Costrutti C - Assembly x86

Istruzione

```
.text: 00401000
                                            epb
                                  push
                                                               Creazione stack
.text: 00401001
                                            epb,
                                  mov
                                                  esp
.text: 00401003
                                  push
                                            exc
                                                                                    Chiamata di funzione
.text: 00401004
                                  push
                                           0
                                                              ; dwReserved
                                                                                    Parametri passati
.text: 00401006
                                                              ; lpdwFlags
                                  push
                                            0
                                                                                    sullo stack tramite
.text: 00401008
                                  call
                                            ds:InternetGetConnectedState
                                                                                    istruzioni push
.text: 0040100E
                                            [ebp+var 4], eax
                                  mov
.text: 00401011
                                            [ebp+var 4], 0
                                  cmp
                                                                       Ciclo IF
.text: 00401015
                                  įΖ
                                            short loc_40102B
.text: 00401017
                                  push
                                            offset a SuccessInternet; "Success: Internet Internet Connection\n"
                                            sub_40105F
.text: 0040101C
                                  call
.text: 00401021
                                  add
                                            esp, 4
.text: 00401024
                                            eax, 1
                                  mov
.text: 00401029
                                            short loc 40103A
                                  jmp
.text: 0040102B;
```

.text: 0040102B

Funzionalità implementata all'interno del malware facile da identificare. Il malware chiama la funzione InternetGetConnectedState e controlla, con un if, il valore di ritorno. Se il valore return è ≠ da 0, significa che c'è una connessione attiva.

Pseudocodice C:

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

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