

S11-L3



Traccia: Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3 sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

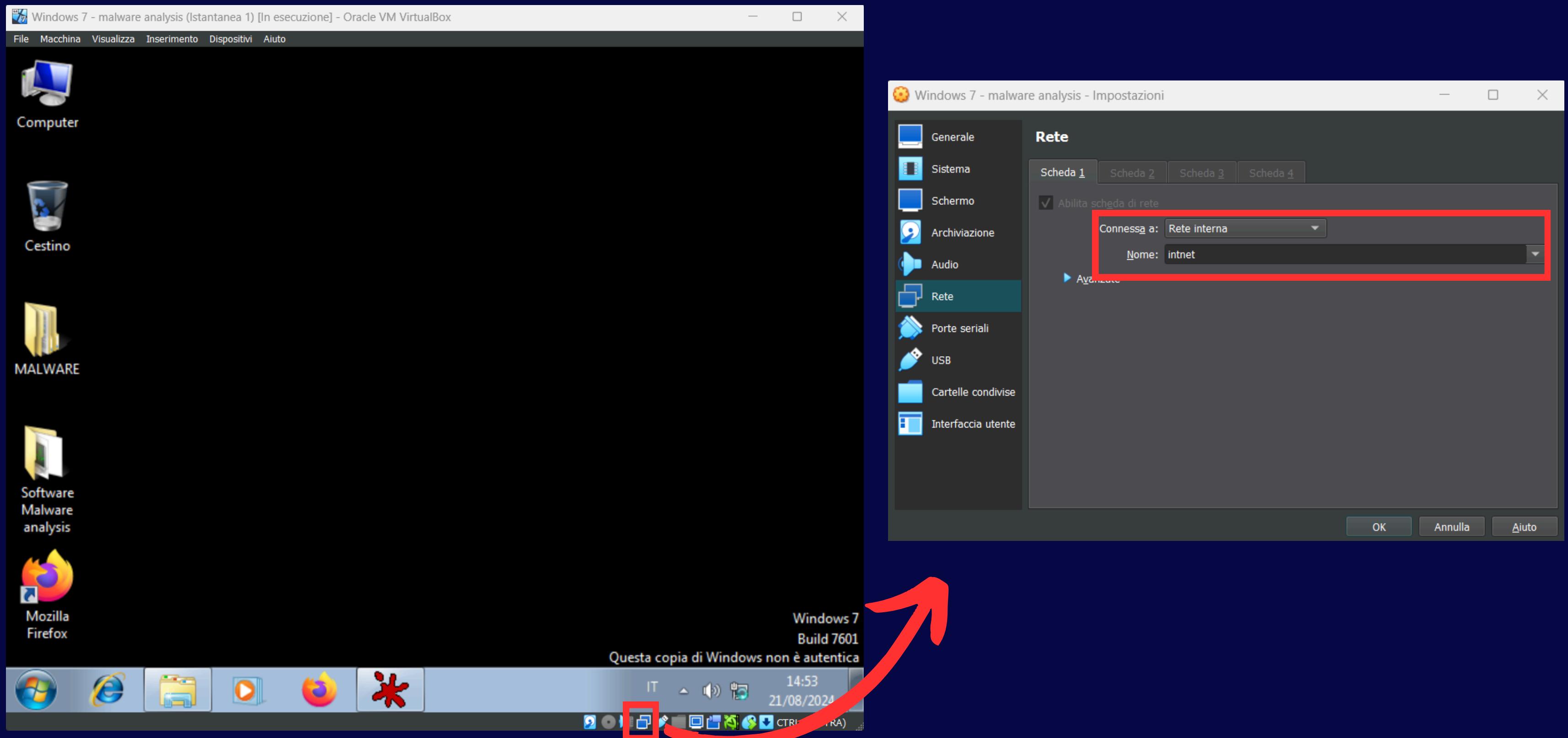
All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack?

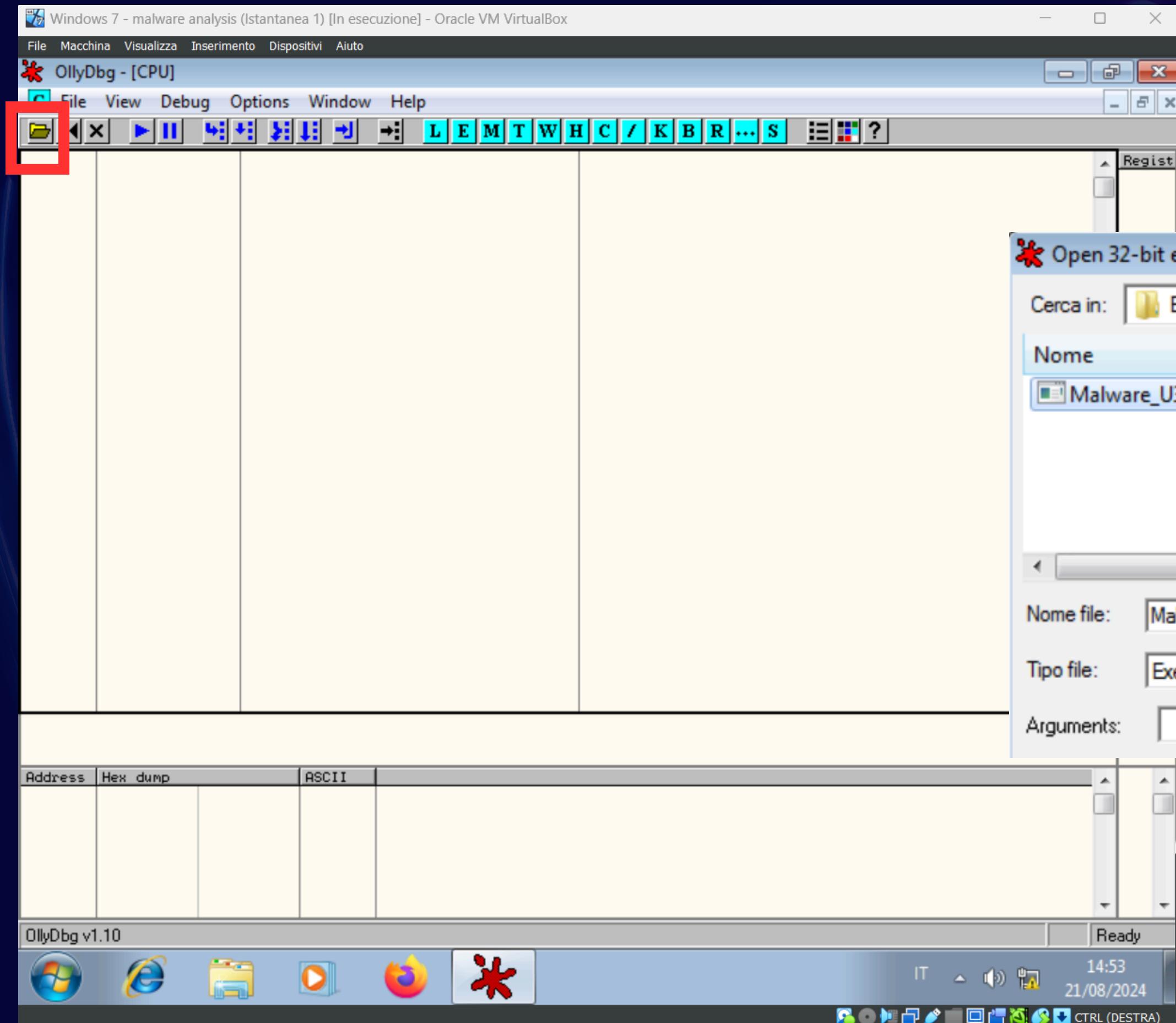
Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita

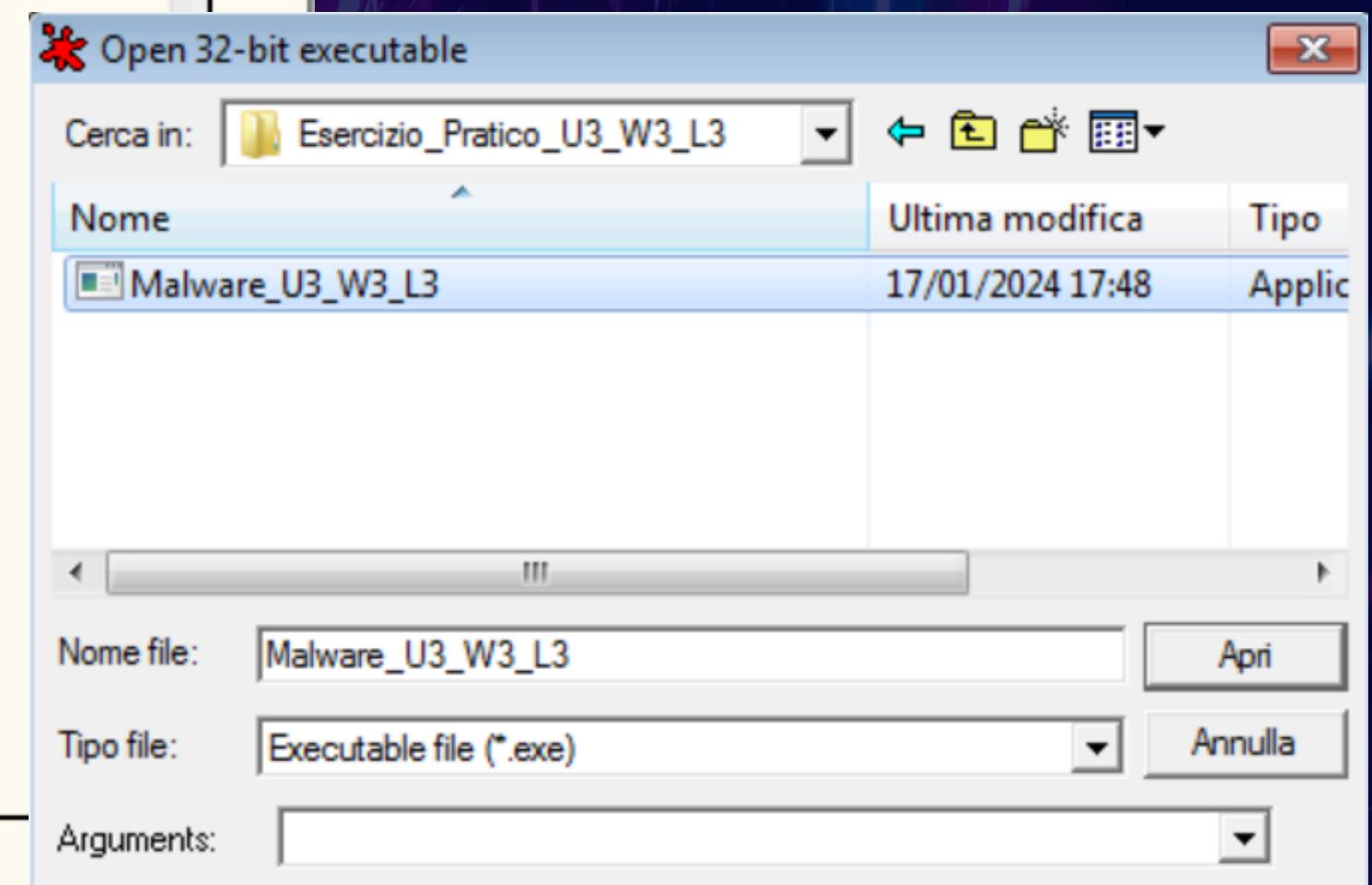
BONUS: spiegare a grandi linee il funzionamento del malware

Prima di tutto isoliamo la macchina andando a settare una rete interna per evitare che analizzando il malware si infettino altre macchine.





Andiamo ad aprire il malware U3_W3_L3



OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module ntdll]

C File View Debug Options Windows Help

L E M T W H C / K B R ... S

```

770201E8 895C24 08 MOV DWORD PTR DS:[ESP+8],EBX
770201EC vE9 C9950200 JMP ntdll.770497BA
770201F1 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
770201F8 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
770201FF 90 NOP
77020200 8BD4 MOV EDX,ESP
77020202 0F34 SYSENTER
77020204 C3 RETN
77020205 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
7702020C 8D6424 00 LEA ESP,DWORD PTR SS:[ESP]
77020210 8D5424 08 LEA EDX,DWORD PTR SS:[ESP+8]
77020214 CD 2E INT 2E
77020216 C3 RETN
77020217 90 NOP
77020218 0000 ADD BYTE PTR DS:[EAX],AL
7702021A 0000 ADD BYTE PTR DS:[EAX],AL
7702021C 381C6E CMP BYTE PTR DS:[ESI+EBP*2],BL
7702021F 5C POP ESP
77020220 0000 ADD BYTE PTR DS:[EAX],AL
77020222 0000 ADD BYTE PTR DS:[EAX],AL
77020224 7A 51 JPE SHORT ntdll.77020277
77020226 0100 ADD DWORD PTR DS:[EAX],EAX
77020228 0100 ADD DWORD PTR DS:[EAX],EAX
7702022A 0000 ADD BYTE PTR DS:[EAX],AL
7702022C F1 INT1
7702022D 07 POP ES
7702022E 0000 ADD BYTE PTR DS:[EAX],AL
77020230 -E9 07000040 JMP B702023C
77020235 0201 ADD AL,BYTE PTR DS:[ECX]
77020237 000422 ADD BYTE PTR DS:[EDX],AL
7702023A 0100 ADD DWORD PTR DS:[EAX],EAX
7702023C A8 41 TEST AL,41
7702023E 0100 ADD DWORD PTR DS:[EAX],EAX
77020240 A4 MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]
77020241 BE 0A0043BF MOV ESI,BF43000A
77020246 0A00 OR AL,BYTE PTR DS:[EAX]
77020248 69BA 0A00FDDB 01 IMUL EDI,DWORD PTR DS:[EDX+BBFD000A],BA
77020252 0A00 OR AL,BYTE PTR DS:[EAX]
77020254 39B8 0A0075BE CMP DWORD PTR DS:[EAX+BE75000A],EDI
7702025A 0A00 OR AL,BYTE PTR DS:[EAX]
7702025C D4 40 AAM 40
7702025E 07 POP ES
7702025F 0031 ADD BYTE PTR DS:[ECX],DH
77020261 2202 AND AL,BYTE PTR DS:[EDX]

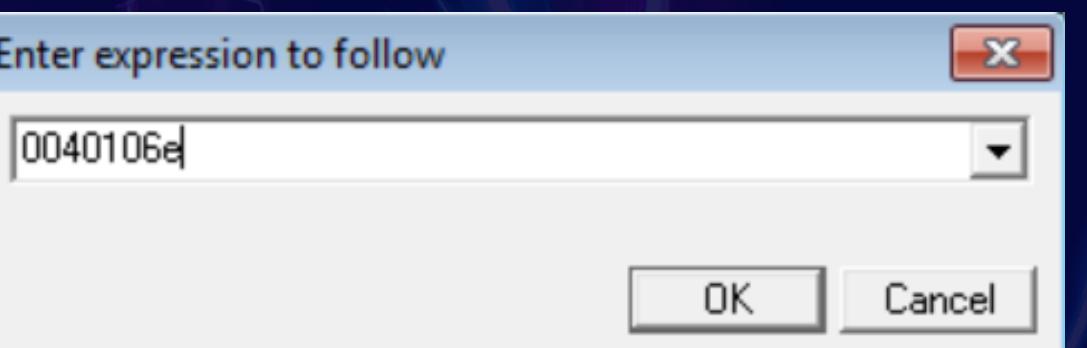
Modification of segment register
EBX=7EFDE000
Stack SS:[0018FFF8]=00000000

Address Hex dump ASCII
00405000 00 00 00 00 00 00 00 00 .....@.
00405008 00 00 00 00 F8 27 40 00 .....@.
00405010 00 00 00 00 00 00 00 00 .....
00405018 00 00 00 00 00 00 00 00 .....
00405020 00 00 00 00 00 00 00 00 .....
00405028 00 00 00 00 00 00 00 00 .....
00405030 63 6D 64 00 46 06 16 54 cmd.F*.T
00405038 42 05 12 1B 47 0C 07 02 B***G..@.
00405040 5D 1C 00 16 45 16 01 1D JL..E..@.
00405048 52 0B 05 0F 48 02 08 09 R***H@.

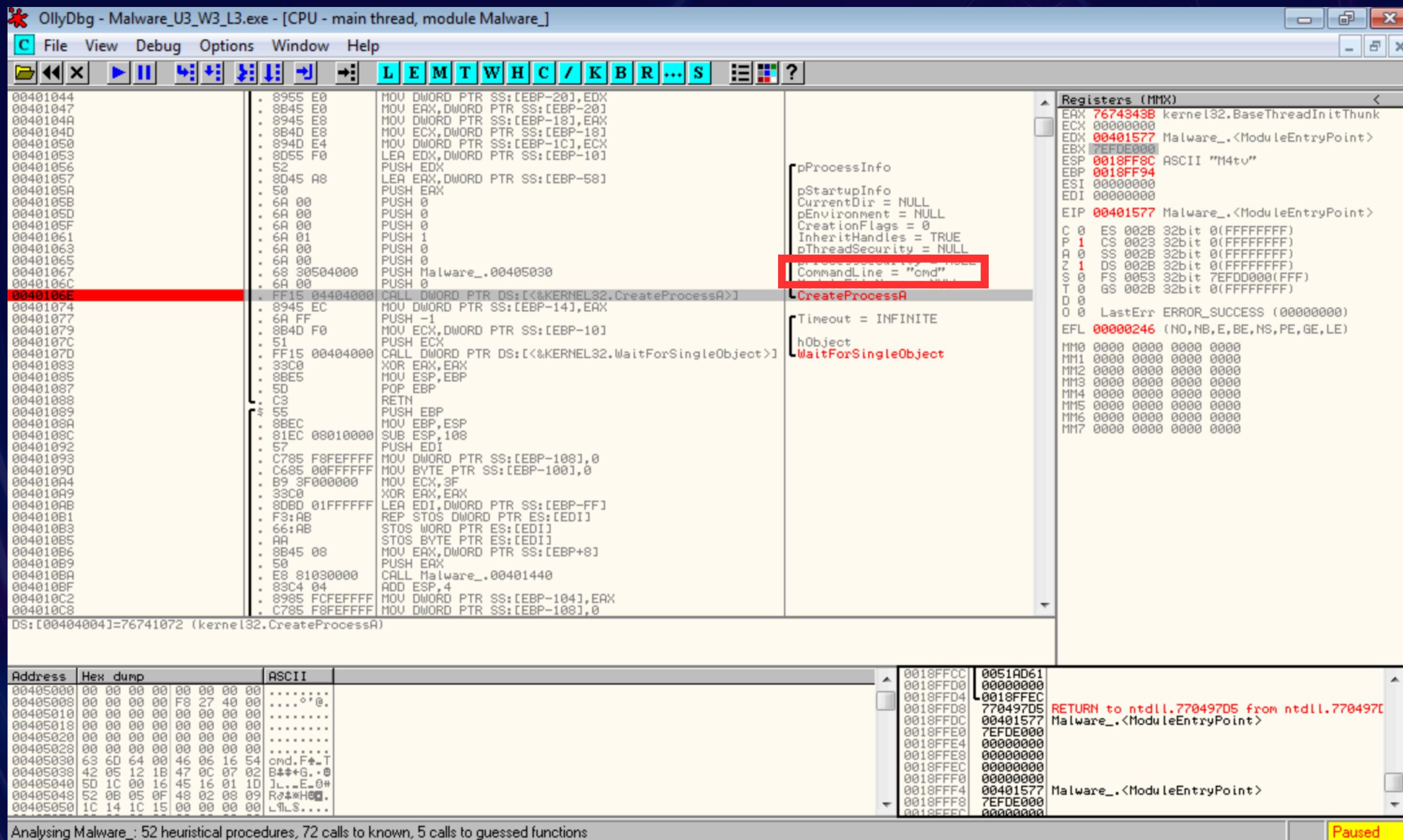
Single step event at ntdll.770201E8 - use Shift+F7/F8/F9 to pass exception to program
Paused

```

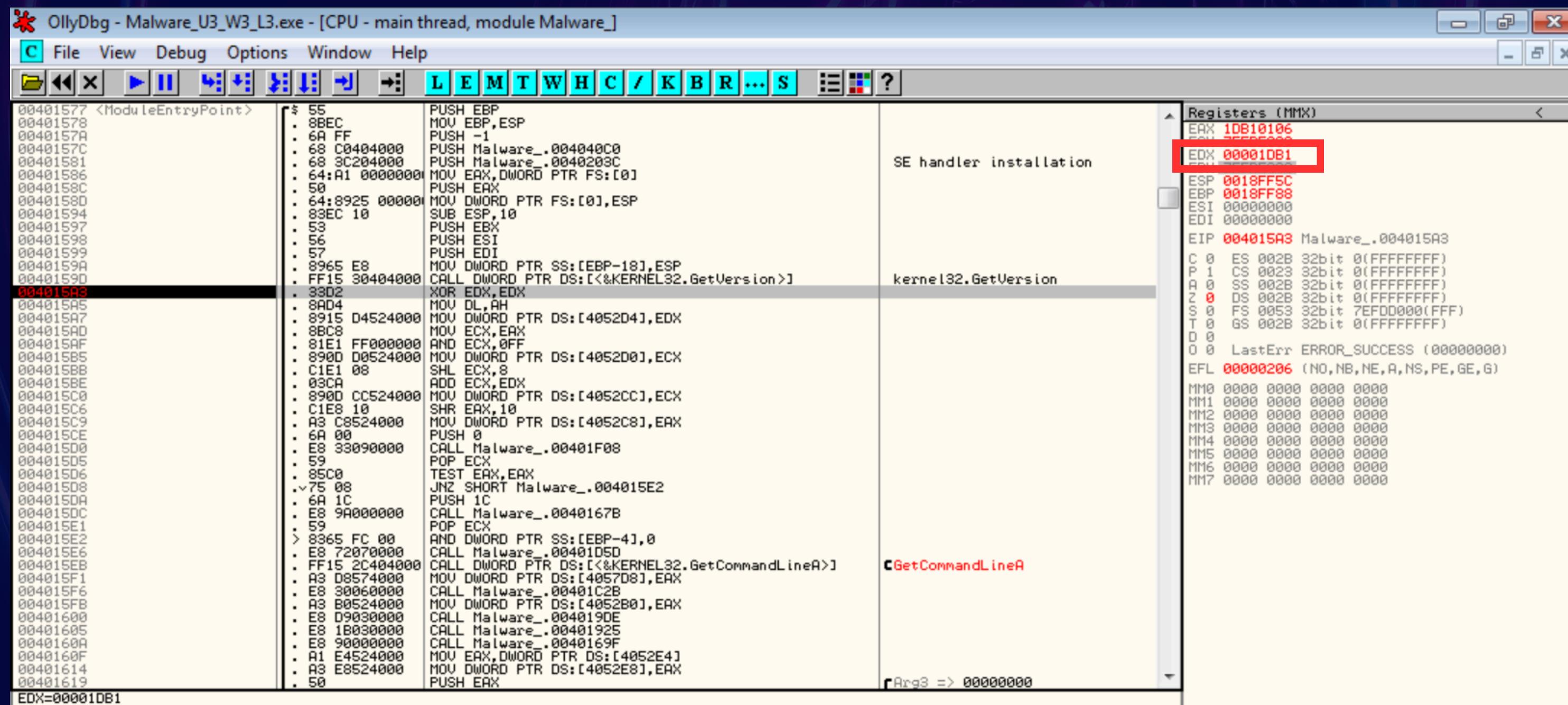
L'esercizio richiedeva di spostarsi all'indirizzo 0040106E, quindi cliccando sull'icona evidenziata inseriamo l'indirizzo richiesto



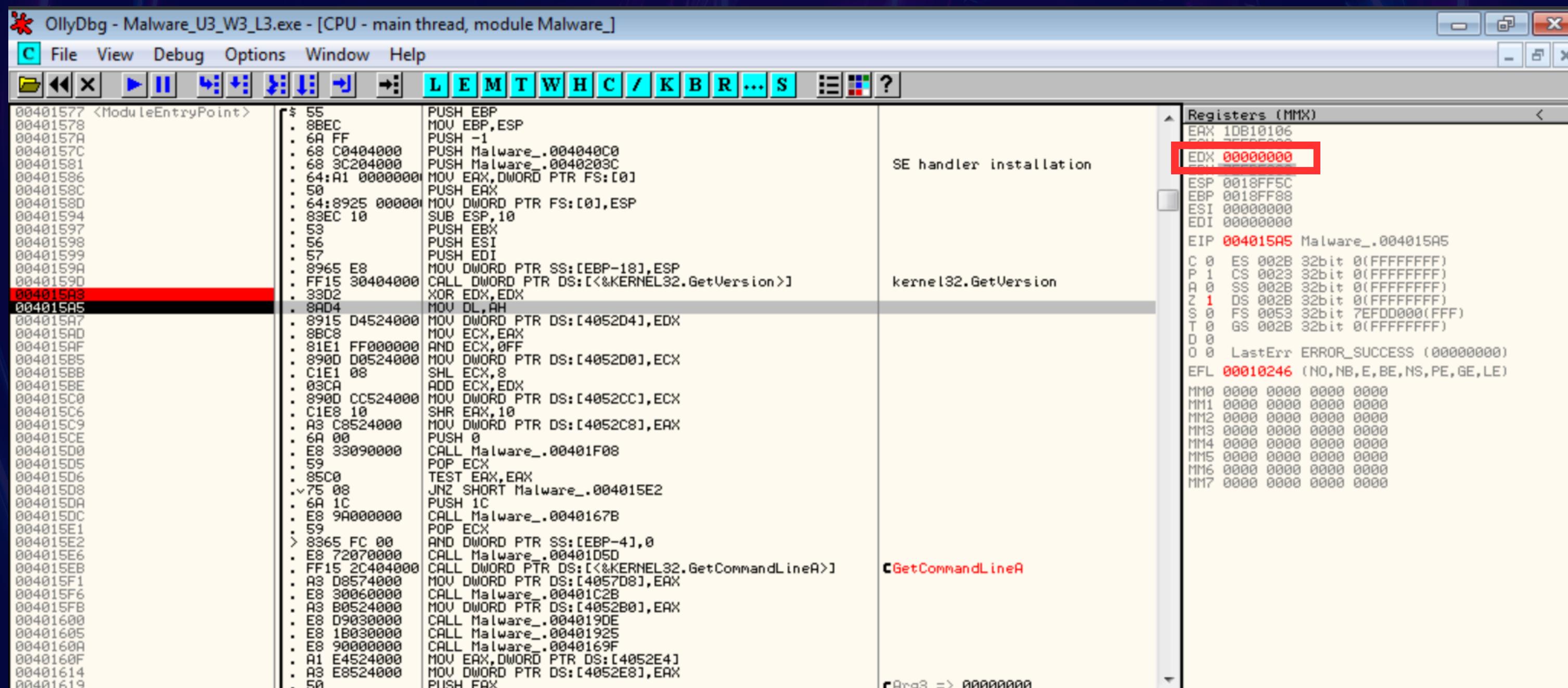
Il parametro che viene passato a CommandLine sullo stack è “cmd”



Inseriamo ora un breakpoint all'indirizzo 004015A3, il valore del registro EDX è 00001DB1 e facciamo uno step-into per vedere i cambiamenti del registro



Il nuovo valore del registro è 00000000, questo perchè è stato effettuato uno XOR del registro EDX con sè stesso di conseguenza il risultato è 0



Inseriamo ora un breakpoint all'indirizzo 004015AF, il valore del registro ECX è 1DB10106 e facciamo uno step-into per vedere i cambiamenti del registro

The screenshot shows the OllyDbg debugger interface. The assembly window displays the following code snippet:

```
00401577 <ModuleEntryPoint>
00401578
0040157A
0040157C
00401581
00401586
0040158C
0040158D
00401594
00401597
00401598
00401599
0040159A
0040159D
004015A3
004015A5
004015A7
004015AD
004015AF
004015B5
004015BB
004015BE
004015C0
004015C6
004015C9
004015CE
004015D8
004015D5
004015D6
004015D8
004015DA
004015DC
004015E1
004015E2
004015E6
004015EB
004015F1
004015F6
004015FB
00401600
00401605
0040160A
0040160F
00401614
00401619

$ 55      PUSH EBP
. 8BEC    MOV EBP,ESP
. 6A FF    PUSH -1
. 68 C0404000 PUSH Malware_.004040C0
. 68 3C204000 PUSH Malware_.0040203C
. 64:A1 00000000 MOV EAX,DWORD PTR FS:[0]
. 50      PUSH EAX
. 64:8925 000000 MOV DWORD PTR FS:[0],ESP
. 83EC 10    SUB ESP,10
. 53      PUSH EBX
. 56      PUSH ESI
. 57      PUSH EDI
. 8965 E8    MOV DWORD PTR SS:[EBP-18],ESP
FF15 30404000 CALL DWORD PTR DS:[<&KERNEL32.GetVersion>]
. 33D2    XOR EDX,EDX
. 8AD4    MOV DL,AH
. 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
. 8BC8    MOV ECX,EAX
. 81E1 FF000000 AND ECX,0FF
. 890D D0524000 MOV DWORD PTR DS:[4052D0],ECX
. C1E1 08    SHL ECX,8
. 03CA    ADD ECX,EDX
. 890D CC524000 MOV DWORD PTR DS:[4052CC],ECX
. C1E8 10    SHR EAX,10
. A3 C8524000 MOV DWORD PTR DS:[4052C8],EAX
. 6A 00    PUSH 0
. E8 33090000 CALL Malware_.00401F08
. 59      POP ECX
. 85C0    TEST EAX,EAX
. v75 08    JNZ SHORT Malware_.004015E2
. 6A 1C    PUSH 1C
. E8 9A000000 CALL Malware_.0040167B
. 59      POP ECX
. > 8365 FC 00 AND DWORD PTR SS:[EBP-4],0
. E8 72070000 CALL Malware_.00401D50
. FF15 2C404000 CALL DWORD PTR DS:[<&KERNEL32.GetCommandLineA>]
. A3 D8574000 MOV DWORD PTR DS:[4057D8],EAX
. E8 30060000 CALL Malware_.00401C2B
. A3 B0524000 MOV DWORD PTR DS:[4052B0],EAX
. E8 D9030000 CALL Malware_.004019DE
. E8 1B030000 CALL Malware_.00401925
. E8 90000000 CALL Malware_.0040169F
. A1 E4524000 MOV EAX,DWORD PTR DS:[4052E4]
. A3 E8524000 MOV DWORD PTR DS:[4052E8],EAX
. 50      PUSH EAX
```

The Registers window shows the following values:

Register	Value
ECX	1DB10106
EBX	7EFDE000
ESP	0018FF5C
EBP	0018FF88
ESI	00000000
EDI	00000000
EIP	004015AF Malware_.004015AF
C 0	ES 002B 32bit 0(FFFFFFFF)
P 1	CS 0023 32bit 0(FFFFFFFF)
A 0	SS 002B 32bit 0(FFFFFFFF)
Z 1	DS 002B 32bit 0(FFFFFFFF)
S 0	FS 0053 32bit 7EFDD000(FFF)
T 0	GS 002B 32bit 0(FFFFFFFF)
D 0	LastErr ERROR_SUCCESS (00000000)
EFL	00000246 (NO,NB,E,BE,NS,PE,GE,LE)
MM0	0000 0000 0000 0000
MM1	0000 0000 0000 0000
MM2	0000 0000 0000 0000
MM3	0000 0000 0000 0000
MM4	0000 0000 0000 0000
MM5	0000 0000 0000 0000
MM6	0000 0000 0000 0000
MM7	0000 0000 0000 0000

The CPU window shows the instruction at address 004015AF:

GetCommandLineA

The Registers window also shows the value of Arg3 (00000000).

Il nuovo valore del registro è 00000006, questo perchè è stato effettuato un AND del registro ECX con il numero esadecimale OFF

