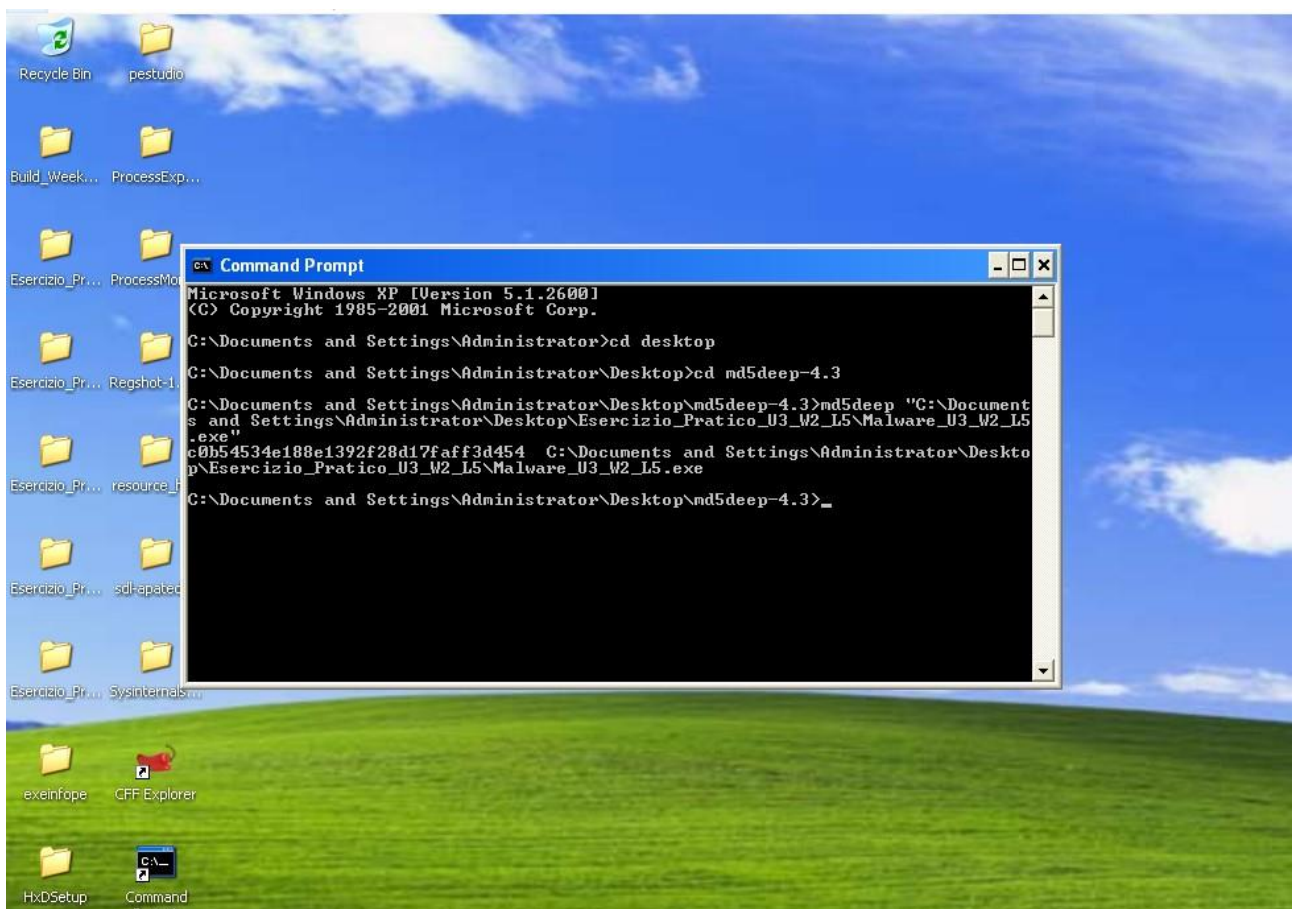


MALWARE_U3_W2_L5

Dobbiamo studiare un potenziale malware. Per farlo andremo ad effettuare diversi tipi di analisi per cercare più informazioni possibili e poi andremo a scremare e selezionare quelle che ci interessano.

ANALISI STATICA BASICA

Sono diverse le operazioni che possiamo effettuare su questo eseguibile. Potremmo partire da un veloce check sul web caricando il file su virustotal, ma siamo in una macchina senza connessione per questioni di sicurezza. Procediamo dunque con le operazioni offline sul file, come ad esempio il controllo della firma o *hash* del file usando **md5deep**. Ci spostiamo nella cartella dove è contenuta l'utility e diamo il comando <md5deep "percorso assoluto file"> da prompt.



Trovato l'hash possiamo andarlo a cercare esternamente sempre su virustotal. La schermata che ci restituisce il sito dalla ricerca dell'hash è la seguente:

39 security vendors and no sandboxes flagged this file as malicious

b71777ed821167c96d20f903c3cb25d4b54b3652db2086dc6ef3d8416a

Size: 40.00 KB | Last Analysis Date: 8 days ago

peexe check-network-adapters runtime-modules armadillo direct-cpu-clock-access

Community Score: 39/71

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.r002c0pdm21 | Threat categories: trojan | Family labels: r002c0pdm21

Security vendors' analysis

Vendor	Detection	Category	Label
Alibaba	Trojan.Win32/Generic.be125c32	Antiy-AVL	Trojan.Win32.BTSGeneric
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.16f74
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DnWeb	Trojan.MulDrop.63090
Elastic	Malicious (high Confidence)	ESET-NOD32	Win32/Agent.WOO
Fortinet	W32/Agent.WOO!tr	GData	Win32:Trojan.Agent.D23C1W
Google	Detected	Gridinsoft (no cloud)	Ransom.Win32.Wacatac.oals1
Ikarus	Trojan.Win32.Agent	Lionic	Trojan.Win32.Generic.4tc
Malwarebytes	Generic.Trojan.Malicious.DDS	MAX	Malware (ai Score=97)

Si tratta sicuramente di un file malevolo, a quanto pare di tipo trojan. Proviamo a cercare informazioni aggiuntive procedendo nell'analisi statica basica, usando questa volta l'utility **strings** di sysinternals per analizzare tutte le *stringhe* di codice contenute nell'eseguibile.

Sempre dal prompt dei comandi, ci spostiamo nella cartella dell'utility e scriviamo il comando <strings "file eseguibile".

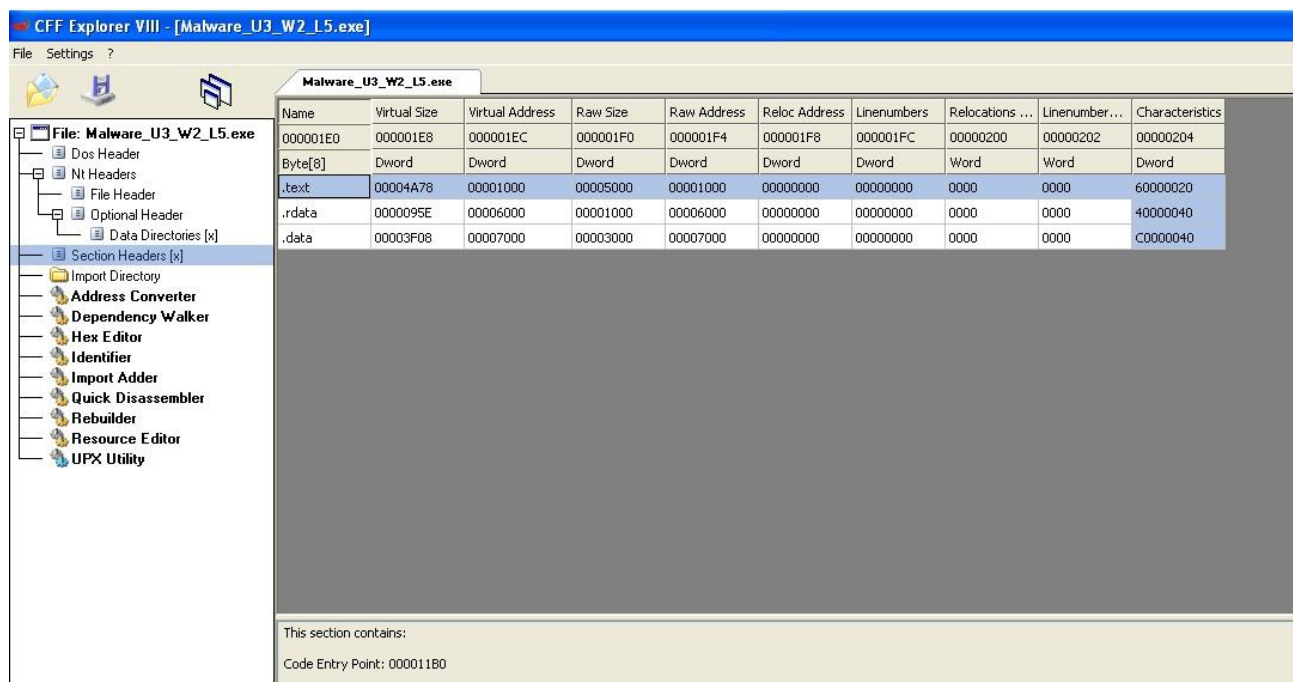
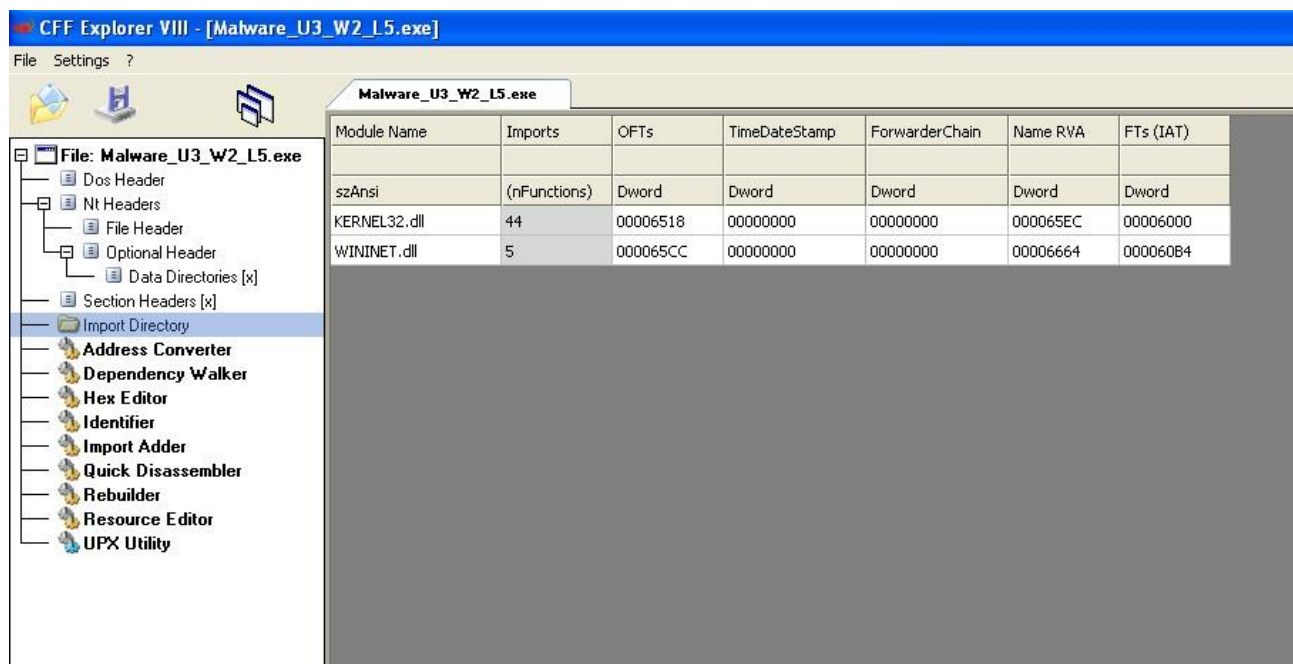
```

C:\> cd C:\Program Files\sysinternals\
C:\Program Files\sysinternals\> strings "C:\Program Files\sysinternals\strings.exe"
R6002
Microsoft Visual C++ Runtime Library
Program:
...
(program name unknown)
GetLastActivePopup
GetActiveWindow
MessageBox
user32.dll
nq
rge
rre
ARR
Sleep
kernel32.dll
InternetGetConnectedState
InternetReadFile
InternetCloseHandle
InternetOpenUrl
InternetOpen
WININET.dll
GetCommandLineA
GetVersion
ExitProcess
TerminateProcess
GetCurrentProcess
UnhandledExceptionFilter
GetModuleFileNameA
FreeEnvironmentStringsA
FreeEnvironmentStringsW
WideCharToMultiByte
GetEnvironmentStrings
GetEnvironmentStringsW
GetHandleCount
GetStdHandle
GetFileType
GetStartupInfoA
GetModuleHandleA
GetEnvironmentVariableA
GetVersionExA
HeapDestroy
HeapCreate
VirtualFree
HeapFree
RtlUnwind
WriteFile
HeapAlloc
GetCPInfo
GetACP
GetOEMCP
VirtualAlloc
HeapAlloc
GetProcAddress
LoadLibraryA
GetLastError
FlushFileBuffers
SetFilePointer
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
SetStdHandle
CloseHandle
MSG
Error 1.1: No Internet
Success: Internet Connection
Error 2.3: Fail to get command
Error 2.2: Fail to ReadFile
Error 2.1: Fail to OpenURL
http://www.practicalmalwareanalysis.com/cc.htm
Internet Explorer 7.5/pna
Success: Parsed command is %c
Ha0

```

Riceviamo una lista di stringhe, e tra molte inutili o incomprensibili (a sinistra) ritroviamo invece delle stringhe che possono confermarci la natura malevola del file. Nell'immagine a destra evidenziate ci sono le librerie richiamate dell'eseguibile, rispettivamente kernel32 e wininet e successivamente infatti sembra che il malware contenga tutte stringhe adibite all'implementazioni di protocolli di rete, probabilmente per creare una backdoor.

Il prossimo tool che andiamo ad utilizzare è **CFF explorer** per controllare dall'header del formato PE (portable executable) le funzioni importate ed esportate dal malware. Dalla finestra principale del programma apriamo il nostro malware ed analizziamo le varie finestre:

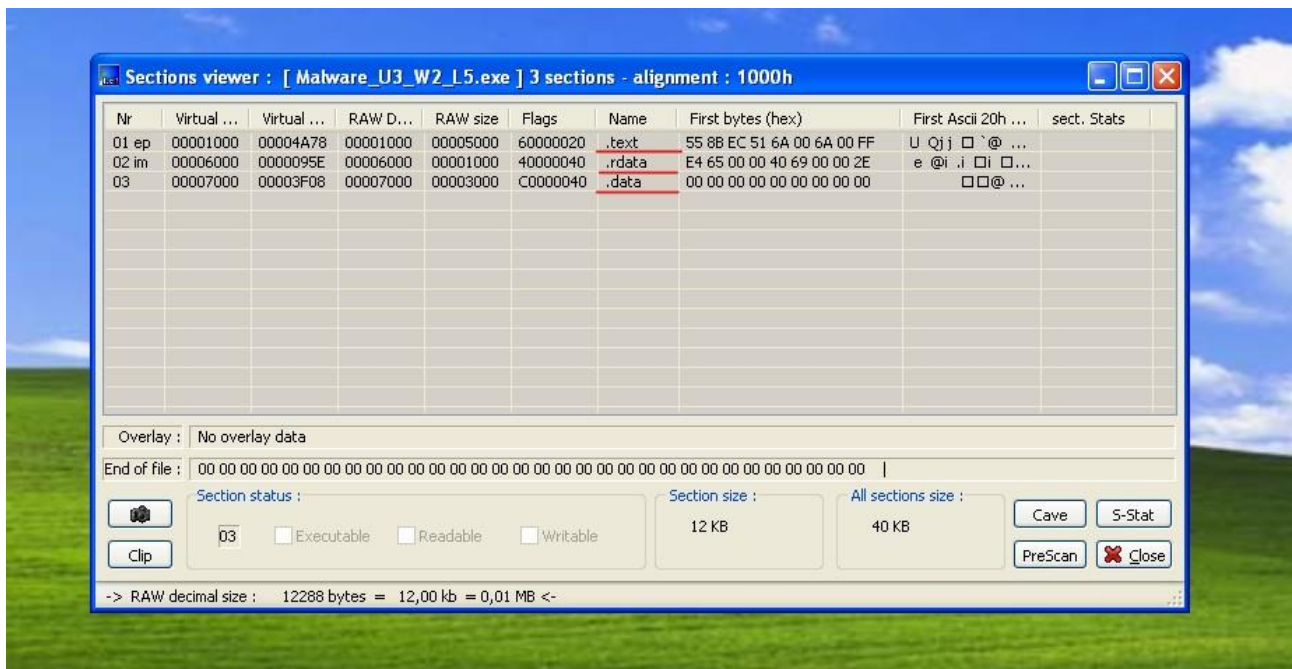


Ritroviamo anche qui le librerie importate *kernel* e *wininet*, nonché le *sezioni* di cui è composto il file, ovvero *“.text”*, *“.rdata”* e *“.data”*. Andiamo ad utilizzare un ultimo tool simile a quello appena visto, per

vedere se possiamo ricavare qualche informazione aggiuntiva: **ExeinfoPE**. Una volta aperto, andiamo a caricare il file dall'opzione in alto a destra in rosso e successivamente andiamo a visualizzare le diverse sezioni dal pulsante in blu.



Il risultato è il seguente:



Quelle evidenziate in rosso sono effettivamente le *sezioni* del file viste prima, con aggiunta delle virtual e raw size, nonché altre informazioni potenzialmente utili. Ora abbiamo una panoramica completa dal punto di vista dell'analisi statica che ci permette di stilare delle conclusioni.

1. LIBRERIE IMPORTATE

Abbiamo visto che il malware sembra importare due **LIBRERIE** importanti:

- KERNEL32.DLL: una delle librerie più comuni di windows, che contiene tutte le funzioni principali per le interazioni con l'OS come la creazione e modifica dei file, o la gestione della memoria
- WININET.DLL: una libreria che contiene le funzioni per l'implementazione dei protocolli di rete (http, FTP...)

Come si evince anche dal risultato dell'analisi delle stringhe dell'eseguibile nonché dalla scansione di virustotal che ce lo riporta come trojan, sembrerebbe legittimo pensare che il malware vada a importare dinamicamente queste due librerie probabilmente per stabilire una connessione non autorizzata a qualche server remoto per l'apertura di una backdoor.

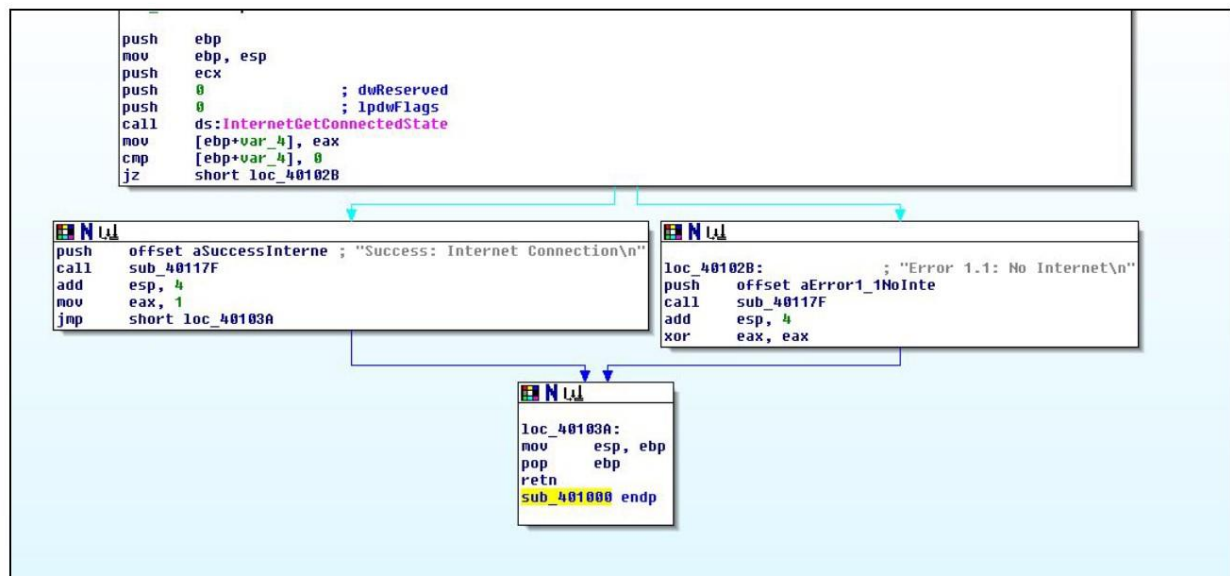
2. SEZIONI DEL FILE MALWARE

Dall'analisi di CFFexplorer prima e ExeinfoPE poi, abbiamo constatato che l'eseguibile si compone di tre **SEZIONI** principali:

- .text: che contiene le istruzioni da far eseguire alla CPU all'avvio del file, ovvero contiene tutte le righe di codice
- .rdata: che contiene le informazioni sulle librerie e le funzioni importate ed esportate (kernel32 e wininet)
- .data: che contiene le variabili globali del codice, che devono essere disponibili per l'accesso da qualsiasi funzione interna

Il file quindi contiene quasi tutte le comuni sezioni rinvenibili nell'header di un eseguibile PE.

ASSEMBLY



3. COSTRUTTI NOTI

In riferimento alla figura in alto possiamo identificare:

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

Questa tripletta iniziale non è che la **creazione dello stack**. Ritroviamo infatti gli stack pointer EBP (Extendend Base Pointer), ESP (Extended Stack Pointer) e ECX che sono tutte voci di registro general purpose per inizializzare una funzione, ovvero ogni chiamata di funzione crea uno stack e queste sono le righe iniziali riferite per l'appunto alla creazione del suddetto stack. In particolare “push ebp” inserisce un il pointer alla base dello stack, “mov ebp, esp” inserisce un pointer in cima allo stack appena creato e “push ecx” inserisce un registro ecx nello stack.

```
push    0           ; dwReserved
push    0           ; lpdwFlags
```

Questi due “push 0” creano uno spazio vuoto nello stack riservato ai valori “dwreserved” e “lpdwflags” di cui è ignoto l'utilizzo. Il secondo probabilmente è un puntatore che riceve info su un set di flag.

```
call    ds:InternetGetConnectedState
```

Questa è una chiamata di funzione, e in particolare una chiamata alla libreria wininet.dll per verificare se è disponibile una connessione ad internet.

```

mov     [ebp+var_4], eax
cmp     [ebp+var_4], 0
jz      short loc_40102B

```

Le righe soprastanti includono un “mov” che copia il valore del registro eax dentro un altro valore [ebp+var_4], e un “cmp” insieme a un “jz” identificabili come un **costrutto if**. In particolare “cmp” compara il valore sorgente 0 al valore destinazione contenuto nel registro [ebp+var_4] e in base al risultato “jz” salta alla locazione di memoria specificata. In altre parole cmp effettua un’operazione aritmetica simile alla sottrazione (sub) senza modificare gli operandi, ma modificando le flag ZF (Zero Flag) e CF (Carry Flag).

Per chiarire: se nel <cmp destinazione, sorgente> la sorgente è uguale alla destinazione si avrà una sottrazione tra numeri uguali e il risultato sarà 0, dunque ZF sarà uguale a 1.

In questo caso l’istruzione “jz” controlla se ZF è vera quindi se ZF=1, e salta alla locazione di memoria indicata se questa condizione è verificata.

Questo costrutto if segna l’inizio di un **ciclo**.

```

loc_40102B:                ; "Error 1.1: No Internet\n"
push     offset aError1_1NoInte
call     sub_40117F
add      esp, 4
xor      eax, eax

```

Se ZF=1, il salto di jz ci porta qui dove notiamo un’istruzione push sullo stack di un errore (print di errore di connessione), una chiamata “call” a una funzione sconosciuta e un’operazione “add” di somma di un valore 4 al registro esp, per poi chiudere con un <xor eax, eax> che inizializza a 0 il registro eax, quindi pulisce il valore per ricominciare il ciclo.

```

push     offset aSuccessInterne ; "Success: Internet Connection\n"
call     sub_40117F
add      esp, 4
mov      eax, 1
jmp      short loc_40103A

```

Se ZF=0, il codice continua qui con un “push” di un messaggio print di successo di connessione, poi anche qui viene effettuata un’operazione “add” del valore 4 al registro esp, l’istruzione “mov” del valore 1 al registro eax e infine il “jmp” a un’altra locazione di memoria.

```
loc_40103A:  
mov     esp, ebp  
pop     ebp  
retn  
sub_401000 endp
```

L'ultimo jmp conduce a questa locazione di memoria che chiude il ciclo: il "mov" va a spostare il l'ebp sullo stack e infine il "pop" lo elimina. "retn" è un ritorno alla funzione chiamante e "endp" termina la funzione chiamata.

4. IPOTESI COMPORTAMENTO

In conclusione questo codice assembly cerca di ottenere una verifica di connessione avvenuta. È in sostanza una funzione della libreria wininet.dll chiamata da un'altra funzione principale (chiamante) che va a fare un controllo su determinati valori inseriti in delle variabili per capire se esiste ed è possibile stabilire una connessione ad internet, ovvero capire se la macchina è online o meno. Nel caso di alcuni codici malevoli, questa è una prerogativa per riuscire ad ottenere connessioni non autorizzate a server remoti o scaricare file indesiderati o pericolosi.