Virus in Assembly:

```
.text:00401000 push ebp |
.text:00401001 mov ebp, esp
.text:00401003 push ecx
.text:00401004 push 0        ; dwReserved
.text:00401006 push 0        ; lpdwFlags
.text:00401008 call ds:InternetGetConnectedState
.text:0040100E mov [ebp+var_4], eax
.text:00401011 cmp [ebp+var_4], 0
.text:00401015 jz short loc_40102B
.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:00401024 jmp short loc_40103A
.text:0040102B ; ----------
.text:0040102B
```

Virus codice convertito in C:

```c
#include <stdio.h>
#include <windows.h>

int main() {
    DWORD dwReserved = 0;
    DWORD lpdwFlags = 0;
    BOOL isConnected = InternetGetConnectedState(&dwReserved, &lpdwFlags);

    if (isConnected) {
        printf("Success: Internet Connection\n");
        return 1;
    }

    return 0;
}

```

Se si osserva il codice in C semplificandolo ma già leggendo l'assembly, si può capire che il virus fa una chiamata tramite internet.

"Il Virus potrebbe tranquillamente essere un Trojan/Backdoor"

Anche guardando la funzione "int main" si può capire che cerca qualcosa questo virus tramite la connessione trasferisce qualcosa.