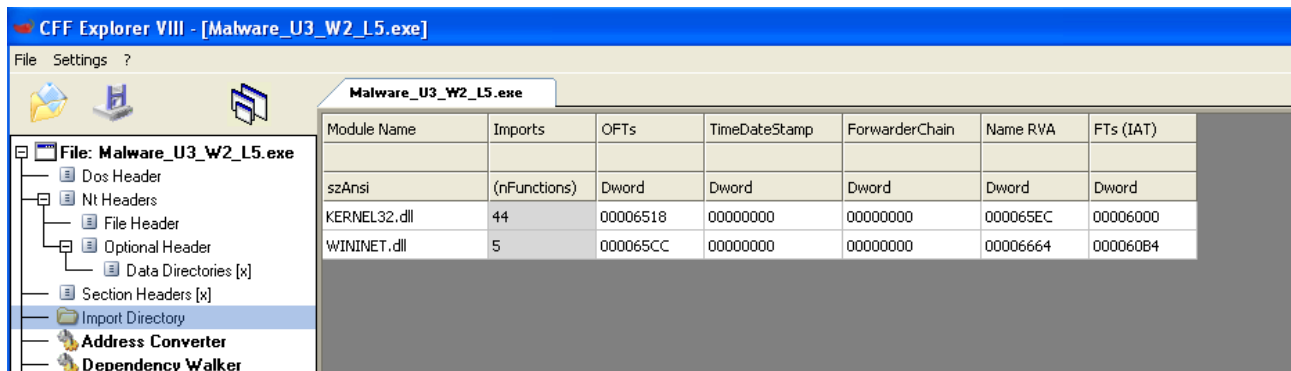


Report sett.10 Venerdì

1. Librerie

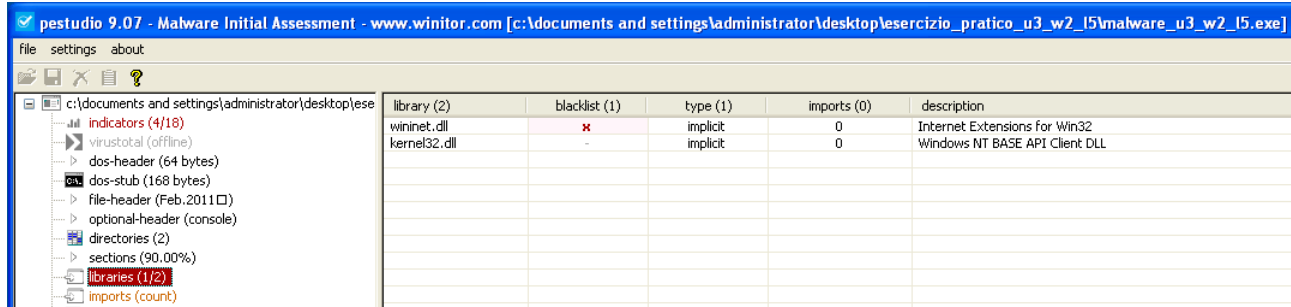
Tool: CFF Explorer

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

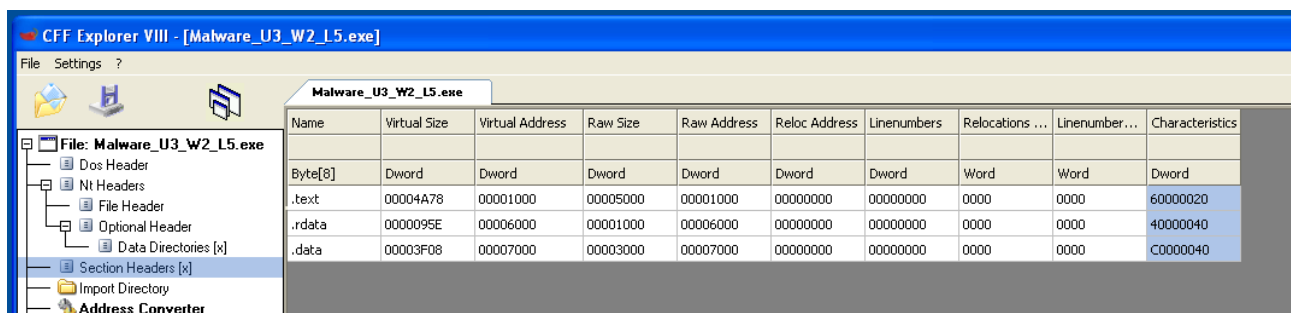
lo stesso risultato otteniamo usando il Pestudio



2. Sezioni

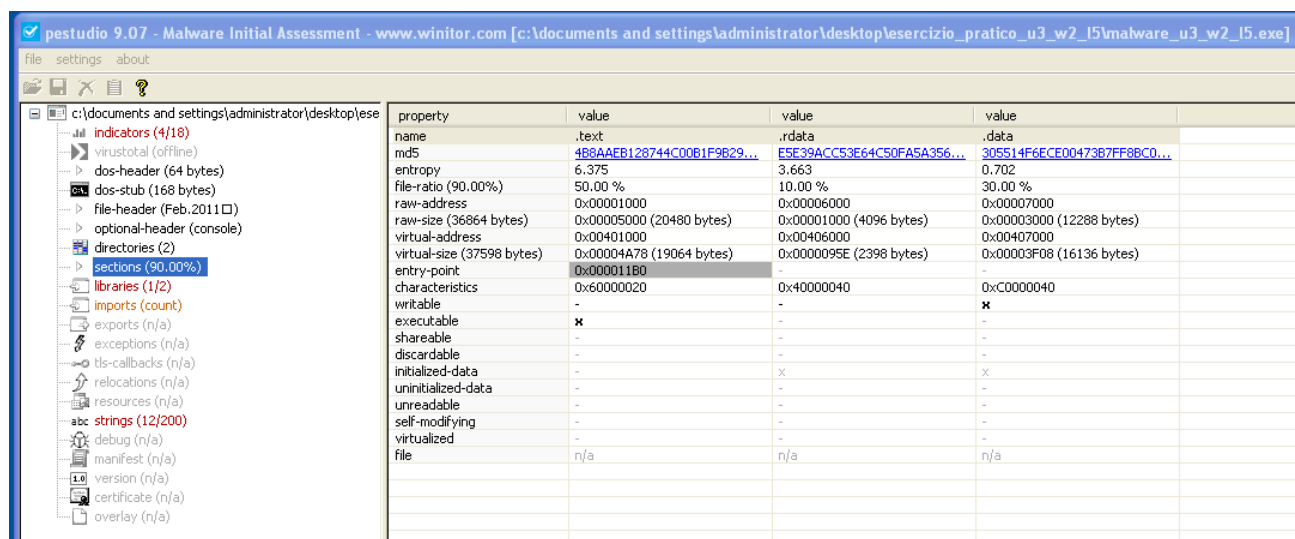
Tool: CFF Explorer

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

Costruzione di stack

```
push ebp
mov ebp, esp
push ecx
push 0 ; dwReserved
push 0 ; lpdwFlags
call ds:InternetGetConnectedState
mov [ebp+var_4], eax
cmp [ebp+var_4], 0
jz short loc_40102B
```

Costrutto condizionale IF

```
push offset aSuccessInterne ; "Success: Internet Connection\n"
call sub_40117F
add esp, 4
mov eax, 1
jmp short loc_40103A
```

```
loc_40102B:
push offset aError1_1NoInte ; "Error 1.1: No Internet\n"
call sub_40117F
add esp, 4
xor eax, eax
```

```
loc_40103A:
mov esp, ebp
pop ebp
retn
sub_401000 endp
```

Rimozione di stack

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

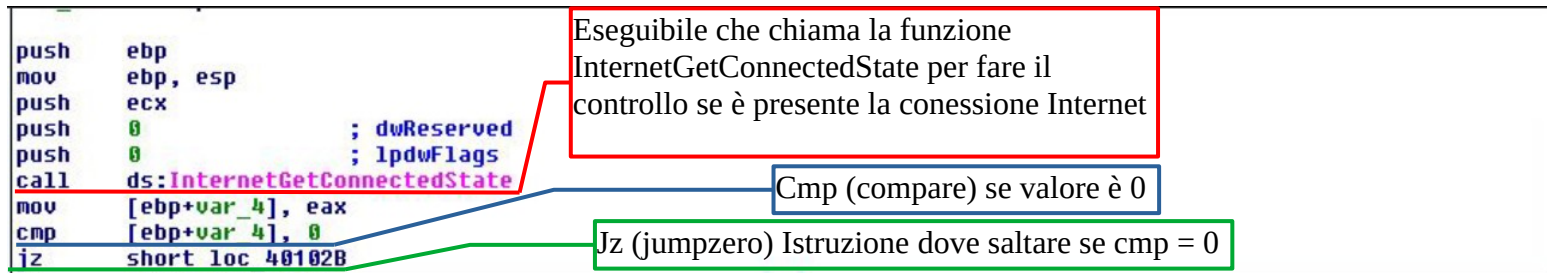
jmp = unconditional absolute jump

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 connessione

```
push    offset aSuccessInterne ; "Success: Internet Connection\n"
call    sub_40117F
add     esp, 4
mov     eax, 1
jmp     short loc_40103A
```

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

```
loc_40102B:           ; "Error 1.1: No Internet\n"
push    offset aError1_1NoInte
call    sub_40117F
add     esp, 4
xor     eax, eax
```

