ESERCIZIO S10L4

Avendo come codice:

```
.text:0040100      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     inc     eax, 1
.text:00401029     jmp     short loc_40103A
```

In questo programma possiamo notare che si tratta di un malware che controlla una connessione internet, nella linea 1011 e 1015, crea un ciclo che controlla l’esistenza di una connessione internet. Nel caso il flag sia uguale a 0, il ciclo si avvera e si esegue il ciclo e al compiersi da come messaggio di successa connessione.

Questo tratto di malware da idea a che possa essere un malware downloader o keylogger, dato che controlla la connessione ad internet, per poi probabilmente scaricare pacchetti, in caso di downloader, o caricare pacchetti, in caso di keylogger.