FLOREA ADRIAN MARIO

S10_L5

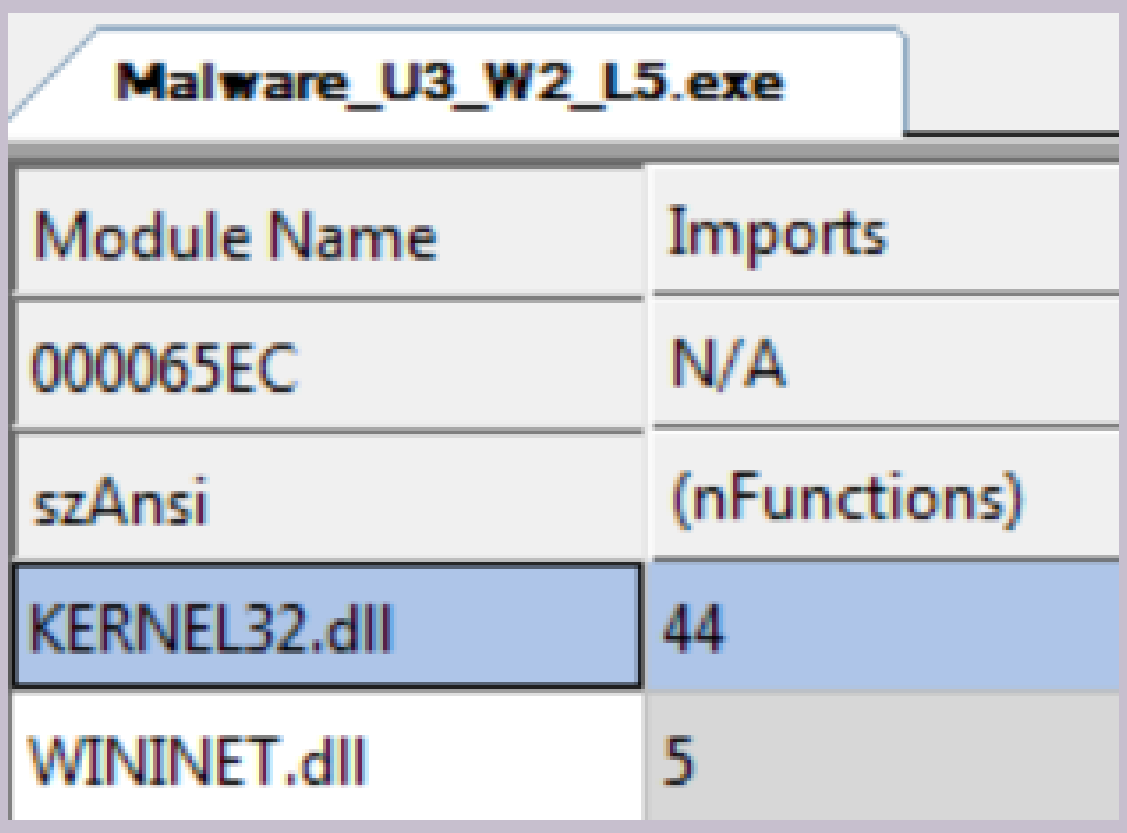
TRACCIA:

CON RIFERIMENTO AL FILE MALWARE_U3_W2_L5 PRESENTE ALL'INTERNO DELLA CARTELLA «ESERCIZIO_PRATICO_U3_W2_L5 » SUL DESKTOP DELLA MACCHINA VIRTUALE DEDICATA PER L'ANALISI DEI MALWARE, RISPONDERE AI SEGUENTI QUESITI:

1. QUALI LIBRERIE VENGONO IMPORTATE DAL FILE ESEGUIBILE ?

2. QUALI SONO LE SEZIONI DI CUI SI COMPONE IL FILE ESEGUIBILE DEL MALWARE ?

1. QUALI LIBRERIE VENGONO IMPORTATE DAL FILE ESEGUIBILE ?



Malware_U3_W2_L5.exe

Module Name	Imports
000065EC	N/A
szAnsi	(nFunctions)
KERNEL32.dll	44
WININET.dll	5

NELLA SEZIONE "IMPORT DIRECTORY" VENGONO VISUALIZZATE LE LIBRERIE CHE IL FILE ESEGUIBILE IMPORTA. IN QUESTO ESEMPIO, POSSIAMO VEDERE CHE SONO PRESENTI DUE LIBRERIE PRINCIPALI:

- **KERNEL32.DLL**
- **WININET.DLL**

QUESTE SONO LE LIBRERIE DI SISTEMA CHE VENGONO IMPORTATE PER FAR FUNZIONARE IL FILE ALL'INTERNO DEL SISTEMA OPERATIVO

NELLA PARTE DESTRA POSSIAMO NOTARE COME SIANO PRESENTI DIVERSE VOCI, LE QUALI CI INDICANO :

- **NOME NELLA LIBRERIA**
- **NUMERO DI FUNZIONI PRESENTI NELLA LIBRERIA**

(QUESTE DUE VOCI SONO QUELLE CHE CI INTERESSANO MAGGIORMENTE RIGUARDANTE LA TRACCIA)

SOTTO OGNI **LIBRERIA**, È POSSIBILE VEDERE **L'ELENCO DELLE FUNZIONI** SPECIFICHE IMPORTATE. AD ESEMPIO, **PER KERNEL32.DLL, SONO MOSTRATE ALCUNE FUNZIONI COME:**

- SZANSI
- SLEEP
- SETSTDHANDLE
- GETSTRINGTYPEW
- GETSTRINGTYPEA
- ..

WININET.DLL CONTIENE INVECE SOLAMENTE QUESTE 5 FUNZIONI:

- INTERNETOPENURLA
- INTERNETCLOSEHANDLE
- INTERNETREADFILE
- INTERNETGETCONNECTEDSTATE
- INTERNETOPENA

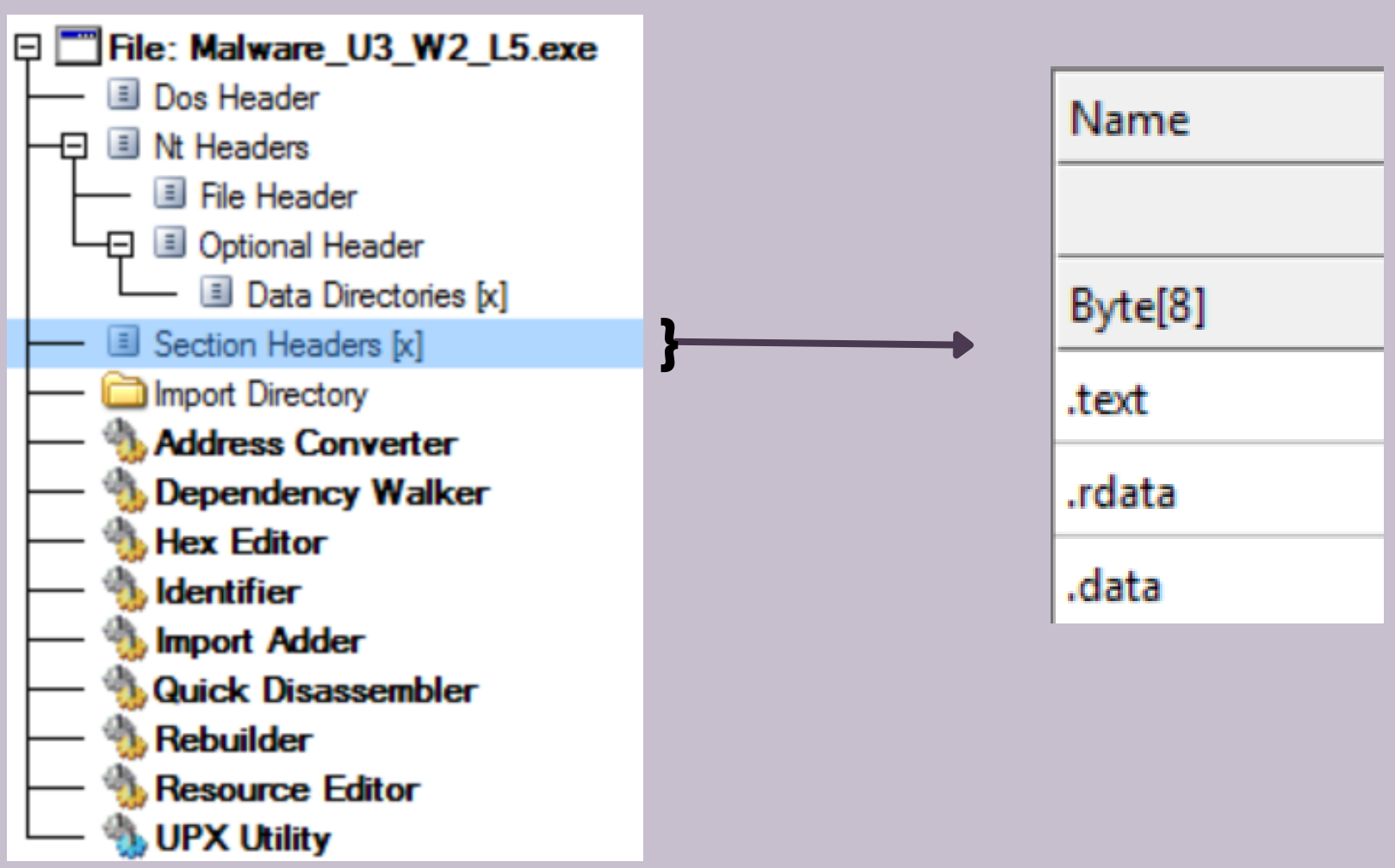
QUESTE FUNZIONI SONO UTILIZZATE DAL PROGRAMMA PER ESEGUIRE OPERAZIONI SPECIFICHE. AD ESEMPIO:

- **SLEEP:** SOSPENDE L'ESECUZIONE DEL PROGRAMMA PER UN DETERMINATO PERIODO.
- **SETSTDHANDLE:** IMPOSTA UN HANDLE STANDARD DI INPUT/OUTPUT.
- **GETSTRINGTYPEW:** OTTIENE INFORMAZIONI SU UN CARATTERE O UNA STRINGA UNICODE.

L'ANALISI E LA COMPRENSIONE DELLE LIBRERIE E DELLE FUNZIONI È IMPORTANTE PERCHÈ CI PERMETTE DI COMPRENDERE COME IL FILE INTERAGISCE CON IL SISTEMA OPERATIVO E CI PERMETTE QUINDI DI CAPIRE ANCHE SE UN FILE POSSA ESSERE POTENZIALMENTE DANNOSO O MENO.

---

2. QUALI SONO LE SEZIONI DI CUI SI COMPONE IL FILE ESEGUIBILE DEL MALWARE ?



SU "**SECTION HEADERS**" NEL PANNELLO SINISTRO DI CFF EXPLORER CI VENGONO MOSTRATE TUTTE LE **PROPRIETÀ**, **TRA CUI** ANCHE I **NOMI DELLE SEZIONI** CHE, IN QUESTO CASO, **SONO I SEGUENTI**:

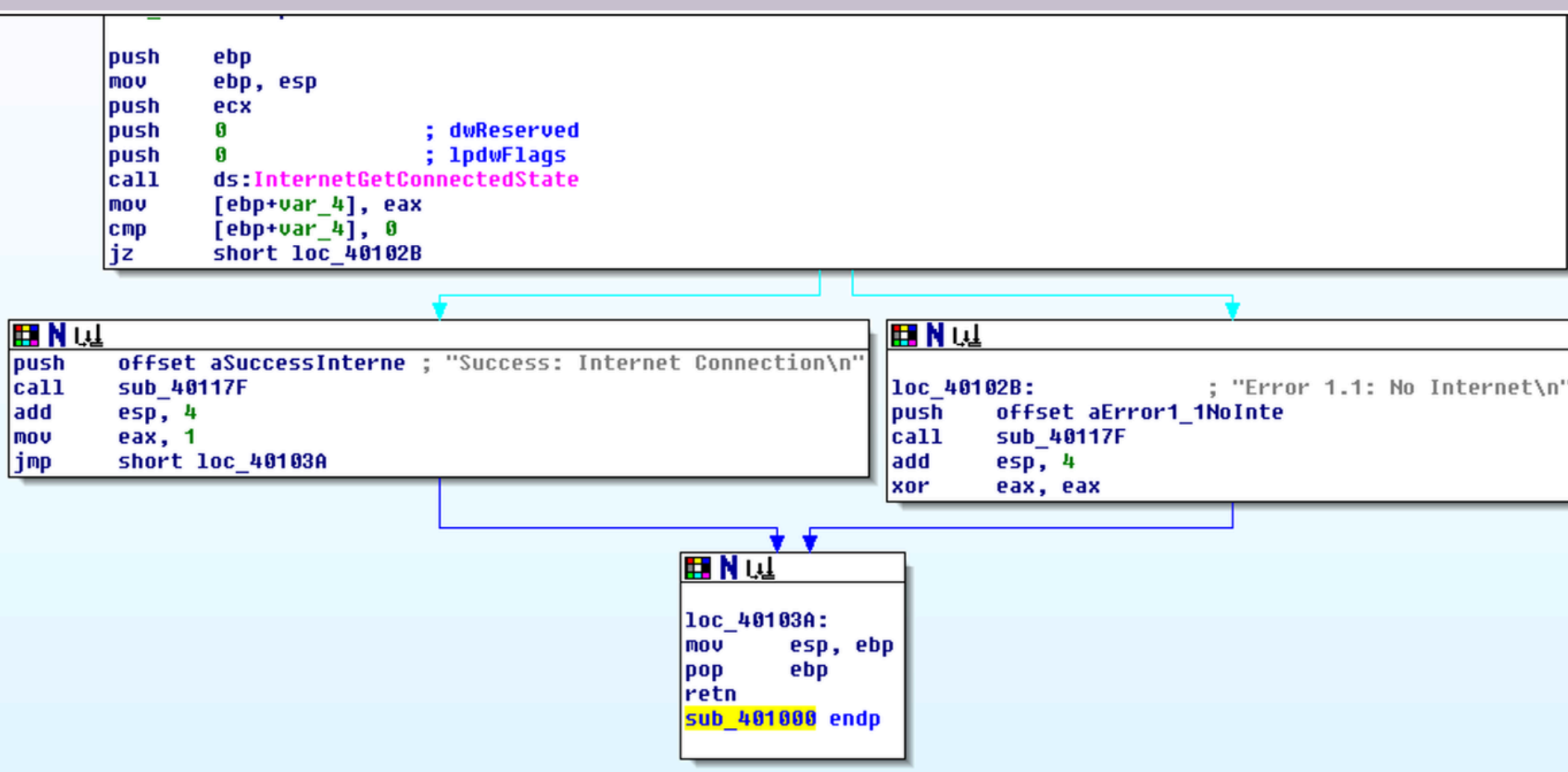
- .TEXT ⟶ **CONTIENE IL CODICE DEL PROGRAMMA.**
- .RDATA ⟶ **CONTIENE DATI DI SOLA LETTURA.**
- .DATA ⟶ **CONTIENE DATI INIZIALIZZATI.**

LE SEZIONI DI UN FILE ESEGUIBILE SONO ESSENZIALI PER CAPIRE SIA LA SUA STRUTTURA CHE IL SUO COMPORTAMENTO. NELL'AMBITO DELL'ANALISI DI MALWARE, STUDIARE QUESTE SEZIONI PUÒ FORNIRE PREZIOSE INDICAZIONI SUL FUNZIONAMENTO DEL MALWARE E SULLE METODOLOGIE CHE ADOTTA.

CON RIFERIMENTO ALLA FIGURA IN SLIDE 3 RISPONDE AI SEGUENTI QUESITI:

3. IDENTIFICARE I COSTRUTTI NOTI (CREAZIONE DELLO STACK, EVENTUALI CICLI, ALTRI COSTRUTTI)

4. IPOTIZZARE IL COMPORTAMENTO DELLA FUNZIONALITÀ IMPLEMENTATA



PUSH EBP

SALVA IL VALORE DEL REGISTRO EBP SULLO STACK.

MOV EBP, ESP

IMPOSTA EBP PER PUNTARE ALLA BASE DELLO STACK FRAME CORRENTE.

PUSH ECX

SALVA IL VALORE DEL REGISTRO ECX SULLO STACK.

PUSH 0

SPINGE IL VALORE 0 SULLO STACK (PARAMETRO DWRESERVED PER INTERNETGETCONNECTEDSTATE).

PUSH 0

SPINGE IL VALORE 0 SULLO STACK (PARAMETRO LPDWFLAGS PER INTERNETGETCONNECTEDSTATE).

CALL DS:INTERNETGETCONNECTEDSTATE

CHIAMA LA FUNZIONE INTERNETGETCONNECTEDSTATE PER VERIFICARE LA CONNESSIONE A INTERNET.

MOV [EBP+VAR_4], EAX

SALVA IL RISULTATO DELLA CHIAMATA DI FUNZIONE NEL VALORE LOCALE VAR_4.

CMP [EBP+VAR_4], 0

CONFRONTA IL VALORE DI VAR_4 CON 0.

JZ SHORT LOC_40102B

SALTA ALL'ETICHETTA LOC_40102B SE IL RISULTATO DEL CONFRONTO È ZERO (NESSUNA CONNESSIONE A INTERNET).

PUSH OFFSET ASUCCESSINTERNE

SPINGE L'INDIRIZZO DELLA STRINGA "SUCCESS: INTERNET CONNECTION" SULLO STACK.

CALL SUB_40117F

CHIAMA LA SUBROUTINE SUB_40117F (PROBABILMENTE PER LOGGARE O MOSTRARE IL MESSAGGIO).

ADD ESP, 4

RIPRISTINA LO STACK RIMUOVENDO IL PARAMETRO PASSATO.

MOV EAX, 1

IMPOSTA IL REGISTRO EAX A 1 (INDICANDO SUCCESSO).

JMP SHORT LOC_40103A

SALTA ALL'ETICHETTA LOC_40103A PER TERMINARE LA FUNZIONE.

LOC_40102B:

ETICHETTA LOC_40102B: INIZIO DEL BLOCCO PER GESTIONE DELL'ERRORE DI CONNESSIONE.

PUSH OFFSET AERROR1_1NOINTE

SPINGE L'INDIRIZZO DELLA STRINGA "ERROR 1.1: NO INTERNET" SULLO STACK.

CALL SUB_40117F

CHIAMA LA SUBROUTINE SUB_40117F (PROBABILMENTE PER LOGGARE O MOSTRARE IL MESSAGGIO DI ERRORE).

ADD ESP, 4

RIPRISTINA LO STACK RIMUOVENDO IL PARAMETRO PASSATO.

XOR EAX, EAX

IMPOSTA IL REGISTRO EAX A 0 (INDICANDO FALLIMENTO).

LOC_40103A:

ETICHETTA LOC_40103A: INIZIO DEL BLOCCO PER TERMINARE LA FUNZIONE.

MOV ESP, EBP

RIPRISTINA IL PUNTATORE DELLO STACK FRAME DEL CHIAMANTE.

POP EBP

RIPRISTINA IL VALORE ORIGINALE DI EBP DAL STACK.

RETN

RITORNA DALLA FUNZIONE.