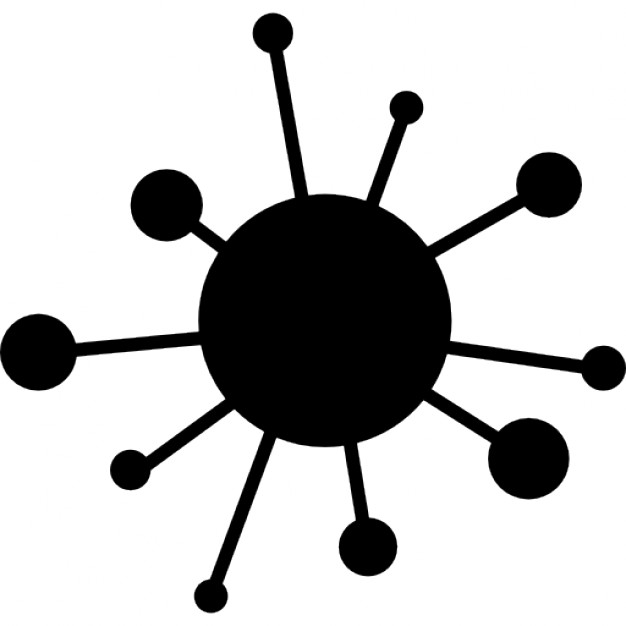
# 计算机病毒学

实验8 PE感染文件制作



学号：0x091395

姓名：uknowho

实验目的

1、 深入理解PE类型可执行文件的格式。

2、 掌握PE类型可执行文件的运行机理。

3、 掌握病毒感染PE类型可执行文件后的数据分布及其规律。

4、 掌握感染PE类型可执行文件病毒程序的基本制作方法和原理。

5、 进一步熟悉debug、debug32工具的使用。

6、 深刻理解病毒代码融入感染文件代码的修饰技巧。

实验原理

正常文件的执行程序

00401000 6A00 PUSH 00h ；对话框不属于任何窗口

00401002 6810304000 PUSH 00403010 ；标题“Program Information”

00401007 6800304000 PUSH 00403000 ；字符串“Hello World”

0040100C 6A00 PUSH 00h ；按钮风格MB\_OK

0040100E E808000000 CALL 0040101B ；显示对话框MessageBoxA()

00401013 6A00 PUSH 00h ；返回码ExitCode，正常返回

00401015 E807000000 CALL 00401021 ；退出进程ExitProcess()

0040101A CC INT 3 ；程序停止运行

紧接着是正常文件执行程序调用外部函数接口：

0040101B FF 25 08 20 40 00 FF 25 00 20 40 00

2、感染代码执行程序

00401030 6A00 PUSH 00h ；对话框不属于任何窗口

00401032 6810304000 PUSH 00403040 ；标题“Computer Virus”

00401037 6800304000 PUSH 00403030 ；字符串“You are killed.”

0040103C 6A00 PUSH 00h ；按钮风格MB\_OK

0040103E E803000000 CALL 00401046 ；显示对话框MessageBoxA()

00401043 EBBB JMP NEAR 00401000 ；跳转到正常文件的执行程序入口

00401045 CC INT 3

紧接着是感染程序调用外部函数接口：

00401046 FF 25 08 20 40 00

如果按照以上程序设计，正常文件的执行程序调用的函数接口安排紧接在其程序的后面，感染代码也一样。附录A给出了这样一个制作实例。

按照这种方式感染文件，很容易让人怀疑是两个文件拼凑而成的。因为，编译链接软件不会为一个程序提供两个外部函数调用接口。稍有经验的用户，会调整EIP指向正常文件的执行程序入口，就避免了感染代码的执行。

为此，可以把感染代码修改成以下形式，就可以避免两个外部函数调用接口的出现：

00401030 6A00 PUSH 00h ；对话框不属于任何窗口

00401032 6810304000 PUSH 00403040 ；标题“Computer Virus”

00401037 6800304000 PUSH 00403030 ；字符串“You are killed.”

0040103C 6A00 PUSH 00h ；按钮风格MB\_OK

0040103E E8FFFFFFD8 CALL 0040101B ；显示对话框MessageBoxA()

00401043 EBBB JMP NEAR 00401000 ；跳转到正常文件的执行程序入口

也就是说，感染代码与正常程序共用了一个外部函数调用接口，减少了用户的怀疑。附录B给出了这样一个制作实例。

当然，正常文件写入感染代码后，不同段的段长度发生了改变；不同段分配的字节数也随之改变；在磁盘上的文件中，不同段的相对偏移也会发生改变；感染后的程序入口要指向感染代码的入口，这样，就需要修改文件头的相关数据，以达到感染的目的。附录A、B给出的感染样例代码中，红色的部分就是修改过的数据。

实验步骤

根据上次实验，获得基本的hello.exe文件，其运行结果如图1所示。



图1 hello.exe运行结果

2、根据附录A的制作过程，制作出正常文件和感染代码各自拥有自己外部函数调用接口的感染文件h2.exe，要求其运行结果如图2所示。

图2 h2.exe运行结果

3、根据附录B的制作过程，制作出正常文件和感染文件共用一个外部函数调用接口的感染文件h3.exe，要求其运行结果如图3所示。

图3 h3.exe运行结果

4、有能力的同学，可以尝试让病毒代码紧接着正常文件代码存放，在病毒代码后面再存放共用的外部函数调用接口，这样，病毒代码和正常代码就融为一体了，一般的用户就很难区分哪儿是病毒代码，哪儿是正常文件代码了。要求制作出的感染程序h4.exe运行结果如图4所示。附录C给出了这样的一个制作实例。

图4 h4.exe运行结果

5、汇总实验数据，总结实验过程，写出实验报告。

实验结果

**附录A PE感染文件制作实例之一**

正常文件代码和病毒代码各自拥有独自的外部函数调用接口。

1. 批处理文件hello2.txt的制作

F 1000 L0A00 00

E 1000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00

E 1010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

E 1030 00 00 00 00 00 00 00 00 00 00 00 00 B0 00 00 00

E 1040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68

E 1050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F

E 1060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20

E 1070 6D 6F 64 65 2E 0D 0D 0A 24

E 10B0 50 45 00 00 4C 01 03 00 98 67 F8 51 00 00 00 00

E 10C0 00 00 00 00 E0 00 0F 01 0B 01 05 0C 00 02 00 00

E 10D0 00 04 00 00 00 00 00 00 30 10 00 00 00 10 00 00 ;程序入口EIP

E 10E0 00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00

E 10F0 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00

E 1100 00 40 00 00 00 04 00 00 00 00 00 00 02 00 00 00

E 1110 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00

E 1120 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00

E 1130 10 20 00 00 3C 00 00 00 00 00 00 00 00 00 00 00

E 1180 00 00 00 00 00 00 00 00 00 20 00 00 10 00 00 00

E 11A0 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00

E 11B0 4C 00 00 00 00 10 00 00 00 02 00 00 00 04 00 00 ;.text实际长度

E 11C0 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60

E 11D0 2E 72 64 61 74 61 00 00 92 00 00 00 00 20 00 00

E 11E0 00 02 00 00 00 06 00 00 00 00 00 00 00 00 00 00

E 11F0 00 00 00 00 40 00 00 40 2E 64 61 74 61 00 00 00

E 1200 4F 00 00 00 00 30 00 00 00 02 00 00 00 08 00 00 ;.data实际长度

E 1210 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0

E 1400 6A 00 68 10 30 40 00 68 00 30 40 00 6A 00 E8 08 ;正常文件代码

E 1410 00 00 00 6A 00 E8 07 00 00 00 CC FF 25 08 20 40 ;外部函数接口

E 1420 00 FF 25 00 20 40 00

E 1430 6A 00 68 40 30 40 00 68 30 30 40 00 6A 00 E8 03 ;感染范例代码1

E 1440 00 00 00 EB BB CC FF 25 08 20 40 00 ;外部函数接口

E 1600 76 20 00 00 00 00 00 00 5C 20 00 00 00 00 00 00

E 1610 54 20 00 00 00 00 00 00 00 00 00 00 6A 20 00 00

E 1620 08 20 00 00 4C 20 00 00 00 00 00 00 00 00 00 00

E 1630 84 20 00 00 00 20 00 00 00 00 00 00 00 00 00 00

E 1640 00 00 00 00 00 00 00 00 00 00 00 00 76 20 00 00

E 1650 00 00 00 00 5C 20 00 00 00 00 00 00 B1 01 4D 65

E 1660 73 73 61 67 65 42 6F 78 41 00 75 73 65 72 33 32

E 1670 2E 64 6C 6C 00 00 9B 00 45 78 69 74 50 72 6F 63

E 1680 65 73 73 00 6B 65 72 6E 65 6C 33 32 2E 64 6C 6C

E 1690 00 00

E 1800 48 65 6C 6C 6F 20 57 6F 72 6C 64 00 ;正常文件提示信息

E 1810 50 72 6F 67 72 61 6D 20 49 6E 66 6F 72 6D 61 74 ;正常文件标题

E 1820 69 6F 6E 00

E 1830 59 6F 75 20 61 72 65 20 6B 69 6C 6C 65 64 2E 00 ;感染文件提示信息

E 1840 43 6F 6D 70 75 74 65 72 20 56 69 72 75 73 00 ;感染文件标题

N c:\h2.dat

R BX

0

R CX

0A00

W 1000

Q

注意：红色部分文字是感染后增加的病毒数据或病毒修改的数据。

2、h2.exe的获得

2.1 执行批处理文件，生成数据文件h2.dat

debug < hello2.txt

2.2 复制数据文件，生成可执行文件h2.exe

copy h2.dat h2.exe

2.3 运行新生成的可执行文件h2.exe，运行效果如图



图1 运行结果

**附录B PE感染文件制作实例之二**

本实例制作的感染文件中，正常文件代码和病毒代码共用一个外部函数调用接口，但是病毒代码在外部函数接口后面。

1、批处理文件hello3.txt的制作

F 1000 L0A00 00

E 1000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00

E 1010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

E 1030 00 00 00 00 00 00 00 00 00 00 00 00 B0 00 00 00

E 1040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68

E 1050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F

E 1060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20

E 1070 6D 6F 64 65 2E 0D 0D 0A 24

E 10B0 50 45 00 00 4C 01 03 00 98 67 F8 51 00 00 00 00

E 10C0 00 00 00 00 E0 00 0F 01 0B 01 05 0C 00 02 00 00

E 10D0 00 04 00 00 00 00 00 00 30 10 00 00 00 10 00 00 ;程序入口EIP

E 10E0 00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00

E 10F0 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00

E 1100 00 40 00 00 00 04 00 00 00 00 00 00 02 00 00 00

E 1110 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00

E 1120 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00

E 1130 10 20 00 00 3C 00 00 00 00 00 00 00 00 00 00 00

E 1180 00 00 00 00 00 00 00 00 00 20 00 00 10 00 00 00

E 11A0 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00

E 11B0 45 00 00 00 00 10 00 00 00 02 00 00 00 04 00 00 ;.text实际长度

E 11C0 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60

E 11D0 2E 72 64 61 74 61 00 00 92 00 00 00 00 20 00 00

E 11E0 00 02 00 00 00 06 00 00 00 00 00 00 00 00 00 00

E 11F0 00 00 00 00 40 00 00 40 2E 64 61 74 61 00 00 00

E 1200 4F 00 00 00 00 30 00 00 00 02 00 00 00 08 00 00 ;.data实际长度

E 1210 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0

E 1400 6A 00 68 10 30 40 00 68 00 30 40 00 6A 00 E8 08 ;正常文件代码

E 1410 00 00 00 6A 00 E8 07 00 00 00 CC FF 25 08 20 40 ;外部函数接口

E 1420 00 FF 25 00 20 40 00

E 1430 6A 00 68 40 30 40 00 68 30 30 40 00 6A 00 E8 D8 ;感染范例代码2

E 1440 FF FF FF EB BB

E 1600 76 20 00 00 00 00 00 00 5C 20 00 00 00 00 00 00

E 1610 54 20 00 00 00 00 00 00 00 00 00 00 6A 20 00 00

E 1620 08 20 00 00 4C 20 00 00 00 00 00 00 00 00 00 00

E 1630 84 20 00 00 00 20 00 00 00 00 00 00 00 00 00 00

E 1640 00 00 00 00 00 00 00 00 00 00 00 00 76 20 00 00

E 1650 00 00 00 00 5C 20 00 00 00 00 00 00 B1 01 4D 65

E 1660 73 73 61 67 65 42 6F 78 41 00 75 73 65 72 33 32

E 1670 2E 64 6C 6C 00 00 9B 00 45 78 69 74 50 72 6F 63

E 1680 65 73 73 00 6B 65 72 6E 65 6C 33 32 2E 64 6C 6C

E 1690 00 00

E 1800 48 65 6C 6C 6F 20 57 6F 72 6C 64 00 ;正常文件提示信息

E 1810 50 72 6F 67 72 61 6D 20 49 6E 66 6F 72 6D 61 74 ;正常文件标题

E 1820 69 6F 6E 00

E 1830 59 6F 75 20 61 72 65 20 6B 69 6C 6C 65 64 2E 00 ;感染文件提示信息

E 1840 43 6F 6D 70 75 74 65 72 20 56 69 72 75 73 00 ;感染文件标题

N c:\h3.dat

R BX

0

R CX

0A00

W 1000

Q

2、h3.exe的获得

2.1 执行批处理文件，生成数据文件h3.dat

debug < hello3.txt

2.2 复制数据文件，生成可执行文件h3.exe

copy h3.dat h3.exe

2.3 运行新生成的可执行文件h3.exe，运行效果如图1所示。

**附录C PE感染文件制作实例之三**

本实例制作的感染文件中，正常文件代码和病毒代码共用一个外部函数调用接口，而且病毒代码在正常文件代码后面。

1、批处理文件hello4.txt的制作

F 1000 L0A00 00

E 1000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00

E 1010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

E 1030 00 00 00 00 00 00 00 00 00 00 00 00 B0 00 00 00

E 1040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68

E 1050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F

E 1060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20

E 1070 6D 6F 64 65 2E 0D 0D 0A 24

E 10B0 50 45 00 00 4C 01 03 00 98 67 F8 51 00 00 00 00

E 10C0 00 00 00 00 E0 00 0F 01 0B 01 05 0C 00 02 00 00

E 10D0 00 04 00 00 00 00 00 00 1B 10 00 00 00 10 00 00 ;程序入口EIP

E 10E0 00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00

E 10F0 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00

E 1100 00 40 00 00 00 04 00 00 00 00 00 00 02 00 00 00

E 1110 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00

E 1120 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00

E 1130 10 20 00 00 3C 00 00 00 00 00 00 00 00 00 00 00

E 1180 00 00 00 00 00 00 00 00 00 20 00 00 10 00 00 00

E 11A0 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00

E 11B0 3C 00 00 00 00 10 00 00 00 02 00 00 00 04 00 00 ;.text实际长度

E 11C0 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60

E 11D0 2E 72 64 61 74 61 00 00 92 00 00 00 00 20 00 00

E 11E0 00 02 00 00 00 06 00 00 00 00 00 00 00 00 00 00

E 11F0 00 00 00 00 40 00 00 40 2E 64 61 74 61 00 00 00

E 1200 4F 00 00 00 00 30 00 00 00 02 00 00 00 08 00 00 ;.data实际长度

E 1210 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0

E 1400 6A 00 68 10 30 40 00 68 00 30 40 00 6A 00 E8 1D ;正常代码

E 1410 00 00 00 6A 00 E8 1C 00 00 00 CC 6A 00 68 10 30 ;感染代码

E 1420 40 00 68 00 30 40 00 6A 00 E8 02 00 00 00 EB D0

E 1430 FF 25 08 20 40 00 FF 25 00 20 40 00 ;外部函数接口

E 1600 76 20 00 00 00 00 00 00 5C 20 00 00 00 00 00 00

E 1610 54 20 00 00 00 00 00 00 00 00 00 00 6A 20 00 00

E 1620 08 20 00 00 4C 20 00 00 00 00 00 00 00 00 00 00

E 1630 84 20 00 00 00 20 00 00 00 00 00 00 00 00 00 00

E 1640 00 00 00 00 00 00 00 00 00 00 00 00 76 20 00 00

E 1650 00 00 00 00 5C 20 00 00 00 00 00 00 B1 01 4D 65

E 1660 73 73 61 67 65 42 6F 78 41 00 75 73 65 72 33 32

E 1670 2E 64 6C 6C 00 00 9B 00 45 78 69 74 50 72 6F 63

E 1680 65 73 73 00 6B 65 72 6E 65 6C 33 32 2E 64 6C 6C

E 1690 00 00

E 1800 48 65 6C 6C 6F 20 57 6F 72 6C 64 00 ;正常文件提示信息

E 1810 50 72 6F 67 72 61 6D 20 49 6E 66 6F 72 6D 61 74 ;正常文件标题

E 1820 69 6F 6E 00

E 1830 59 6F 75 20 61 72 65 20 6B 69 6C 6C 65 64 2E 00 ;感染文件提示信息

E 1840 43 6F 6D 70 75 74 65 72 20 56 69 72 75 73 00 ;感染文件标题

N c:\h4.dat

R BX

0

R CX

0A00

W 1000

Q

注意：红色部分文字是感染后增加的病毒数据或病毒修改的数据。

2、h4.exe的获得

2.1 执行批处理文件，生成数据文件h4.dat

debug < hello4.txt

2.2 复制数据文件，生成可执行文件h4.exe

copy h4.dat h4.exe

2.3 运行新生成的可执行文件h4.exe，运行效果如图1所示。