

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:

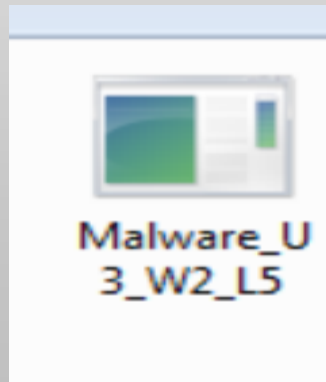
1. Quali **librerie** vengono importate dal file eseguibile?
2. Quali sono le **sezioni** di cui si compone il file eseguibile del malware?

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**
5. **BONUS** fare tabella con significato delle singole righe di codice assembly

1 IDENTIFICAZIONE DELLE LIBRERIE IMPORTATE DAL FILE ESEGUIBILE

- L'ESERCIZIO È CONCENTRATO SULL'ANALISI DEL FILE DI TEST MALWARE_U3_W2_L5.EXE.

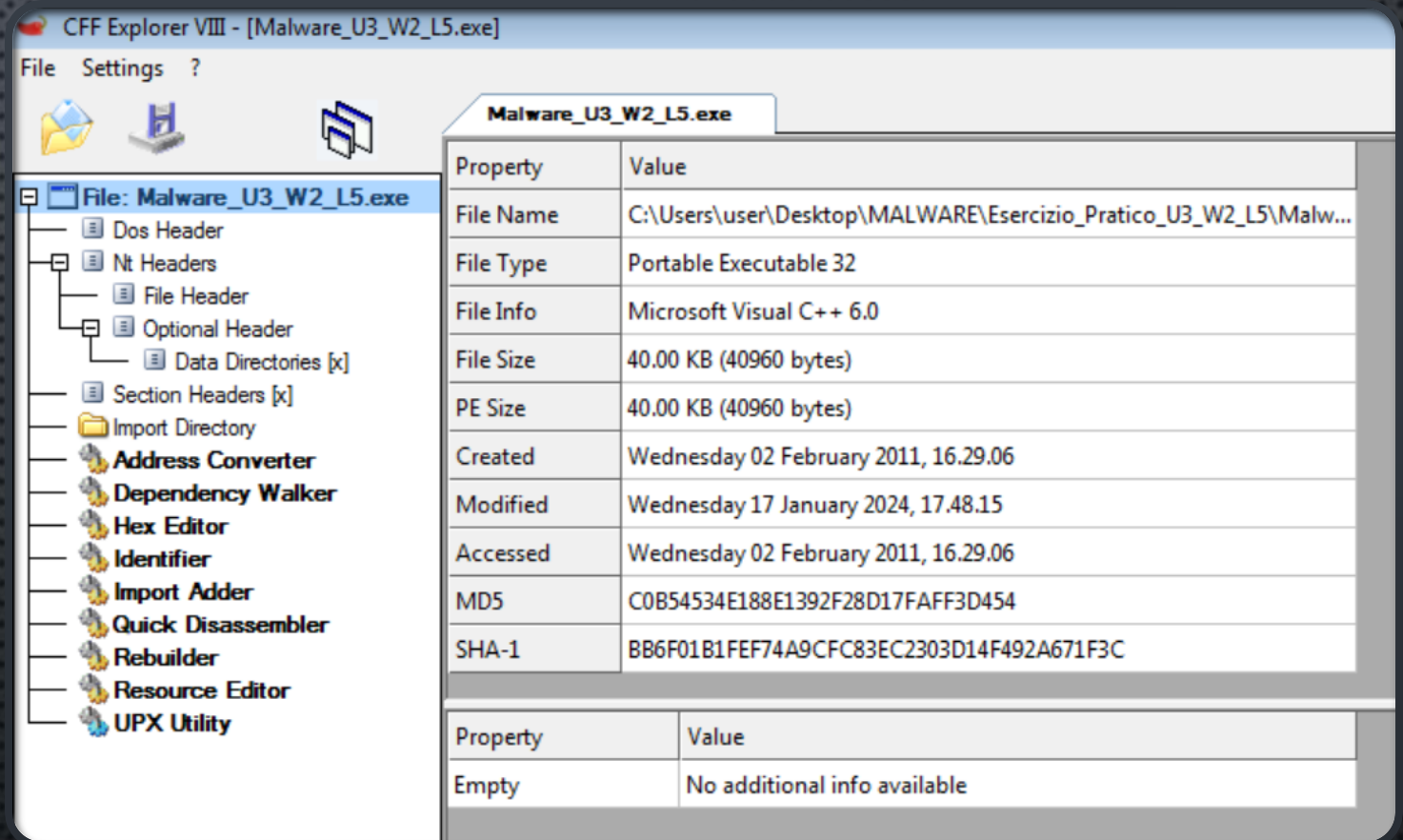


ANALISI STATICA BASICA

- L'ANALISI DEI MALWARE PERMETTE DI ANALIZZARE ACCURATAMENTE UN MALWARE PER VERIFICARNE IL COMPORTAMENTO , LO SCOPO È RIMUOVERLO CORRETTAMENTE DAL SISTEMA.
- NELLA PRIMA SEZIONE DEL TEST SVOLGEREMO L'ANALISI STATICA BASICA, ANDANDO A STUDIARE UN FILE ESEGUIBILE CON ESTENSIONE .EXE..
- LO SCOPO È QUELLO DI ANDARE AD ANALIZZARE IL COMPORTAMENTO MALEVOLO DI UN FILE E DESCRIVERE INFORMAZIONI GENERICHE DELLA SUA FUNZIONALITÀ.
- PER L'ANALISI UTILizzerEMO IL TOOL CFF EXPLORER, SI OCCUPA DI STUDIARE L'HEADER DEL FORMATO PE (PORTABLE EXECUTABLE). ALL'INTERNO TROVIAMO ALCUNE INFORMAZIONI NECESSARIE AL SISTEMA OPERATIVO PER CAPIRE COME GESTIRE IL CODICE DEL FILE.
- ALL'INTERNO TROVIAMO :
- ELENCO DELLE LIBRERIE IMPORTATE E DELLE FUNZIONI RICHIESTE DA UN ESEGUIBILE.
- FUNZIONI ESPORTATE
- SEZIONI DI CUI SI COMPONE UN SOFTWARE
- LA LIBRERIA È UN INSIEME DI FUNZIONI , PER FUNZIONARE UN MALWARE RICHIAMA DELLE FUNZIONI RIPORTATE IN UNA O PIÙ LIBRERIE , CONTROLLARE QUALI SONO LE LIBRERIE E LE SUE FUNZIONI È FONDAMENTALE PER VERIFICARE LO SCOPO DEL MALWARE.

AVVIO TOOL CFF EXPLORER

- NELLA SCHERMATA PRINCIPALE, RESTITUISCE INFORMAZIONI COME LE DIMENSIONI, DATA DI CREAZIONE, HASH (MD5 E SHA-1).



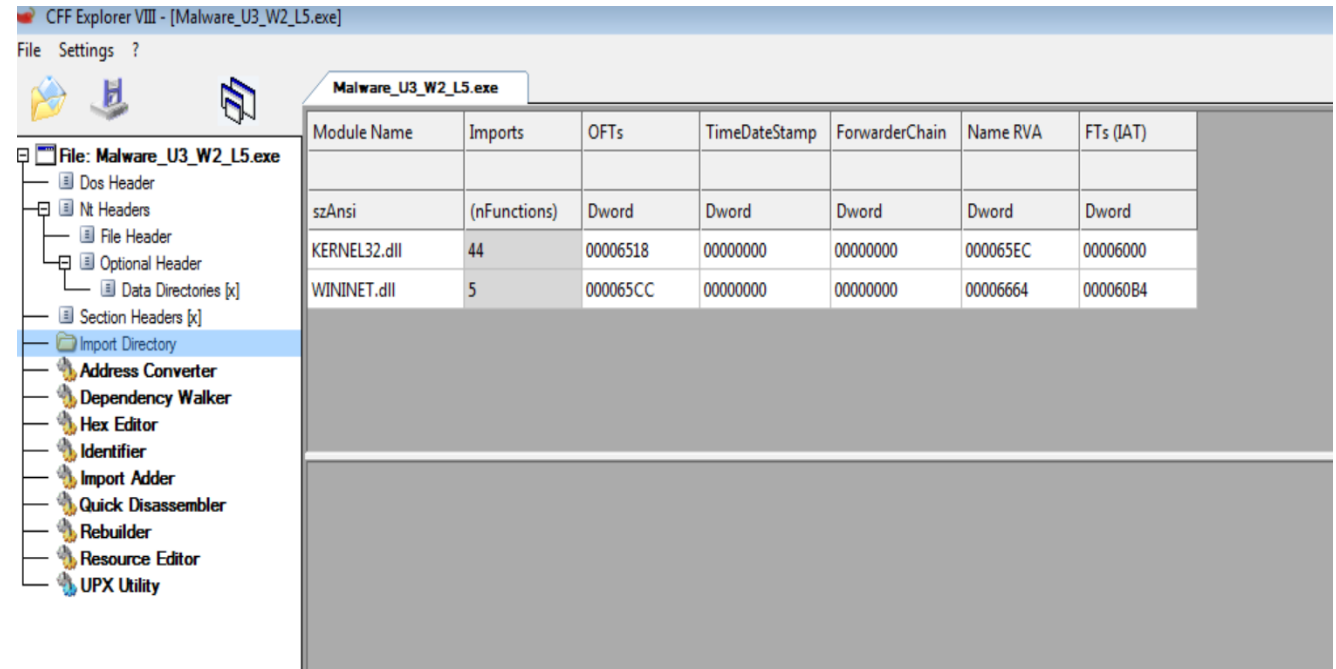
The screenshot displays the CFF Explorer VIII application window. The title bar reads "CFF Explorer VIII - [Malware_U3_W2_L5.exe]". The menu bar includes "File", "Settings", and "?". Below the menu bar are three icons: a folder, a document, and a folder with a document. The left pane shows a tree view of the file structure for "File: Malware_U3_W2_L5.exe", including "Dos Header", "Nt Headers", "File Header", "Optional Header", "Data Directories [x]", "Section Headers [x]", "Import Directory", and various utilities like "Address Converter", "Dependency Walker", "Hex Editor", "Identifier", "Import Adder", "Quick Disassembler", "Rebuilder", "Resource Editor", and "UPX Utility". The right pane shows a tab labeled "Malware_U3_W2_L5.exe" with a table of properties.

Property	Value
File Name	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L5\Malw...
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	40.00 KB (40960 bytes)
PE Size	40.00 KB (40960 bytes)
Created	Wednesday 02 February 2011, 16.29.06
Modified	Wednesday 17 January 2024, 17.48.15
Accessed	Wednesday 02 February 2011, 16.29.06
MD5	C0B54534E188E1392F28D17FAFF3D454
SHA-1	BB6F01B1FEF74A9CFC83EC2303D14F492A671F3C

Property	Value
Empty	No additional info available

SEZIONE IMPORT DIRECTORY

- NELLA SEZIONE DI IMPORT DIRECTORY NOTIAMO L'IMPORTAZIONE DELLE LIBRERIE DAL MALWARE.
- KERNEL32.DLL= LA LIBRERIE CONTIENE LE FUNZIONI PER INTERAGIRE CON IL SISTEMA OPERATIVO AD ESEMPIO LA GESTIONE DELLA MEMORIA.
- WININET.DLL= LA LIBRERIA IMPLEMENTA LE FUNIZIONI DI ALCUNI PROTOCOLLI RETE AD ESEMPIO HTTP E FTP.



CFF Explorer VIII - [Malware_U3_W2_L5.exe]

File Settings ?

Malware_U3_W2_L5.exe

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

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 Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

2. IDENTIFICAZIONE DELLE SEZIONI DI CUI SI COMPONE IL FILE ESEGUIBILE

NELLA SEZIONE SECTION HEADERS , NOTIAMO LE SEZIONI:

.TEXT= FILE ESEGUIBILE CONTENENTE ISTRUZIONI IN CODICE MACCHINA CHE LA CPU ELABORA DURANTE L'AVVIO DEL SOFTWARE. QUESTA SEZIONE È CRUCIALE POICHÉ GUIDA IL FUNZIONAMENTO DEL PROGRAMMA. LE ALTRE SEZIONI CONTENGONO PRINCIPALMENTE DATI O SUPPORTO PER IL PROGRAMMA. LA CPU ESEGUE SOLO QUESTA SEZIONE POICHÉ CONTIENE LE ISTRUZIONI ESSENZIALI PER L'ESECUZIONE DEL SOFTWARE.

.RDATA= CONTIENE INFORMAZIONI SULLE LIBRERIE E FUNZIONI IMPORTATE ED ESPORTATE DALL'ESEGUIBILE.

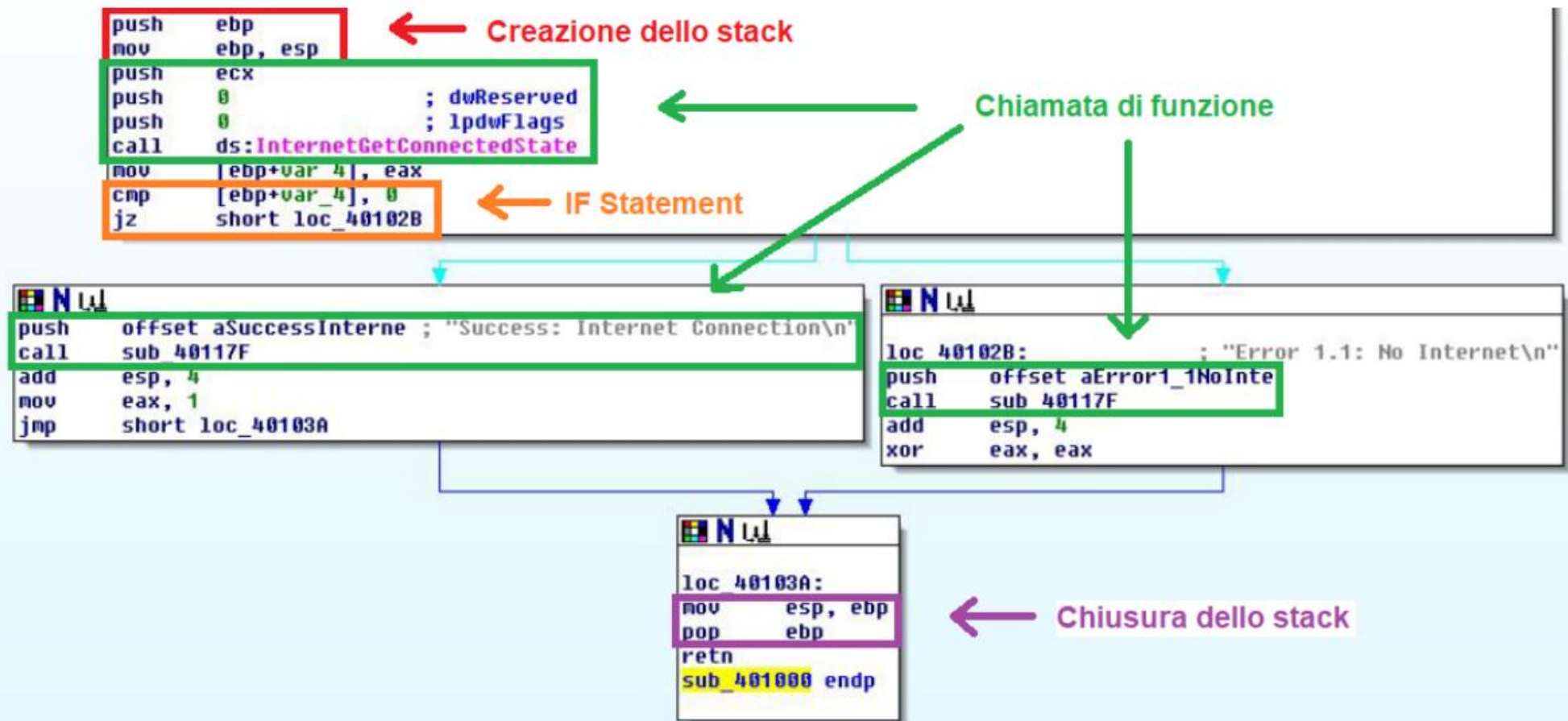
.DATA= CONTIENE DATI VARIABILI GLOBALI DELL'ESEGUIBILE, DISPONIBILI DA QUALSIASI PARTE DEL PROGRAMMA.

The screenshot displays the CFF Explorer VIII interface for the file 'Malware_U3_W2_L5.exe'. The left pane shows the file's structure, including headers, section headers, and various utilities. The right pane shows the file's properties.

Property	Value
File Name	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L5\Malw...
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	40.00 KB (40960 bytes)
PE Size	40.00 KB (40960 bytes)
Created	Wednesday 02 February 2011, 16.29.06
Modified	Wednesday 17 January 2024, 17.48.15
Accessed	Wednesday 02 February 2011, 16.29.06
MD5	C0B54534E188E1392F28D17FAFF3D454
SHA-1	BB6F01B1FEF74A9CFC83EC2303D14F492A671F3C

Property	Value
Empty	No additional info available

3. IDENTIFICAZIONE DEI COSTRUTTI NOTI A PARTIRE DALLE ISTRUZIONI IMPLEMENTATE IN LINGUAGGIO ASSEMBLY



4. IPOTESI SUL COMPORTAMENTO DELLE FUNZIONALITÀ IMPLEMENTATE

- IL PROGRAMMA CREA UNO STACK PER LE VARIABILI LOCALI USANDO I PUNTATORI EBP ED ESP. SUCCESSIVAMENTE, VERIFICA SE LA MACCHINA HA ACCESSO A INTERNET TRAMITE LA FUNZIONE `InternetGetConnectedState`. SE C'È CONNESSIONE, ESEGUE DETERMINATE OPERAZIONI E CHIUDE LO STACK. SE NON C'È CONNESSIONE, REIMPOSTA IL REGISTRO EAX A 0. IL MALWARE POTREBBE SFRUTTARE LA CONNESSIONE INTERNET PER INVIARE FILE A SERVER REMOTI, SCARICARE FILE DANNOSI, CONNETTERSI A DOMINI INFETTI O CREARE UNA BACKDOOR PER UNA COMUNICAZIONE PERSISTENTE. POTREBBE ESSERE UN DOWNLOADER, UN TROJAN O UNA BACKDOOR.

37

/72

Punteggio della comunità

37/72 fornitori di sicurezza e nessun sandbox hanno contrassegnato questo file come dannoso

RianalizzareSimileDi più

b71777edbf21167c96d20ff803cbcb25d24b94b3652db2f286dcd6efd3d8416a

Misurare
40,00KB

Data dell'ultima modifica
2 giorni fa

EXE

peexe

controlla gli adattatori di rete

moduli runtime

accesso diretto all'orologio della CPU

armadillo

RILEVAMENTO

DETTAGLI

RELAZIONI

COMPORTAMENTO

TELEMETRIA

COMUNITÀ7

Unisciti alla community VT e usufruisci di ulteriori approfondimenti della community e rilevamenti in crowdsourcing, oltre a una chiave API per automatizzare i controlli.

Etichetta di minaccia popolaretrojan.r002c0pdm21

Categorie di minaccia Trojan

Etichette familiarir002c0pdm21

Analisi dei fornitori di sicurezza

Vuoi automatizzare i controlli?

Alibaba	Trojan:Win32/Generic.2cc376c1	AliCloud	Porta sul retro
Antiy-AVL	Trojan/Win32.BTSGenerico	Avast	Win32:PUP-gen [PUP]
AVG	Win32:PUP-gen [PUP]	Bkav Pro	W32.Common.362CBAB4
CrowdStrike Falcon	Vittoria/malicious_confidence_100% (W)	Istinto profondo	MALIZIOSO
DrWeb	Trojan.MulDrop7.63090	Elastico	Dannoso (confidenza alta)
ESET-NOD32	Win32/Agent.WOO	Fortinet	W32/Agente.WOOltr
GData	Win32.Trojan.Agent.DZ3C1W	Google	Rilevato
Gridinsoft (senza cloud)	Ransom.Win32.Wacatac.oals1	Ikarus	Trojan.Win32.Agent
Kingsoft	Win32.Troj.Undef.a	Leone	Trojan.Win32.Generic.4!c
Malwarebytes	Generic.Trojan.Malicious.DDS	MASSIMO	Malware (punteggio ai=97)

VIRUS TOTAL
ANDANDO AD ANALIZZARE
GLI HASH RICAVATI DA CFF
EXPLORER VIRUS TOTAL CI
DA COME RISULTATO LA
SEGUENTE IMMAGINE, LO
SCORE È DI 37/72 E VIENE
IDENTIFICATO COME
SOFTWARE MALEVOLO. LO
IDENTIFICA COME
MALWARE DI TIPO TROJAN

Istruzione	Descrizione
Push ebp	"Pusha" il registro Extended Base Pointer sulla cima dello stack
Mov ebp, esp	Assegna il valore del registro dell'Extended Stack pointer al registro dell'Extended Base Pointer
Push ecx	Posta il valore nel registro "ecx" in cima allo stack
Push 0	Pusha (= "spinge") il parametro 0 di una variabile in cima allo stack
Push 0	Pusha il parametro 0 di una variabile in cima allo stack
Call ds: InternetGetConnectedState	Chiama la funzione "InternetGetConnectedState" per verificare lo stato di connettività del sistema locale
Mov [ebp+var_4], eax	Copia il valore contenuto nel registro EAX nel registro [ebp+var_4]
Cmp [ebp+var_4], 0	Effettua una sottrazione tra il parametro nel registro [ebp+4_var] e 0, modificando le flag ZF e CF
Jz short loc_40102B	Salto se zero: controlla la Zero Flag ottenuta dalla precedente istruzione cmp
Push offset aSuccessInterne	Posta la stringa "Success: Internet Connection\n" in un registro in cima allo stack
Call sub_40117F	Chiama la funzione all'indirizzo di memoria 40117F
Add esp, 4	Somma 4 al valore contenuto nel registro ESP
Mov eax, 1	Sostituisce il valore nel registro EAX con 1
Jmp short loc_40103A	Salta all'indirizzo di memoria 40103A
loc_40102B	Etichetta per la locazione di memoria 40102B
Push offset aError1_1NoInte	Pusha l'offset aError1_NoInte in cima allo stack
Call sub_40117F	Chiama la funzione all'indirizzo di memoria 40117F
Add esp, 4	Somma 4 al valore contenuto nel registro ESP
Xor eax, eax	Usa l'istruzione XOR per inizializzare a 0 il registro EAX
loc_40103A	Etichetta per la locazione di memoria 40103A
Mov ebp, esp	Copia il contenuto del registro EBP nel registro ESP
Pop ebp	Rimuove il contenuto del registro EBP dallo stack
Retn	Ritorna al programma chiamante al termine di una procedura
sub_401000 endp	Indica la fine della procedura all'indirizzo di memoria 401000

5. BONUS FARE TABELLA CON SIGNIFICATO DELLE SINGOLE RIGHE DI CODICE ASSEMBLY