

Creazione dello stack

Chiamata di funzione: i parametri vengono passati sullo stack mediante le istruzioni push

Ciclo IF

♦ .text:00401000
♦ .text:00401001
♦ .text:00401003
♦ .text:00401004
♦ .text:00401006
♦ .text:00401008
♦ .text:0040100E
♦ .text:00401011
♦ .text:00401015
♦ .text:00401017
♦ .text:0040101C
♦ .text:00401021
♦ .text:00401024
♦ .text:00401029
♦ .text:0040102B
♦ .text:0040102B

```
push    ebp
mov     ebp, esp
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
push    offset aSuccessInterne
call    sub_40105F
add     esp, 4
mov     eax, 1
jmp     short loc_40103A
```

L'implementazione all'interno del malware è abbastanza facile da individuare. Esso invoca la funzione internetgetconnectedstate e valuta il suo valore di ritorno tramite un'istruzione "if". Se il valore di ritorno della funzione è diverso da zero, indica la presenza di una connessione attiva.

Pseudocodice C:

```
state = internetgetconnectedstate
```

```
(par1,0,0); If (state !=0) printf ("Active connection");  
Else return 0;
```