

20373585 夏瑞斌 200612

## 1. 解读水印地址及内容

```
DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
Program terminated normally
-r
AX=078A BX=0000 CX=02C3 DX=0000 SP=0200 BP=0000 SI=0000 DI=0000
DS=078A ES=075A SS=076A CS=078F IP=0040  NU UP EI PL NZ NA PO NC
078F:0040 BB0100      MOV     BX,0001
-d ds:0
078A:0000  10 00 FF FF 21 33 85 12-90 01 2C 01 42 00 41 00  ....!3.....B.A.
078A:0010  3C 00 28 00 14 00 0A 00-08 00 03 00 02 00 01 00  <.(.....
078A:0020  00 00 4D 79 20 6E 61 6D-65 20 69 73 20 32 30 30  ..My name is 200
078A:0030  36 31 32 32 30 33 37 33-35 38 35 20 58 69 61 20  61220373585 Xia
078A:0040  52 75 69 62 69 6E 24 00-30 00 20 78 56 34 12 00  Ruibin$.0. xU4..
078A:0050  B8 6A 07 8E D0 BC 00 02-B8 8A 07 8E D8 EB 30 90  .j.....0.
078A:0060  C5 36 47 00 C4 3E 4B 00-EB 24 EB 22 90 EB 1F 90  .6G..>K..$. "....
078A:0070  90 90 FF E3 FF E3 FF 27-FF 27 FF 2F FF 2E 47 00  .....'. ' /..G.
-e ds:47 85 35 12 06
-d ds:0
078A:0000  10 00 FF FF 21 33 85 12-90 01 2C 01 42 00 41 00  ....!3.....B.A.
078A:0010  3C 00 28 00 14 00 0A 00-08 00 03 00 02 00 01 00  <.(.....
078A:0020  00 00 4D 79 20 6E 61 6D-65 20 69 73 20 32 30 30  ..My name is 200
078A:0030  36 31 32 32 30 33 37 33-35 38 35 20 58 69 61 20  61220373585 Xia
078A:0040  52 75 69 62 69 6E 24 85-35 12 06 78 56 34 12 00  Ruibin$.5..xU4..
078A:0050  B8 6A 07 8E D0 BC 00 02-B8 8A 07 8E D8 EB 30 90  .j.....0.
078A:0060  C5 36 47 00 C4 3E 4B 00-EB 24 EB 22 90 EB 1F 90  .6G..>K..$. "....
078A:0070  90 90 FF E3 FF E3 FF 27-FF 27 FF 2F FF 2E 47 00  .....'. ' /..G.
```

将原先 ADD1 中的 20003000 改为了班号学号（太长了，截取部分）06123585

## 2. 解读 JMP DWORD PTR ADD1 执行后的 CS:IP

```
DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
DS=078A ES=075A SS=076A CS=078F IP=002C  NU UP EI PL NZ NA PO NC
078F:002C FF2E4700      JMP     FAR [0047]      DS:0047=3585
-u
078F:002C FF2E4700      JMP     FAR [0047]
078F:0030 FFD3           CALL    BX
078F:0032 FF17           CALL    [BX]
078F:0034 FF17           CALL    [BX]
078F:0036 FF1E4700      CALL    FAR [0047]
078F:003A FF1E4700      CALL    FAR [0047]
078F:003E 90           NOP
078F:003F 90           NOP
078F:0040 BB0100      MOV     BX,0001
078F:0043 8B0E0000     MOV     CX,[0000]
078F:0047 49           DEC     CX
078F:0048 8D360200     LEA     SI,[0002]
-r
AX=078A BX=0000 CX=02C3 DX=0000 SP=0200 BP=0000 SI=0000 DI=0000
DS=078A ES=075A SS=076A CS=078F IP=002C  NU UP EI PL NZ NA PO NC
078F:002C FF2E4700      JMP     FAR [0047]      DS:0047=3585
-t
AX=078A BX=0000 CX=02C3 DX=0000 SP=0200 BP=0000 SI=0000 DI=0000
DS=078A ES=075A SS=076A CS=0612 IP=3585  NU UP EI PL NZ NA PO NC
0612:3585 5E           POP     SI
```

其实单步执行的话应该用 p，不过这里用 t 效果都一样，就不再改了

CS:IP 变为了 0612:3585，也就是 JMP 指令的转移目标地址（位于 ADD1 中）。

### 3. 解读 CALL DWORD PTR ADD1 执行后栈顶数据区的地址及内容

```

DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
IP 002C
:36
-r
AX=078A BX=0000 CX=02C3 DX=0000 SP=01FC BP=0000 SI=0000 DI=0000
DS=078A ES=075A SS=076A CS=078F IP=0036  NU UP EI PL NZ NA PO NC
078F:0036 FF1E4700 CALL FAR [0047] DS:0047=3585
-u
078F:0036 FF1E4700 CALL FAR [0047]
078F:003A FF1E4700 CALL FAR [0047]
078F:003E 90 NOP
078F:003F 90 NOP
078F:0040 BB0100 MOV BX,0001
078F:0043 8B0E0000 MOV CX,[0000]
078F:0047 49 DEC CX
078F:0048 8D360200 LEA SI,[0002]
078F:004C 8B04 MOV AX,[SI]
078F:004E 3B4402 CMP AX,[SI+02]
078F:0051 7308 JNB 005B
078F:0053 874402 XCHG AX,[SI+02]
-p
AX=078A BX=0000 CX=02C3 DX=0000 SP=01F8 BP=0000 SI=0000 DI=0000
DS=078A ES=075A SS=076A CS=0612 IP=3585  NU UP EI PL NZ NA PO NC
0612:3585 5E POP SI

```

(发现用 p 和用 t 一样，应该是跳转地址是乱填的缘故)

CS:IP 变为了 0612:3585，同样是 CALL 段间间接调用的跳转目标地址。

```

DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
0612:3586 F0 LOCK
0612:3587 D1E3 SHL BX,1
0612:3589 A16408 MOV AX,[0864]
0612:358C 8900 MOV [BX+SI],AX
0612:358E C45EF6 LES BX,[BP-0A]
0612:3591 26 ES:
0612:3592 8B470C MOV AX,[BX+0C]
0612:3595 BE6408 MOV SI,0864
0612:3598 8B1C MOV BX,[SI]
0612:359A FF04 INC WORD PTR [SI]
0612:359C D1E3 SHL BX,1
0612:359E 8B36E625 MOV SI,[25E6]
0612:35A2 8900 MOV [BX+SI],AX
0612:35A4 8B5EF6 MOV BX,[BP-0A]
-d ss:01f8
076A:01F0 3A 00 8F 07 3A 00 8F 07 :...:...
076A:0200 10 00 FF FF 21 33 85 12-90 01 2C 01 42 00 41 00 ....?3.....,B.A.
076A:0210 3C 00 28 00 14 00 0A 00-08 00 03 00 02 00 01 00 <.(.....
076A:0220 00 00 4D 79 20 6E 61 6D-65 20 69 73 20 32 30 30 ..My name is 200
076A:0230 36 31 32 32 30 33 37 33-35 38 35 20 58 69 61 20 61220373585 Xia
076A:0240 52 75 69 62 69 6E 24 85-35 12 06 78 56 34 12 00 Ruibin$.5..xU4..
076A:0250 B8 6A 07 8E D0 BC 00 02-B8 8A 07 8E D8 EB 30 90 .j.....0.
076A:0260 C5 36 47 00 C4 3E 4B 00-EB 24 EB 22 90 EB 1F 90 .6G..>K..$. "....
076A:0270 90 90 FF E3 FF E3 FF 27 .....

```

可以看到栈顶存储的双字为 078f:003a，即为跳转回来后的下一条指令地址

(第二行开始往下的内容，和 DS:0000 的内容一模一样，不是很清楚原理)