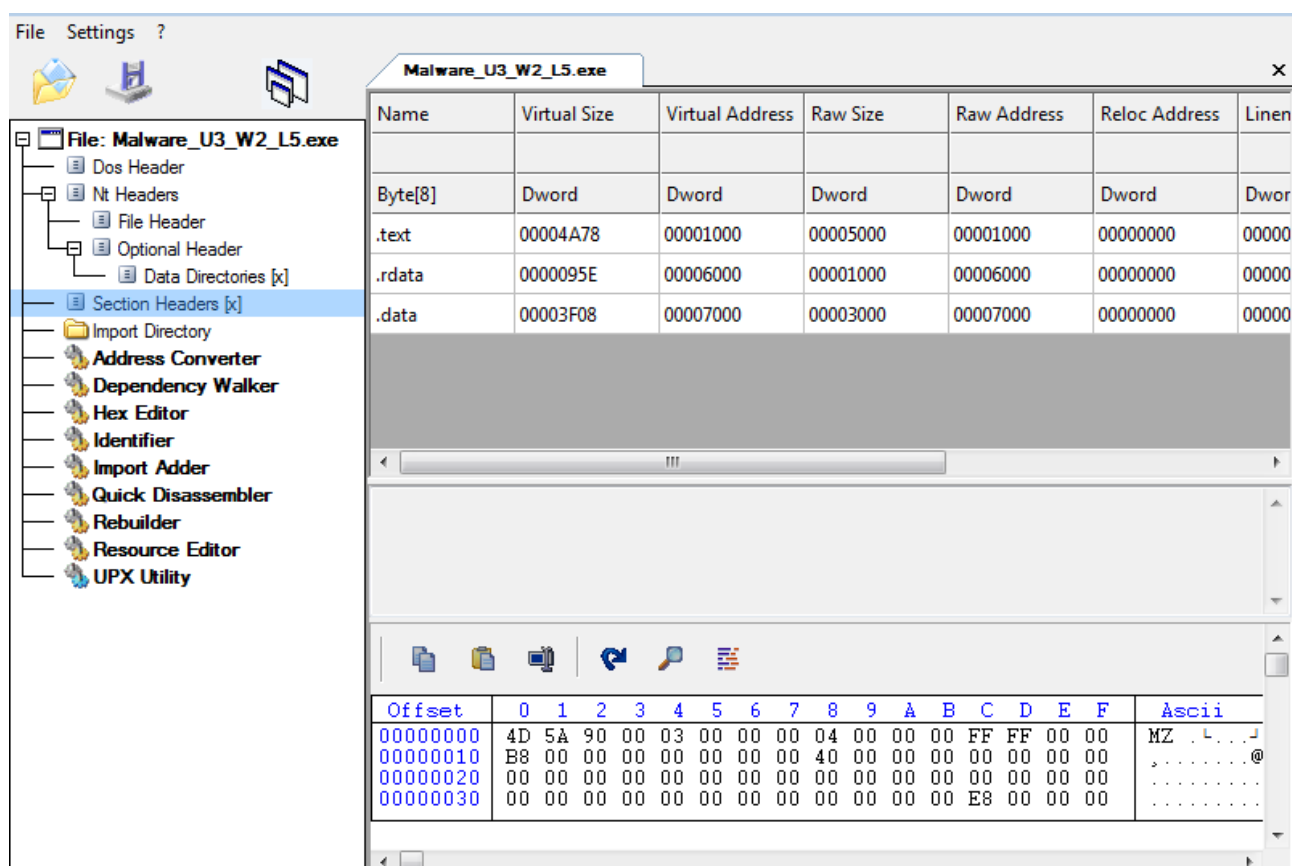
WININET.dll è un'altra dynamic link library (DLL) presente nei sistemi operativi Windows. Questa libreria fornisce un insieme di funzioni per supportare le operazioni di rete e la connessione a Internet nelle applicazioni Windows. È particolarmente utilizzata per la gestione delle operazioni di rete e la comunicazione attraverso il protocollo HTTP.

Alcune delle funzionalità principali offerte da WININET.dll includono:

- **Operazioni di Rete:** Fornisce funzioni per la gestione delle connessioni di rete, la lettura e la scrittura di dati su Internet, e la gestione delle richieste e delle risposte HTTP.
- **Supporto ai Protocolli di Rete:** Supporta vari protocolli di rete, inclusi HTTP, HTTPS, FTP, consentendo alle applicazioni di comunicare con Internet.
- **Cache delle Risorse:** Gestisce la cache delle risorse Internet, consentendo alle applicazioni di memorizzare e recuperare dati da risorse web in modo efficiente.
- **Gestione dei Cookie:** Supporta la gestione dei cookie durante le interazioni con siti web, consentendo di mantenere lo stato della sessione durante le connessioni.
- **Gestione delle Certificazioni:** Fornisce funzionalità per la gestione dei certificati digitali e la sicurezza durante le connessioni sicure (HTTPS).
- **Gestione dei Proxy:** Consente di configurare e gestire le impostazioni di proxy per le connessioni a Internet.

WININET.dll è spesso utilizzata da applicazioni Windows che richiedono la connessione a Internet e l'accesso a risorse online. Questa libreria facilita l'implementazione di funzionalità di rete in modo efficiente e standardizzato per le applicazioni Windows.

## 2. SEZIONE DEL MALWARE



Spostandoci nel menu delle sezioni possiamo trovare:

- .text
- .rdata
- .data

### .TEXT

Indica che quella particolare sezione contiene il codice eseguibile del programma. Questo è tipico per file eseguibili compilati da linguaggi come C, C++ e Assembly.

Gli header delle sezioni vengono spesso utilizzati dal sistema operativo per caricare e organizzare le diverse parti di un programma in memoria durante l'esecuzione. La sezione ".text" contiene le istruzioni della macchina che verranno eseguite quando il programma viene avviato.

La sezione ".text" è fondamentale in quanto contiene il codice che definisce il comportamento del programma quando viene eseguito.

## **.RDATA**

La sezione ".rdata" in un file eseguibile si riferisce a una sezione che contiene dati di sola lettura (read-only data). È spesso utilizzata per memorizzare dati costanti o in sola lettura che il programma può accedere durante l'esecuzione, ma che non può modificare.

Alcuni contenuti tipici sono:

- **Stringhe Costanti:** utilizzate dal programma e che non vengono modificate durante l'esecuzione. (messaggi di errore o informativi)
- **Tabelle di costanti:** ad esempio tabelle di lookup o tabelle di conversione.
- **Dati costanti:** che sono utilizzati dal programma, ma che non devono essere modificati.

L'utilizzo di una sezione ".rdata" aiuta a garantire che i dati all'interno di questa sezione siano trattati come dati di sola lettura, impedendo al programma di modificarli accidentalmente o intenzionalmente durante l'esecuzione.

## **.DATA**



La sezione ".data" in un file eseguibile è utilizzata per contenere dati globali e variabili inizializzate. Questi dati sono accessibili e modificabili durante l'esecuzione del programma. La sezione ".data" è una parte essenziale di molti file eseguibili e consente al programma di memorizzare e manipolare dati durante l'esecuzione.

Alcuni contenuti che sono presenti nella sezione ".data":

- **Variabili Globali:** che possono essere accessibili da diverse parti del programma e che devono mantenere il loro stato tra diverse chiamate di funzione.
- **Variabili Statiche:** dichiarate come static all'interno di funzioni, che mantengono il loro valore tra le chiamate di quella specifica funzione.
- **Variabili Inizializzate:** Dati che devono essere inizializzati con un valore specifico prima dell'esecuzione del programma.
- **Dati Globali:** Altri dati che sono accessibili globalmente nel programma.

Analizzando più attentamente le sezioni, in particolare quella *.data*, possiamo notare come la sezione in *ASCII* rileva un messaggio

“error 1.1 No In”, il che fa presumere una correlazione tra il malware e la verifica della connessione ad Internet.

.data	00003F08	00007000	00003000	00007000	00000000	00000000										
This section contains:																
<div></div>																
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00	00	00	00	00	00	00	00	00	00	00	00	09	1C	40	00	.....@.
64	35	40	00	00	00	00	00	00	00	00	00	AE	1C	40	00	d5@.....®@.
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
45	72	72	6F	72	20	31	2E	31	3A	20	4E	6F	20	49	6E	Error.1.1:No.In

### 3. COSTRUTTI NOTI PRESENTI NEL CODICE

Procedendo all'analisi del codice in Assembly x86, possiamo notare diversi costrutti:

- **Creazione dello stack**
- **Condizionale if**

## - Rimozione dello stack

### Creazione dello stack

```
push    ebp
mov     ebp, esp
```

Attraverso la funzione *push* e *move*, viene inserito il valore *esp* in *ebp*.

La funzione ha lo scopo di inizializzare lo spazio di memoria e di gestire i dati presenti nello stack.

### Condizionale if

```
cmp     [ebp+var_4], 0
jz      short loc_40102B
```

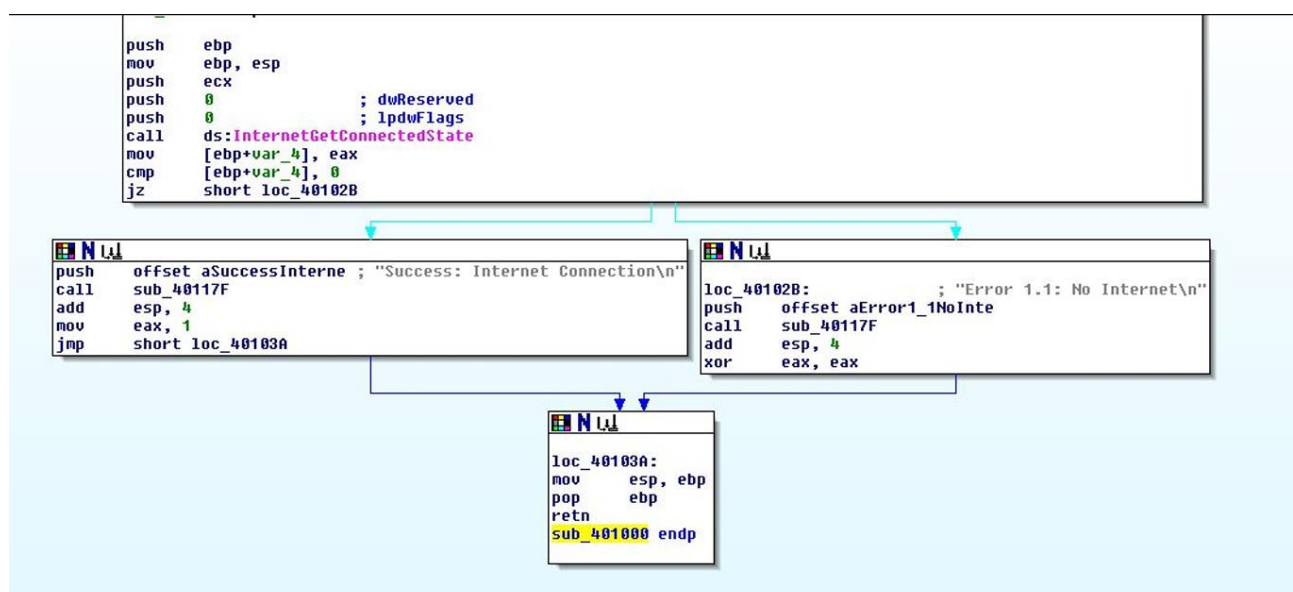
Attraverso la funzione *CMP*, vengono confrontati i due valori, nel caso in cui siano differenti l'esecuzione prosegue con la funzione *JZ*, altrimenti prosegue all'esecuzione del codice successivo.

### Rimozione dello stack

```
mov     esp, ebp
pop     ebp
```

Tramite le istruzioni *mov* e *pop*, viene pulito lo stack deallocando lo spazio riservato ai dati locali.

## 4. COMPORTAMENTO DEL CODICE



Il codice fornito è usato per verificare se c'è una connessione ad Internet o meno.

Tramite il costrutto if, viene verificato se il valore restituito dalla funzione **getinternetconnectstate** è uguale a 0, in questo caso stampa a schermo un messaggio che indica la mancanza di connessione.

Nel caso in cui il valore comparato risulta diverso da 0, la funzione restituisce a schermo un messaggio che comunica l'avvenuta connessione ad internet.