Analisi codice Assembly

```
text:00401000                   push    ebp
text:00401001                   mov     ebp, esp
```

Creazione della stack

```
text:00401003                   push    ecx
text:00401004                   push    0                       ; dwReserved
text:00401006                   push    0                       ; lpdwFlags
text:00401008                   call    ds:InternetGetConnectedState
```

Viene chiamata la funzione, i parametri vengono passati sullo stack tramite le istruzioni push

```
text:00401011                   cmp     [ebp+var_4], 0
text:00401015                   jz      short loc_40102B
```

Condizione del ciclo if e salto condizionale

```
text:00401017                   push    offset aSuccessInterne ; "Success: Internet Connection\n"
text:0040101C                   call    sub_40105F
text:00401021                   add     esp, 4
text:00401024                   mov     eax, 1
text:00401029                   jmp     short loc_40103A
text:0040102B ; ---------------------------------------------------------------------------
```

Il malware chiama la funzione internetgetconnectedstate e ne controlla con un «if» il valore di ritorno.

Se la funzione ritorna un valore diverso da 0, viene stampato a schermo “Success...”.

C

```c
connected = internetgetconnectedstate(par1,0,0);

if (connected != 0) {
  printf("Success: Internet Connection\n");
}
```