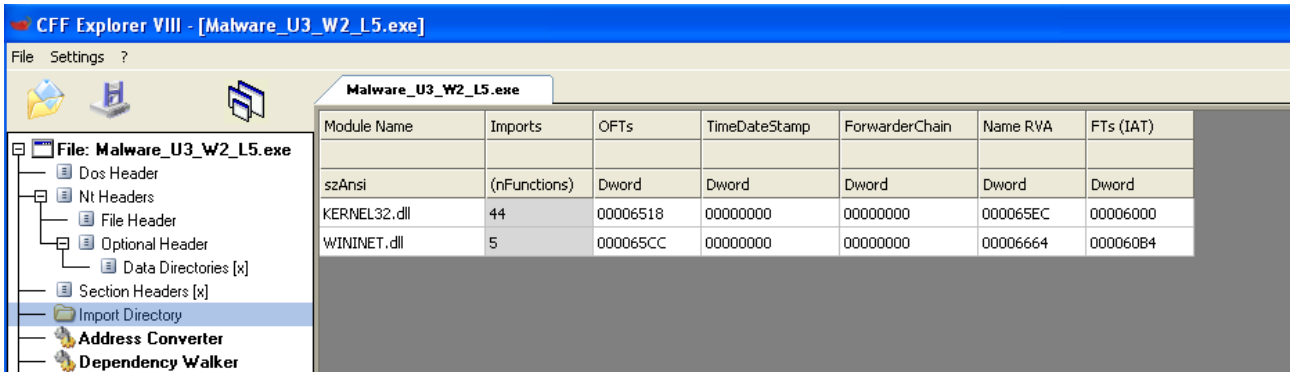
Report sett.10 Venerdi

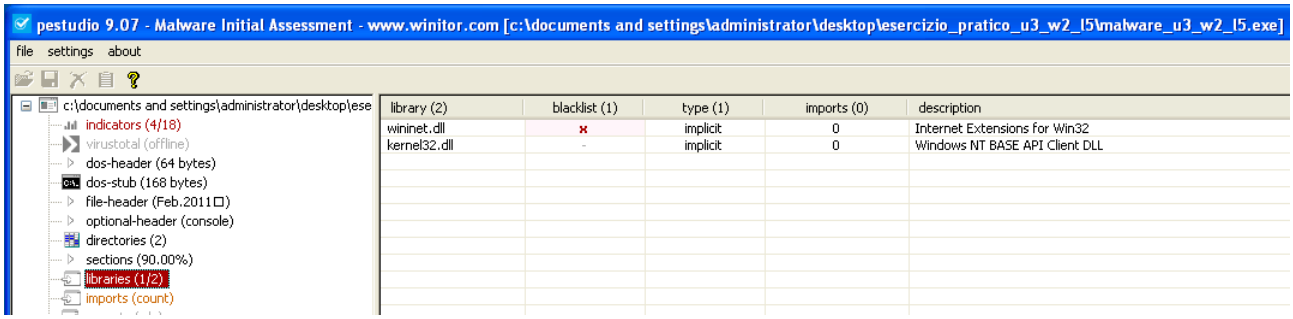
1. Librerie

Tool: CFF Explorer
Per controllare le librerie importate del file Malware_U3_W2_L5.exe possiamo utilizzare CFF Explorer, dove selezionando **Import Directory** ci mostra 2 librerie del file eseguibile: KERNEL32.dll e WININET.dll



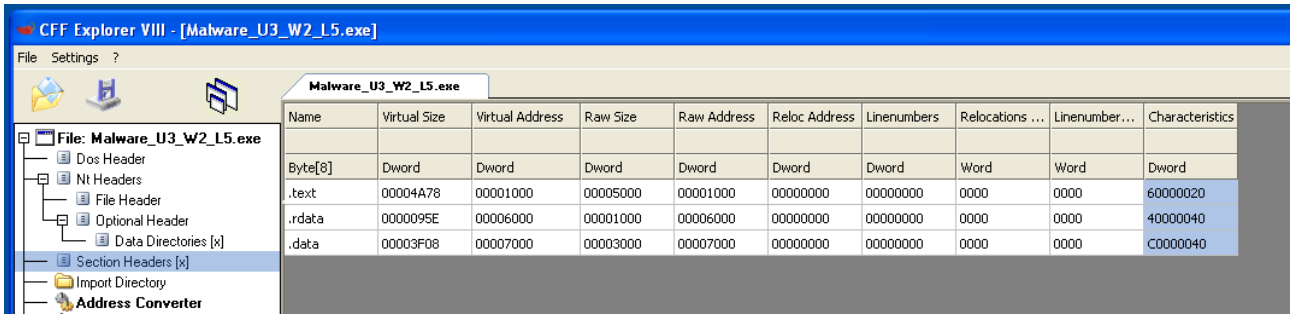
Tool: pestudio

lo stesso risultato otteniamo usando il Pestudio



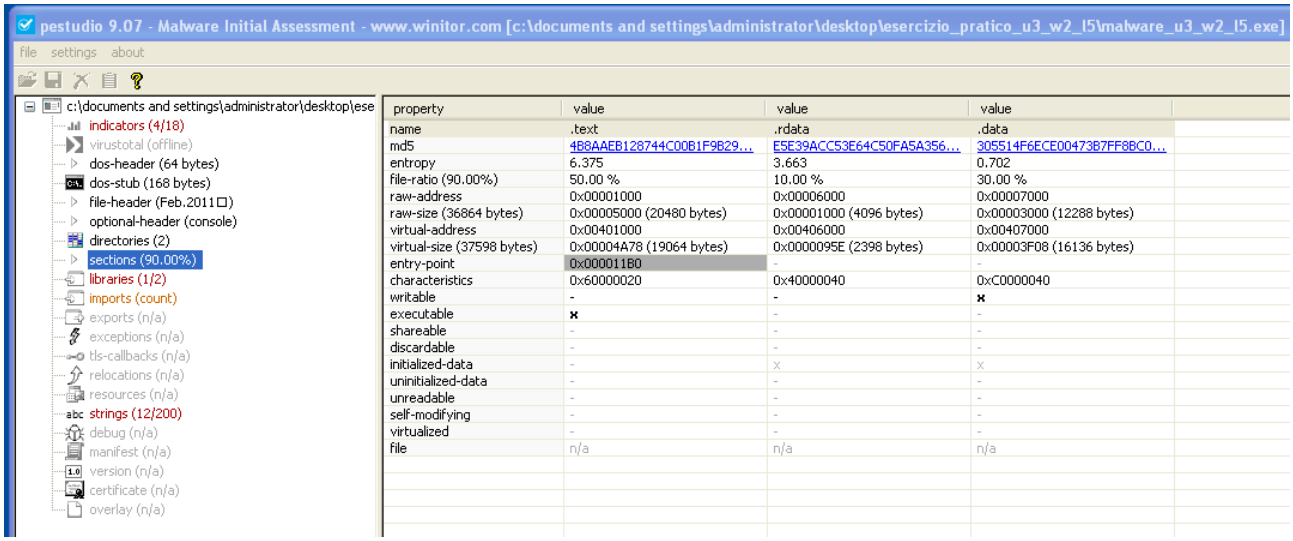
2. Sezioni

Tool: CFF Explorer
Utilizzando CFF Explorer possiamo controllare le sezioni del file, selezionando Section Headers che ci mostra 3 sezioni presenti dentro il file eseguibile: .text, .rdata e .data

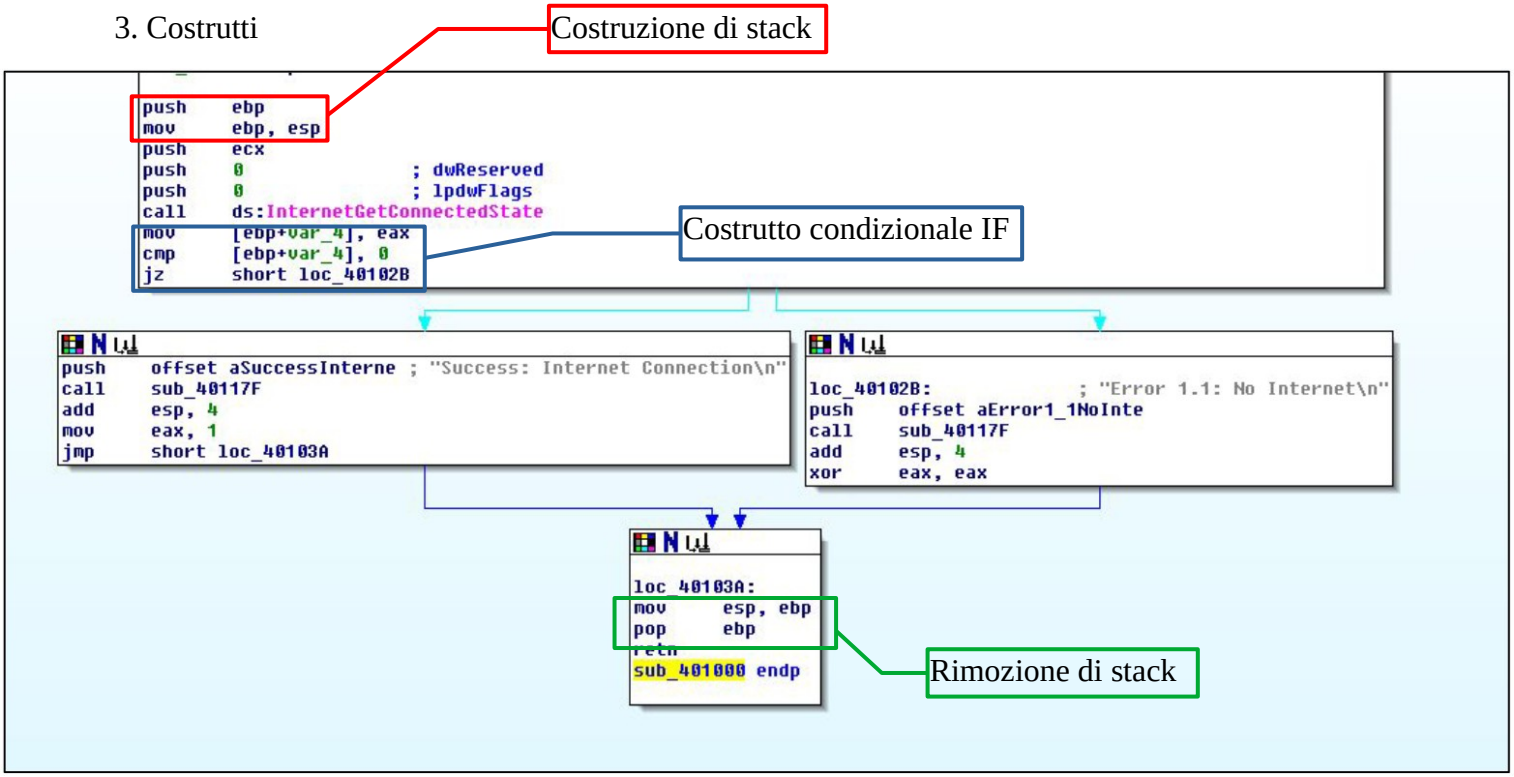


Tool: Pestudio

ancora una volta possiamo utilizzare il Pestudio per trovare le sezioni



3. Costrutti



push = push item (constant or register) to stack

pop = pop item from stack

esp, ebp = 32-bit register

call = transfer control

add = dest = dest+src

mov = copy src to dest

cmp = compare arg1 to arg2

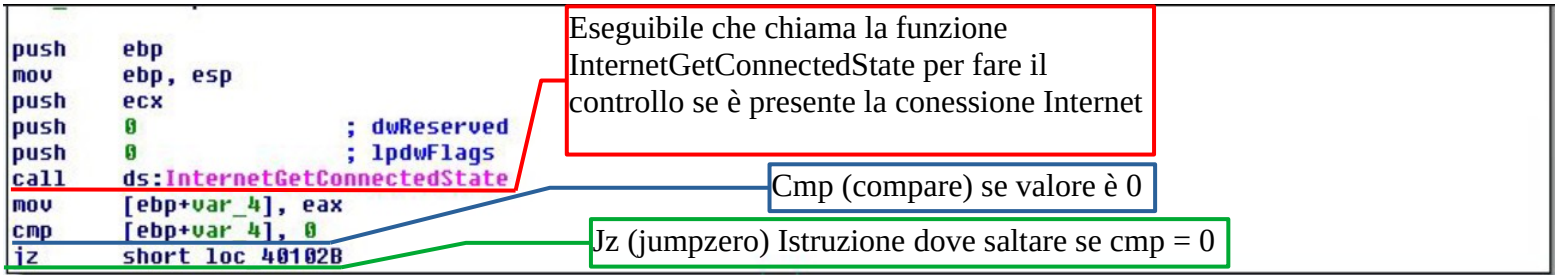
jmp = unconditional absolute jump

jz = jump to label if bits were set (“not zero”)

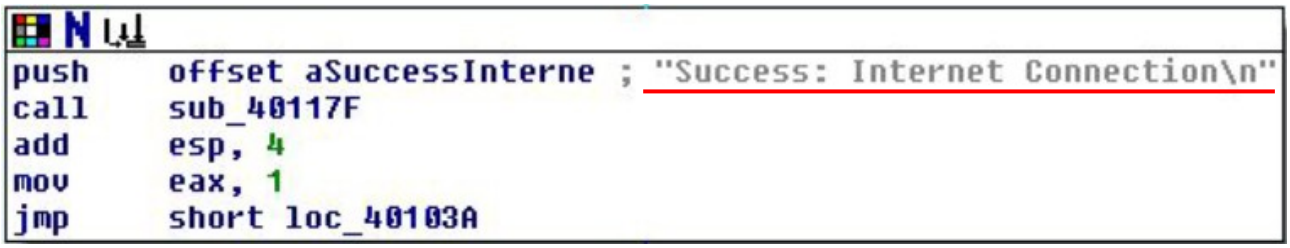
xor = dest = src ^ dest

retn = return address located on the stack

4. Ipotesi



Se il valore è diverso da 0 il jz viene saltato procedendo a stabilire la conessione



se invece il valore è 0, effetua il jump al loc_40102B con error no internet