Il seguente codice è stato estratto da un malware.
Identificare i costrutti noti e spiegarli mediante una breve descrizione.

- **CREAZIONE STACK:**
    - 00401000: push ebp - Crea il valore ebp, creando lo stack
    - 00401001: mov ebp, esp - Sposta il valore esp su ebp
- **CHIAMATA DI FUNZIONE:**
    - 00401003: push ecx - Crea il valore ecx sullo stack
    - 00401004: push 0 - Crea il valore 0 sullo stack come primo parametro (var 004)
    - 00401006: push 0 - Crea il valore 0 sullo stack come secondo parametro (var 006)
    - 00401008: call ds:InternetGetConnectedState - Chiama la funzione "InternetGetConnectedState"
    - 0040106E: mov [ebp+var_4], eax - Sposta il valore di eax nella variabile ebp+var_4 salvata nello stack
- **CICLO IF:**
    - 00401011: cmp [ebp+var_4], 0 - Confronta il valore di ebp+var_4 con 0
    - 00401015: jz short loc_406102B - Salta all'indirizzo loc_406102B se i due valori sono uguali
    - 00401017: push offset aSuccessInterne - Crea l'indirizzo della stringa "Success: Internet Connection\n" sullo stack
    - 0040101C: call sub_40105F - Chiama l'indirizzo di memoria "sub_40105F" (non presente nel codice)
    - 00401021: add esp, 4 - Aggiunge 4 all'indirizzo di memoria esp
    - 00401024: mov eax, 1 - Sposta il valore 1 nel registro eax
    - 00401029: jmp short loc_461083A - Salta all'indirizzo loc_461083A
- **FINE CODICE:**
    - 0040102B