



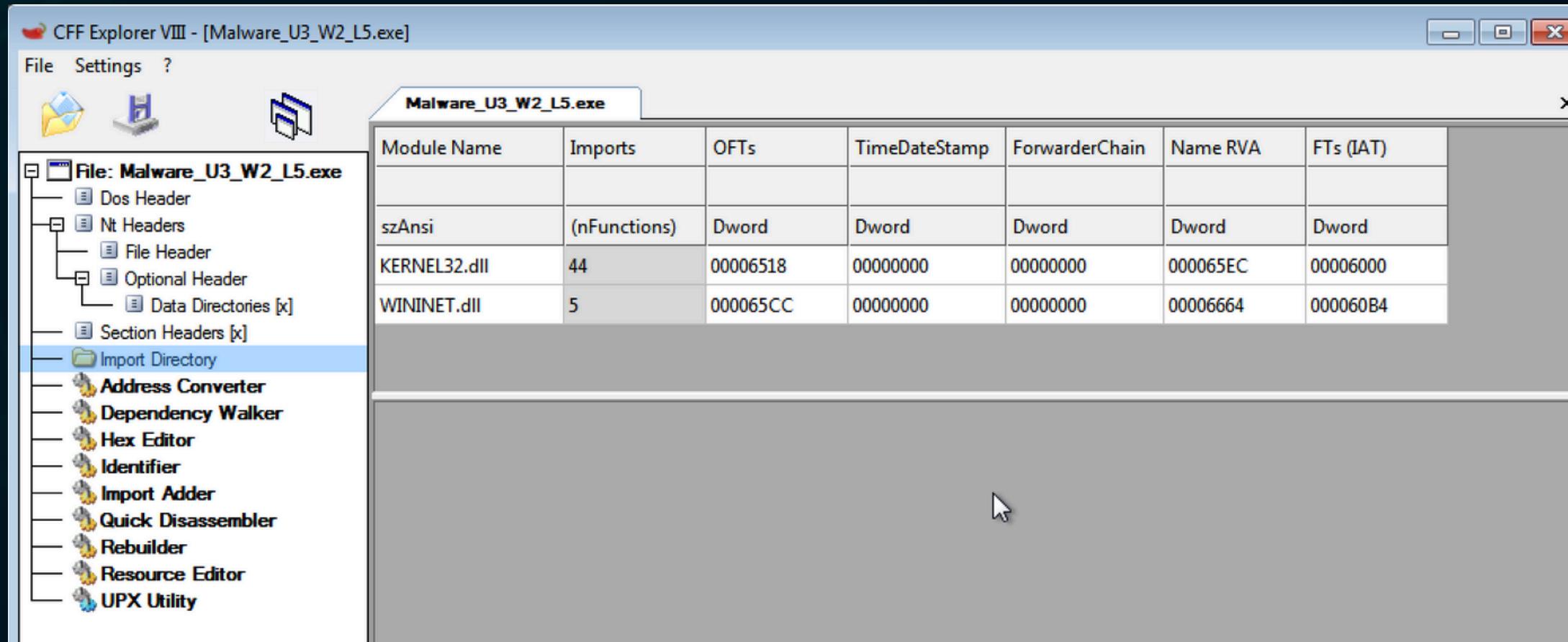
Analisi del malware del file “Malware_U3_W2_L5”

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, rispondete 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. Quali librerie vengono importate dal file eseguibile?



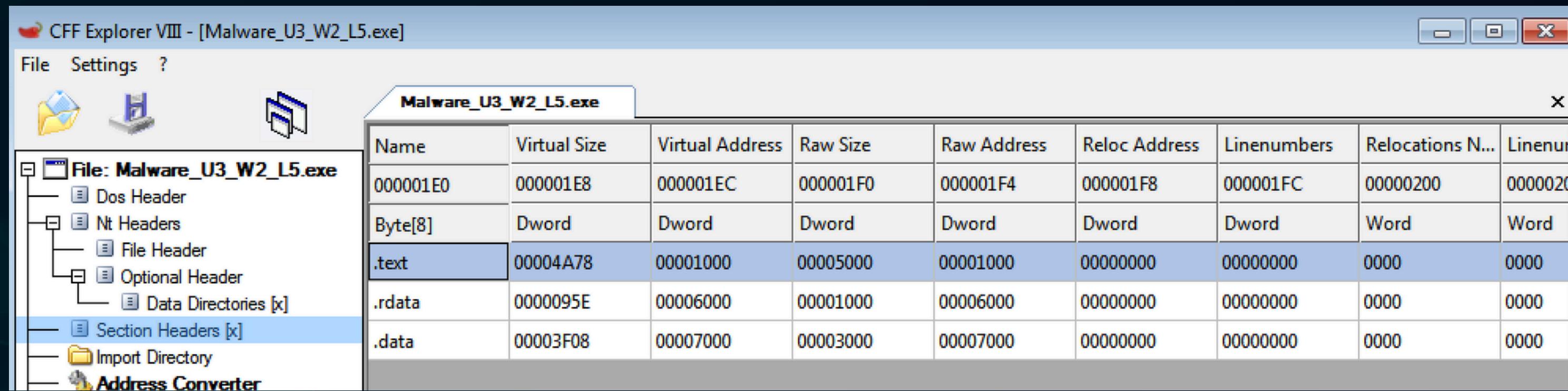
Dalle analisi, utilizzando **CFF Explorer**, si nota che le librerie presenti sono:

- KERNEL32.dll
- WININET.dll

KERNEL.dll è una libreria di Windows e fornisce funzioni essenziali per il sistema operativo, come ad esempio, la gestione della memoria, dei processi e dei file.

WININET.dll è una libreria che permette alle applicazioni di comunicare tramite Internet, gestendo protocolli quali HTTP, HTTPS e FTP.

2. Quali sono le sezioni di cui si compone il file eseguibile del malware?



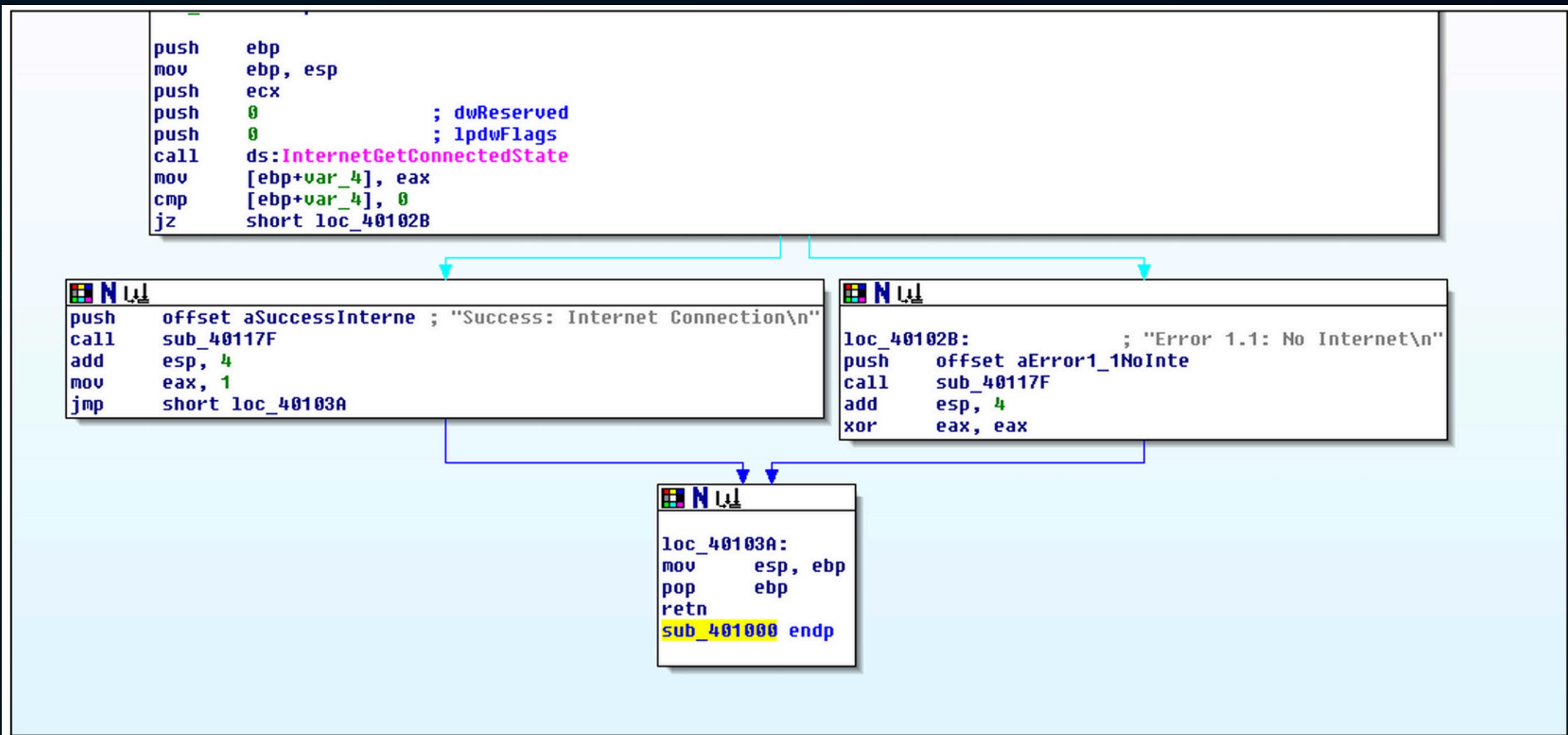
The screenshot shows the CFF Explorer VIII interface with the file "Malware_U3_W2_L5.exe" open. On the left, a tree view shows the file structure with nodes for Dos Header, Nt Headers, File Header, Optional Header, Data Directories, Section Headers, Import Directory, and Address Converter. The "Section Headers" node is selected. On the right, a table displays the section details:

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenum
000001E0	000001E8	000001EC	000001F0	000001F4	000001F8	000001FC	00000200	00000200
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word
.text	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000

Come possiamo notare, le sezioni di cui si compone sono 3:

- “**.text**”; contiene il codice eseguibile; qui si trovano le istruzioni delle funzioni e dei metodi.
- “**.rdata**”; qui sono contenuti dati in sola lettura, stringhe di testo, variabili numeriche, dati che non necessitano alcuna modifica.
- “**.data**”; qui si trovano dati che possono essere modificati durante l'esecuzione, quali variabili globali ed altri dati.

3. Identificare i costrutti noti (creazione dello stack, eventuali cicli, altri costrutti)



[Figura di riferimento]

push	ebp
mov	ebp, esp



Questa parte indica la creazione dello stack

Qui si può dedurre che ci sia un ciclo IF



cmp	[ebp+var_4], 0
jz	short loc_40102B

mov	esp, ebp
pop	ebp



Questa parte indica la chiusura dello stack

4. Ipotizzare il comportamento della funzionalità implementata

Dall'analisi del codice, si è giunti alla conclusione che esso controlli l'eventuale connettività ad internet della macchina.

```
push    ecx
push    0          ; dwReserved
push    0          ; lpdwFlags
call    ds:InternetGetConnectedState
mov    [ebp+var_4], eax
cmp    [ebp+var_4], 0
jz     short loc_40102B

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

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

In caso di controllo negativo questa sarà la parte eseguita dal codice

Mentre questa parte viene eseguita in caso di controllo positivo

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

push	ebp	Si punta alla base del stack
mou	ebp, esp	Si copia il contenuto di esp[che punta alla cima dello stack] in ebp

Creazione di una variabile nello stack

push	ecx	
push	0	
push	0	
		; dwReserved
		; lpdwFlags

Si inserisce lo zero nello stack e si riserva per eventuali utilizzi futuri

In questo caso possiamo notare che il commento indica il tipo di funzionalità, che sembrerebbe essere un puntatore a delle segnalazioni

Chiamata alla funzione InternetGetConnectedState

Copia del valore di eax nella variabile

```
call  
mov  
cmp  
jz
```

```
ds:InternetGetConnectedState  
[ebp+var_4], eax  
[ebp+var_4], 0  
short loc_40102B
```

Qui si fa un controllo del tipo `i==0`, dove i è la variabile `[ebp+var_4]`

Nel caso in cui il valore della variabile sia uguale a 0 allora si fa un salto alla locazione `40102B`

Questo push riguarda la funzione `printf` che appunto stamperà "No Internet" in caso di esito negativo

Chiamata di una subroutine all'indirizzo di memoria 40117F, che probabilmente riguarda funzioni sulla connettività

Vengono aggiunti 4 byte al puntatore esp per la pulizia dello stack

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

Inizializzazione di eax a 0

Stessa chiamata all **sotto-routine** all'indirizzo specificato

Abbiamo nuovamente un push della funzione **printf**, in questo caso per indicare che c'è connessione a internet

Anche in questo caso si fa **pulizia** dello stack

si copia il valore di **1** in **eax**

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

Salto alla locazione
40103A

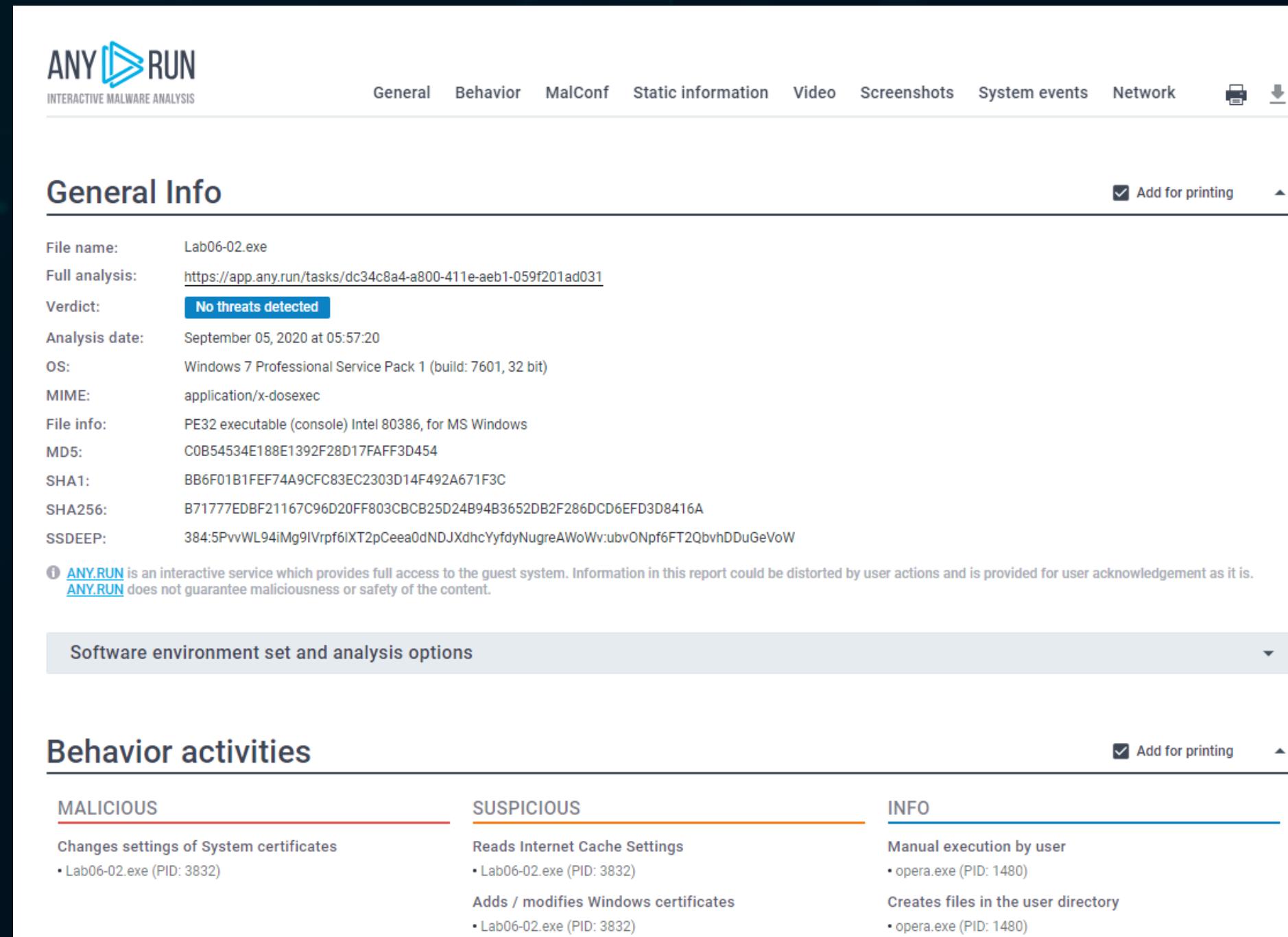
Avviene la **rimozione** del puntatore ebp tramite l'istruzione **pop**

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

Chiusura della subroutine

Copiamo il valore del puntatore ebp in esp

Grazie all'**MD5** ricavato da CFF Explorer, si può anche verificare su siti come [any.run](#) e [virustotal](#) la natura del virus, e le attività sospette che lo stesso può fare. Andiamo a vedere nel dettaglio:



General Info

File name: Lab06-02.exe
Full analysis: <https://app.any.run/tasks/dc34c8a4-a800-411e-aeb1-059f201ad031>
Verdict: No threats detected
Analysis date: September 05, 2020 at 05:57:20
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
MIME: application/x-dosexec
File info: PE32 executable (console) Intel 80386, for MS Windows
MD5: C0B54534E188E1392F28D17FAFF3D454
SHA1: BB6F01B1FEF74A9CFC83EC2303D14F492A671F3C
SHA256: B71777EDBF21167C96D20FF803CBCB25D24B94B3652DB2F286DCD6EFD3D8416A
SSDEEP: 384:5PvvWL94IMg9IVrp6lXT2pCeea0dNDJXdhcYyfdyNugreAWoWv:ubvONpf6FT2QbvhDDuGeVoW

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
Changes settings of System certificates • Lab06-02.exe (PID: 3832)	Reads Internet Cache Settings • Lab06-02.exe (PID: 3832) Adds / modifies Windows certificates • Lab06-02.exe (PID: 3832)	Manual execution by user • opera.exe (PID: 1480) Creates files in the user directory • opera.exe (PID: 1480)

Secondo il report di [AnyRun](#), salvo alcuni comportamenti “malicious”, il malware non è una particolare minaccia.

38 / 72 security vendors and no sandboxes flagged this file as malicious

b71777edbf21167c96d20ff803cbcb25d24b94b3652db2f286dc6efd3d8416a
Malware_U3_W2_L5.exe

Size 40.00 KB | Last Modification Date 8 minutes ago | EXE

Community Score 38 / 72

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

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 7

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label	Threat categories	Family labels	
trojan.r002c0pdm21	trojan	r002c0pdm21	
Security vendors' analysis			
Alibaba	Trojan:Win32/Generic.2cc376c1	AliCloud	Backdoor
Antiy-AVL	Trojan/Win32.BTSGeneric	Avast	Win32:PUP-gen [PUP]
AVG	Win32:PUP-gen [PUP]	Bkav Pro	W32.Common.362CBAB4
Cylance	Unsafe	DeepInstinct	MALICIOUS
DrWeb	Trojan.MulDrop7.63090	Elastic	Malicious (high Confidence)
ESET-NOD32	Win32/Agent.WOO	Fortinet	W32/Agent.WOO!tr
GData	Win32.Trojan.Agent.DZ3C1W	Google	Detected
Gridinsoft (no cloud)	Ransom.Win32.Wacatac.oa!s1	Ikarus	Trojan.Win32.Agent

VirusTotal ci dice che molto probabilmente siamo davanti ad un trojan, a seguito di verifiche con i più famosi antivirüs



Matteo Leoni
Rosario Giaimo
Stefano Di Prospero
Lorenzo Moro
Gianmarco Mazzoni

GRAZIE