一种新型计算机病毒的分析和诊治

周建钦 （曲阜师范大学数学系）

笔者最近发现了一种新的良性计算机病毒，用现有的CPAV,SCAN等反病毒软件都不能诊治。感染该病毒的程序比原来增加了1465个字节，因而笔者称这种病毒为1465病毒。分析了该病毒的程序后，用C语言编制了诊治该病毒的程序。

1465病毒附在COM和EXE文件的后部。运行有毒文件时，首先执行病毒部分。病毒先检查21号中断，如果21号中断已感染病毒，则执行文件的正常部分；如果21号中断未感染病毒，则修改21号中断，使其附有1465病毒，并感染COMMAND.COM文件。在内存感染的情况下使用DIR命令，感染相应的COM和EXE文件，并显示文件原来的长度，如果使用COPY命令复制COM或EXE文件，则感染源文件和目标文件。

下面是病毒程序的一部分：

```
119   call    1do     ;检测21号中断是否被感染
11c   pop     si
11d   jz      0123    ;若感染则去执行程序的正常部分
11f   push    cs
120   call    0179    ;去感染21号中断
123   mov     di,0100; 正常COM文件从100处开始执行
126   push    di
127   add     si,0524
12b   mov     cl,05
12d   call    0273    ;恢复COM文件的前5个字节
130   pop     si
131   pop     sp
132   jmp     si      ;从100处执行正常文件
```

消除病毒有两种方法，一种是彻底清除病毒，恢复正常文件，这时工作量较大。另一种比较简单，只需修改一个字节即可，即将11d句的jz 0123改为jmp 0123。这样病毒没有机会感染21号中断，既不影响程序的正常执行，也不会感染其它可执行文件，同时这样修改的文件具有了免疫功能，即不会再被1465病毒感染。

下面是诊治病毒的C语言程序的一部分：

```
int antivirus (char * specifile) / * return 1:ok,0:infected * /
{
    char ch,cc;
    int fold,fnew,i=0;
    long count,last,lseek();
    fcount++;
    printf("%S",specifile);
    if((fold=open(specifile,O__RDWR   O__BINARY))<0)
    {
      printf("Techkey antivirus can't open %s\n",specifile);
      return(1);
    }
    last=lseek(fold,01,2);
    count=14651;
    lseek(fold,-count,2)    ;/ * 找到病毒可能在的起始位置 * /
    read(fold,&ch,1);
    if(ch==\x8b')           / * 以下判断是否感染病毒 * /
    {
    read(fold,&ch,1);
    if (ch==\xc4')
      {
    read(fold,&ch,1);
    if(ch==\x8b')
        {
    read(fold,&ch,1);
    if(ch==\xe6')
          {
    read(fold,&ch,1);
    if(ch==\x81')
            {
    ch=\x0eb';
    count=14441;
    lseek(fold,-count,2);
    read(fold,&cc,1);
    if(cc==\x74')
    {
    / * 将病毒中的 jz xxxx 语句改为 jmp xxxx 语句 * /
    lseek(fold,-count,2);
    write(fold,&ch,1);
    }
    count=13891;
    lseek(fold,-count,2);
    read(fold,&cc,1);
    if(cc==\x74')
    {
    / * 将病毒中的 jz xxxx 语句改为 jmp xxxx 语句 * /
    lseek(fold,-count,2);
    write(fold,&ch,1);
    printf("delete the virus successfully\n");
    }
    close(fold);
    return(0);
    }    }}}}
    close(fold);
    return(1);
}
```