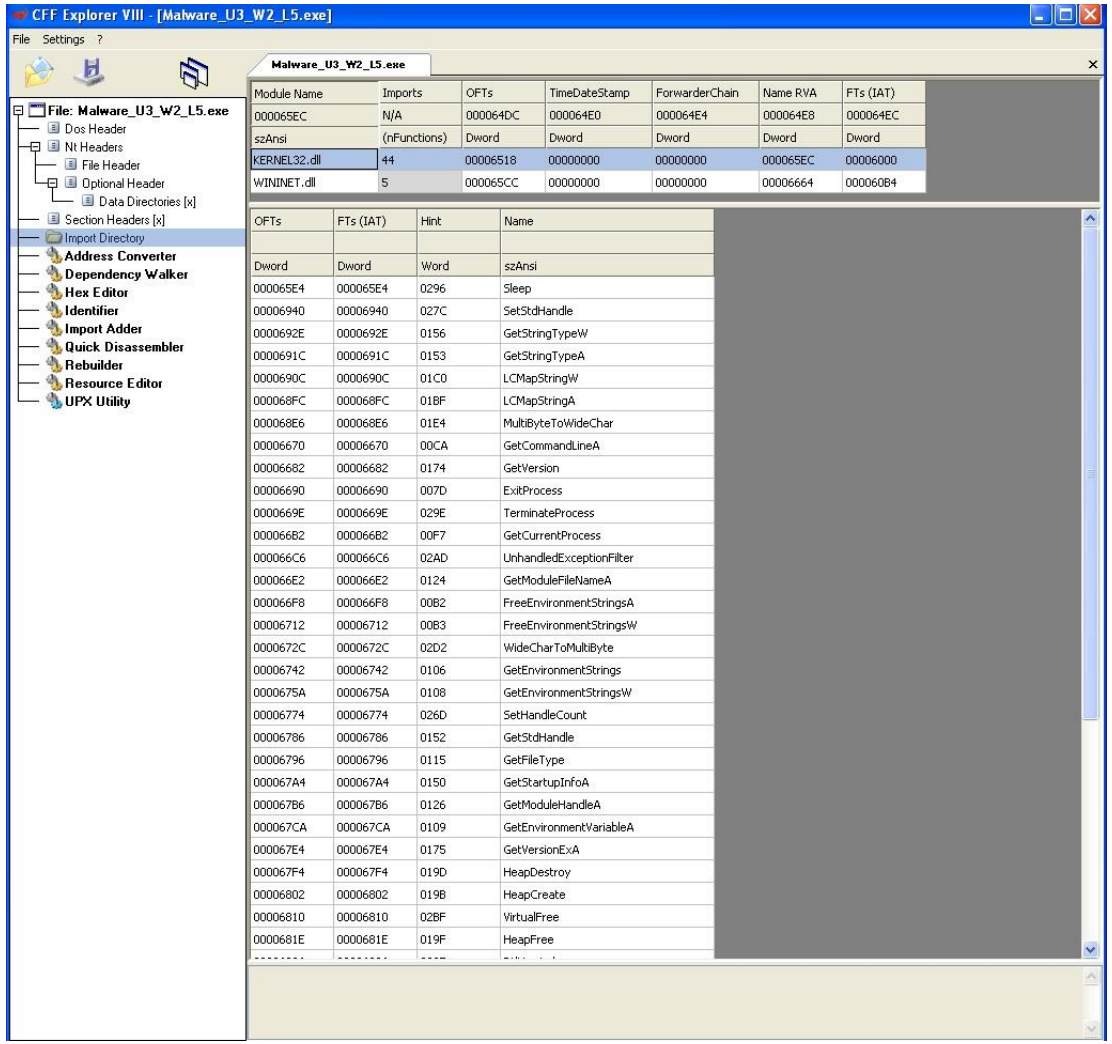
Progetto

Analisi Statica basica

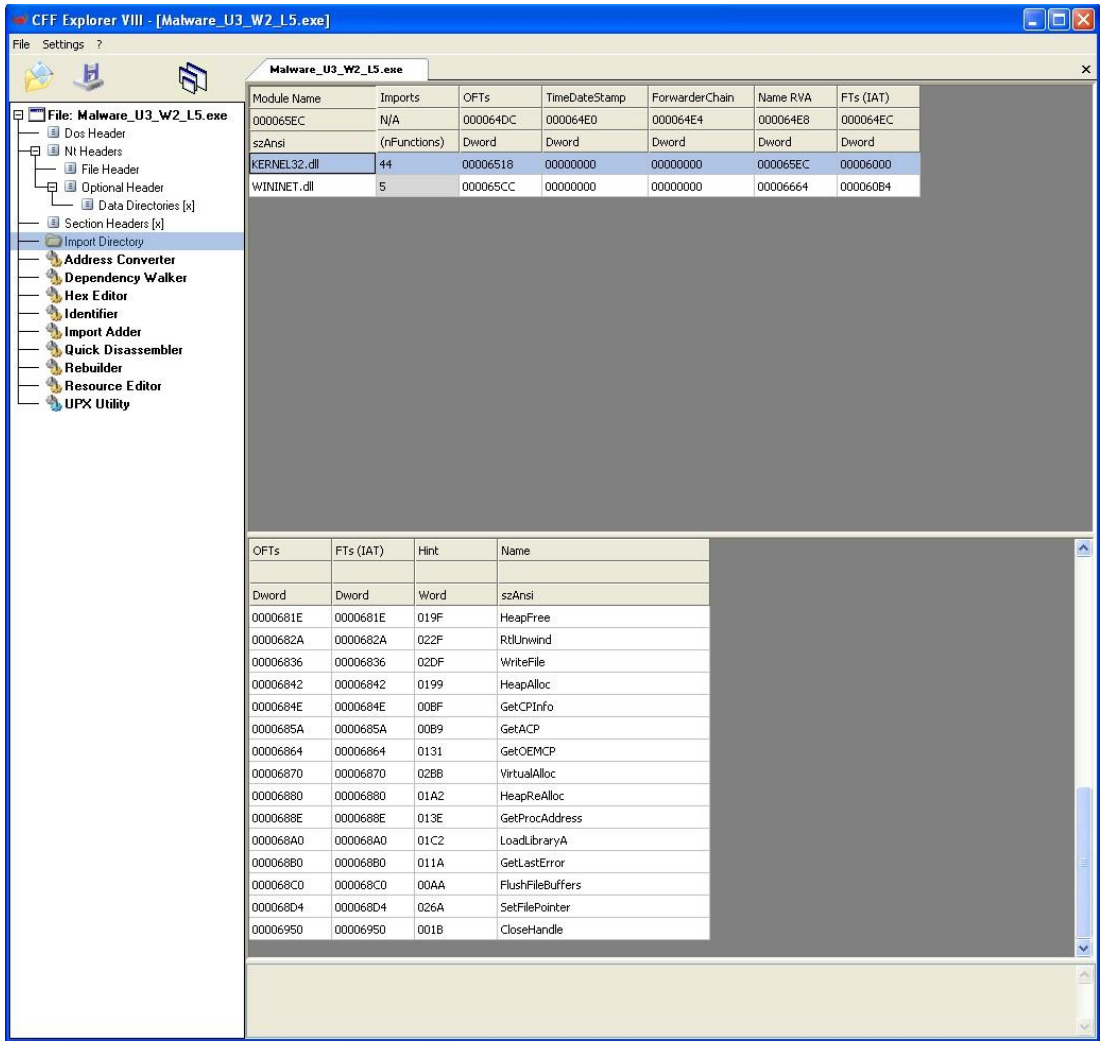
Malware_U3_W2_L5

Orlando Tangari



Libreria KERNEL32.DLL

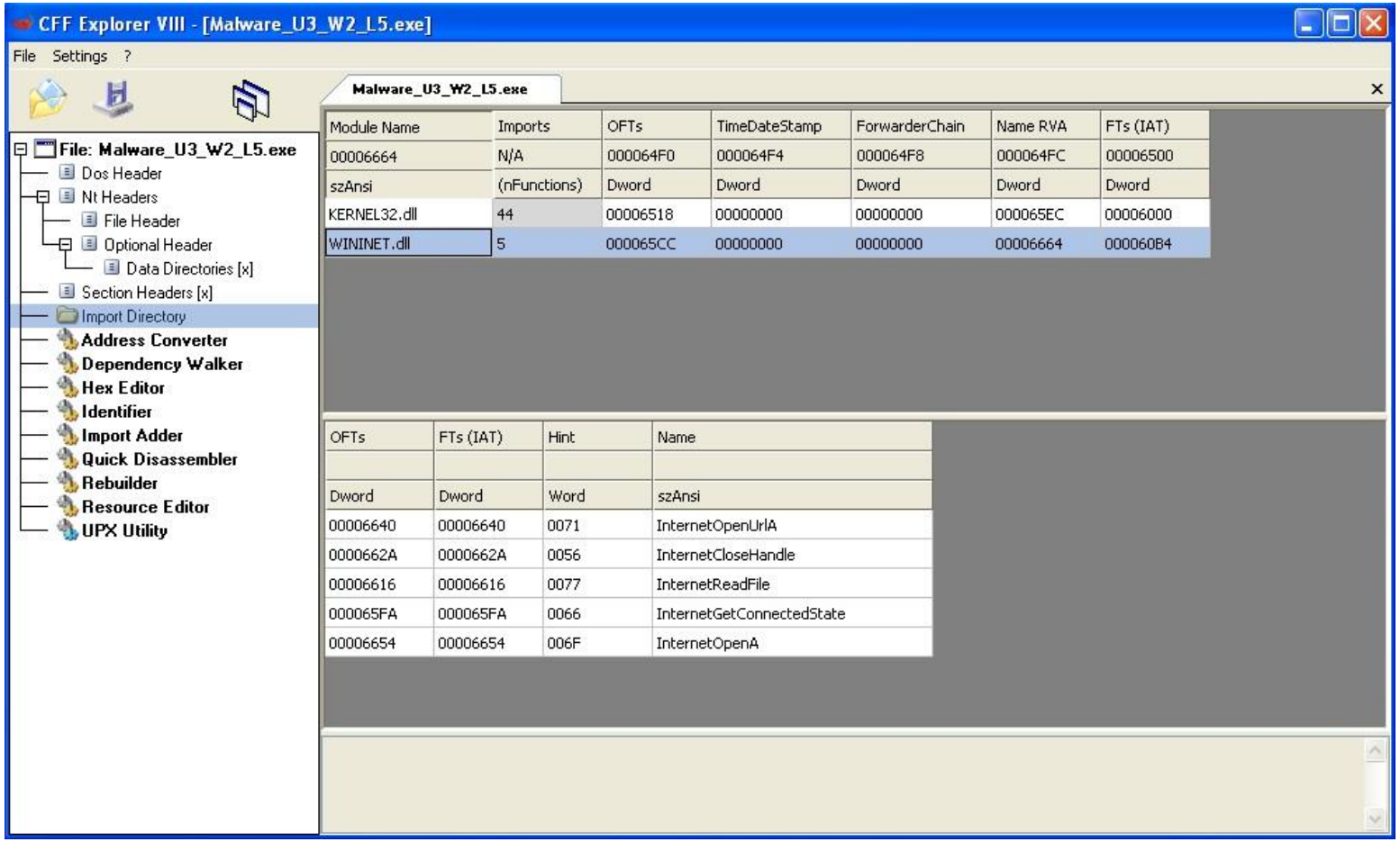
Libreria contenente le funzioni principali per interagire con il sistema operativo.



Libreria KERNEL32.DLL

Libreria contenente le funzioni principali per interagire con il sistema operativo.

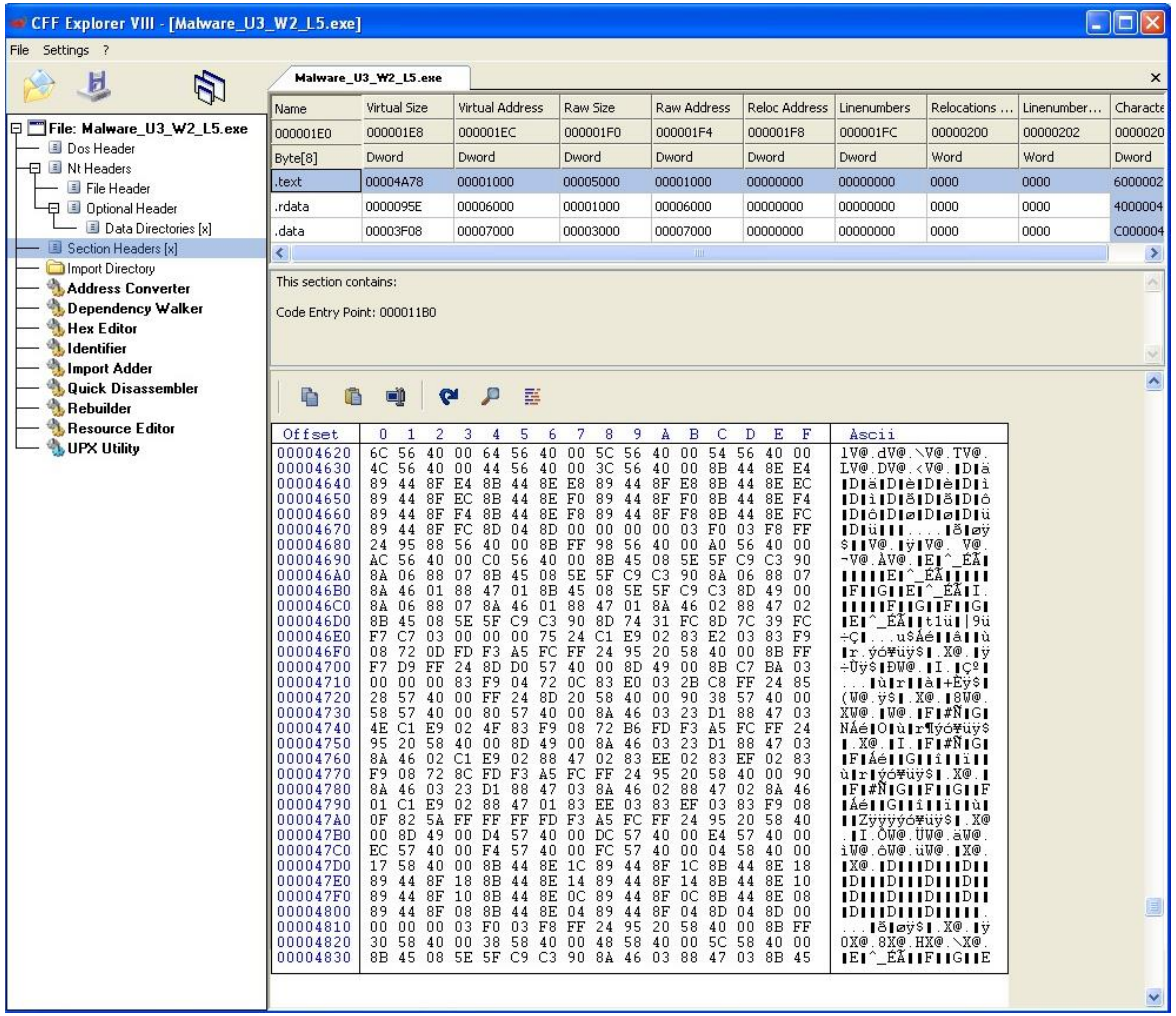
Librerie importate dal malware (part. 1)



Libreria WININET.dll

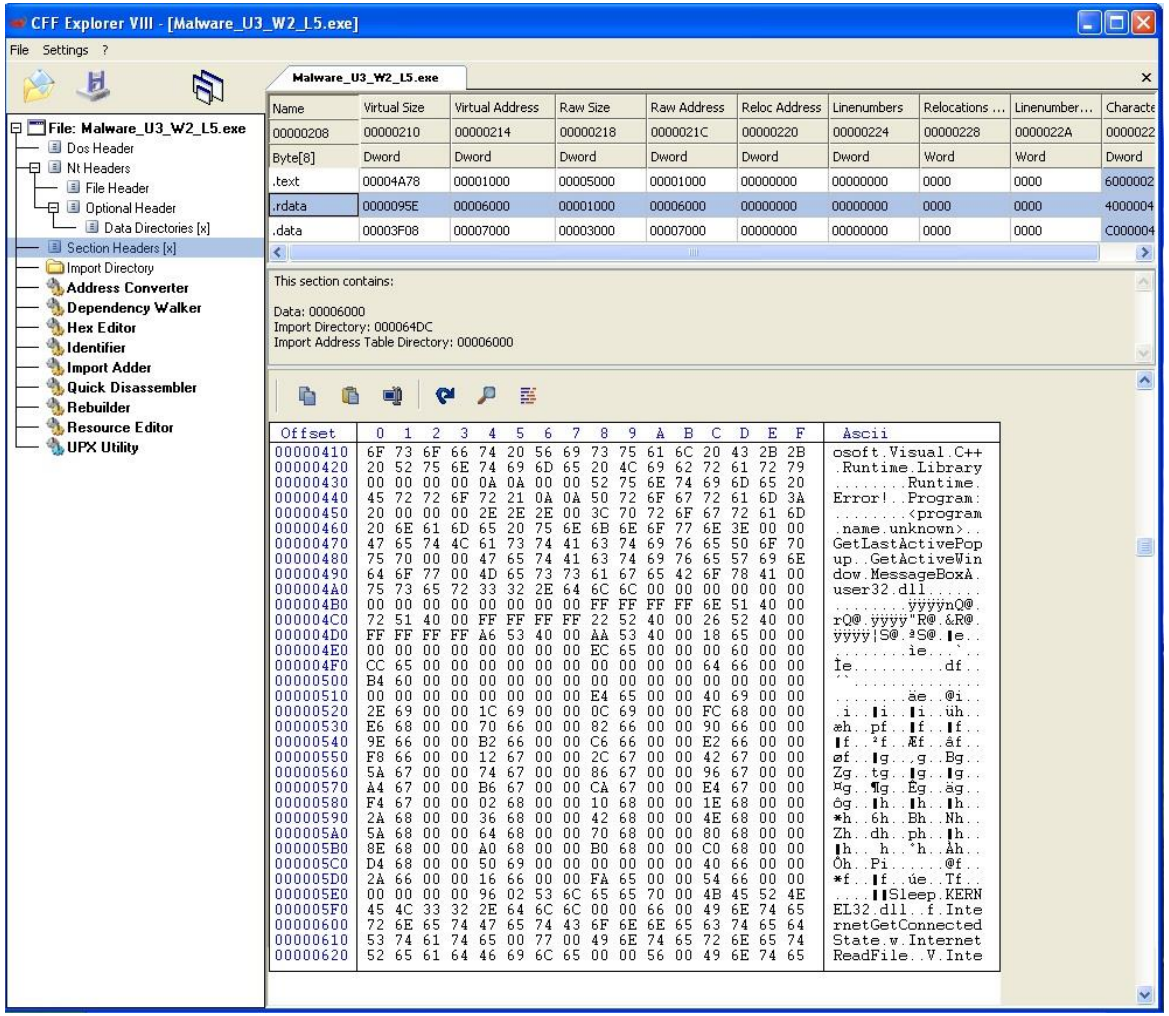
Libreria contenente le funzioni per implementare alcuni protocolli di rete come:
HTTP, FTP, NTP.

Librerie importate dal malware (part. 2)



Sezione .text

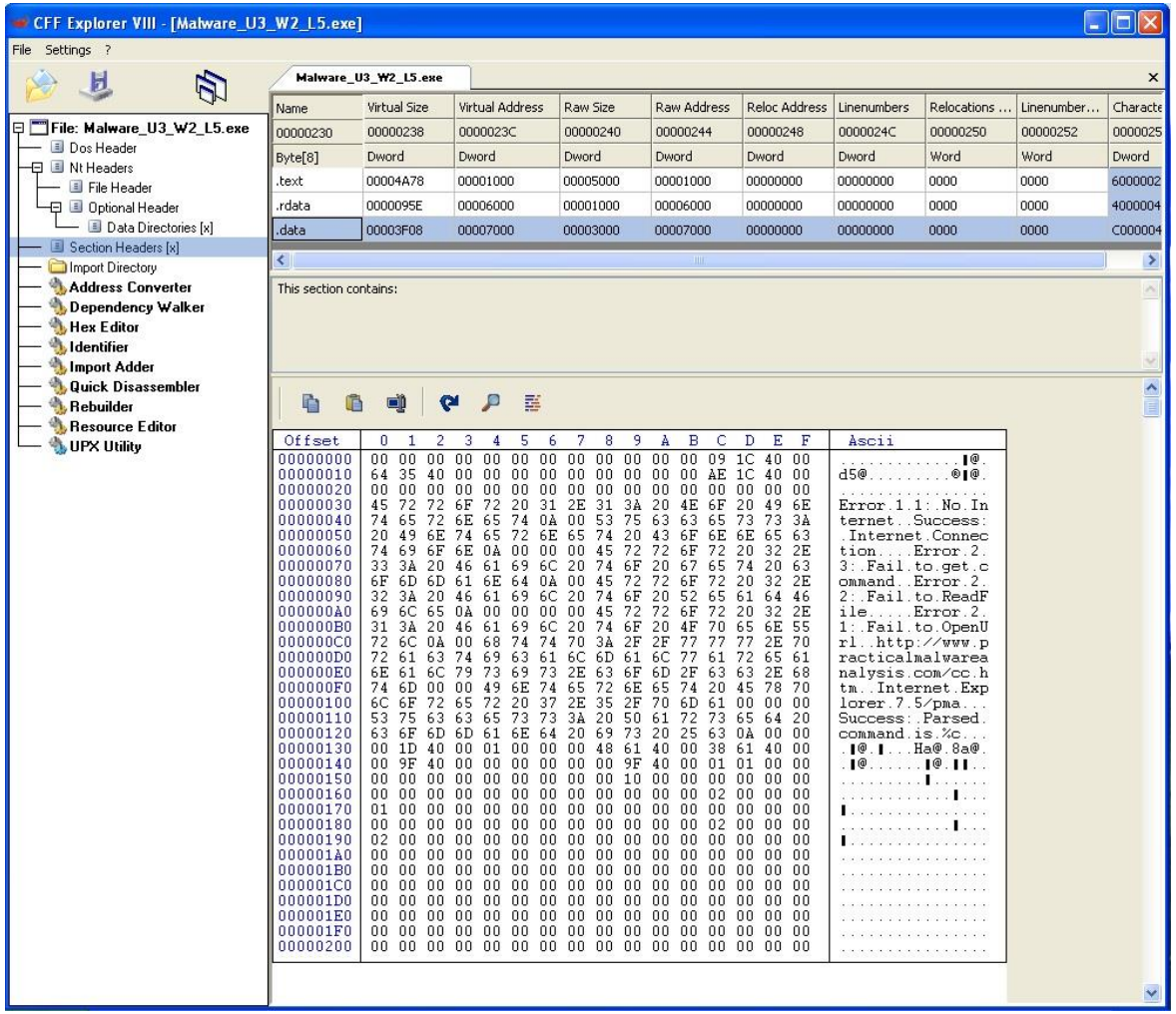
Sezione che contiene le righe di codice che la CPU eseguirà una volta che il software sarà avviato. Unica sezione di un file eseguibile che viene eseguita dalla CPU.



Sezione .rdata

Sezione che include le informazioni delle librerie e le funzioni importate ed esportate dall'eseguibile.

Sezioni in cui si compone il malware (part. 1)



Sezione .data

Sezione contenente tipicamente dati/variabili globali del programma eseguibile che devono essere eseguibili da qualsiasi parte del programma.

Sezioni in cui si compone il malware (part. 2)

Dall’analisi statica basica, si è giunti alla conclusione che, il malware Malware_U3_W2_L1, crei un oggetto sulla macchina vittima per stabilire una connessione di tipo: HTTP, o FTP, o NTP.

Considerazioni finali

Progetto

Assebly X86

Identificazione costrutti noti
Ipotesi di comportamento della funzione implementata

Orlando Tangari

```
push    epb
mov     epb,  esp
push    exc
push    0                       ; dwReserved
push    0                       ; lpdwFlags
call    ds:InternetGetConnectedState
jz      short loc_40102B
```

Creazione stack

Chiamata di funzione
Parametri passati
sullo stack tramite
istruzioni push

```
push    offset a SuccessInternet ;  ‘‘Success: Internet Internet Connection\n’’
call    sub_40105F
add     esp, 4
mov     eax, 1
jmp     short loc_40103A
```

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

```
loc_40103A:
mov     esp,  ebp
pop     ebp
retrn
Sub_401000
```

Identificazione costrutti noti

Funzionalità implementata all’interno del malware facile da identificare. Il malware chiama la funzione InternetGetConnectedState.

Pseudocodice C:

```
state = internetgetconnectedstate (par1,0,0);

If (state(=0) printf (‘‘Active connection’’);
 Else return 0;
```

Ipotesi di comportamento della funzione implementata