```
'-', '=', 0, 0, 'Q', 'W', 'E', 'R', 'T', 'Y', 'U', 'I',
'O', 'P', '[', ']', 0, 0, 0, 'A', 'S', 'D', 'F', 'G', 'H',
'J', 'K', 'L', ';', '\'', '`', 0, '\\', 'Z', 'X', 'C',
'V', 'B', 'N', 'M', ',', '.', '/', 0, 0, 0};
main()
{
int i;
printf("Password 1.0! / nCopywrite by Wang Yong Wu! / n / n");
for (i=0;i<7;i++)
{outp(PORTINDEX,(char)i+BEGIN);
redbuf[i]=inp(PORTDATA);
printf("The password number%d is :%x / n",i,readbuf[i]);
} / read from cmos 37h--3dh
printf(" / n");
m unpass();
printf(f" / n");
scan unpass();
printf("OK"! / n");
return 0;
}
void m unpass(void)
{
int i;
unsigned char buf,shift;
readbuf[0] &=0xf0;
for (i=0;i<6;i++)
{if(!readbuf[i+1])break;
passwd[i]=1;buf=readbuf[i];
for(;;)
{shift=((buf & 0x80)>>7)+((buf & 0x40)>>6)
+((buf & 0x02)>>1)+buf & 0x1;
shift=(shift & 0x1)<<7;
buf=(buf>>1)|shift;
if(buf==readbuf[i+1]    passwd[i]='?';
}
printf("IF use M queue; The password is:%s / n",passwd);
}
void scan unpass(void)
{
int i;
for (i=1;i<7;i++)
{if(!readbuf[i] break;
if(!scan[readbuf[i]])passwd[i-1]='?';
else passwd[i-1]=scan[readbuf[i]];
}
printf("IF use scan code;The password is:%s / n",passwd);
}
```

用0磁道格式化清除主引导区新病毒

董翔英　　(海军后勤学院)

摘要:本文介绍一种不能用覆盖法清除的主引导区病毒的解决办法。

我单位两台长城386微机不慎被人安装某一不知名的财务软件,感染了一个未曾见过的病毒,导致硬盘不能启动。采取一般方法,如用软件杀毒法、主引导区覆盖法、物理格式化后重新分区法,均不见效。最后在万般无奈时,采取将硬盘0头0面0道单独格式化后,才消除了病毒。现将该病毒的病毒现象及消除过程介绍给大家,期望在病毒日益猖厥的今天,能够有助于同行在工作中遇到同类病毒袭击时,开拓思路,清除病毒。

一、病毒现象

1.开机系统自检正常,当A驱不插系统盘时,C盘不能启动机器,并且A驱灯亮,发出沉重的读盘声响,持继不断;

2.当A驱插入系统盘后,系统启动成功。能转C盘,并且此后一切读写操作均正常;

3.当启动时按下DEL键试图进入系统设置,则询问口令(原系统设置并无口令检测);

4.用软盘启动后读出主引导扇区内容,发现分区表仍是正确的,但主引导程序已是面目全非。很显然,该机主引导区已被病毒感染;

5.用手中现有的最高版本的杀毒软件,如:CPAV、KILL、SCAN等进行清毒时,均查不出该病毒;

6.当进入DEBUG,试图将好的主引导区写至该机的坏主引导区时,硬盘指示灯不亮,系统不能进行写操作;

7.用FDISK删除所有分区(该机只有一个DOS分区),进行硬盘重新分区,屏幕显示error disk write,操作失败;

8.用DM的自动方式作硬盘物理格式化时,硬盘类

型设置正确，但硬盘指示灯不亮，屏幕仍显示 error disk write，操作失败。

二、解决步骤

1.用 DOS5.0 系统盘启动后，运行 A 盘上 DEBUG；

2.用 DEBUG 汇编命令，将硬盘 0 头 0 面 0 道格式化；

```
-a100
XXXX:0100 MOV AH,05
XXXX:0102 MOV BX,800
XXXX:0105 MOV CX,0000
XXXX:0108 MOV DX,0080
XXXX:010B INT13
XXXX:010D INT3
XXXX:010E
-e800
```

将 800H 至 821H 的连续 34 个内存单元的内容改为：

```
00 01 00 02 00 03 00 04 00 05 00 06 00 07 00 08 00 09 00 0A
00 0B 00 0C 00 0D 00 0E 00 0F 00 10 00 11
-g=100
```

3.用 DEBUG 汇编命令，将主引导区内容读出；

```
-a100
XXXX:0100 MOV AX,0201
XXXX:0103 MOV BX,0200
XXXX:0106 MOV CX,0001
XXXX:0109 MOV DX,0080
XXXX:010C INT13
XXXX:010E INT3
XXXX:010F
-g=100
-d200
```

屏幕显示主引导扇区为全 0 数据；

4.将好的主引导区写入该机，该机正确的主引导扇区在 DON1 盘的第 10 扇，将 DON1 盘插入 A 驱，

```
-l200 0 10 1          (装入正确的主引导区)
-a100
XXXX:0100 MOV AX,0301  (将读操作改为写操作)
-g=100
```

此时硬盘灯亮，操作成功。

5.开机，硬盘启动成功。且硬盘数据完好无损。

三、分析与结论

该病毒属主引导区病毒，是一种恶性病毒。开机无论是否用 A 盘启动，只要系统检测到 C 盘，病毒就被激活，即内存就已带毒。并且该病毒具有自我保护的能力，拒绝用户改写主引导区。当用户遇到这种不能用主引导区覆盖法消除的主引导区型病毒，并且所有的杀毒软件均无能为力时，为了不破坏硬盘中的大量参数，可以用 0 磁道格式化法，只格式化硬盘 0 头 0 面 0 道。对于一般容量的硬盘（如该机硬盘为 40M），0 道的 17 个扇区为系统的隐藏扇区，0 道格式化不破坏存放在 0 磁道以外的数据，即不破坏 DOS 分区内及其它分区内的所有数据，并可将存在于隐藏扇区内的病毒程序一并清除。当 0 道格式化成功后，再将保存的该机的主引导区备份写回即可，或读另一相同机型相同系统的主引导区写入该机。我们用该方法成功地恢复了这两台机器。

当我们将事先已保存下来的病毒再反复感染该机，经不断分析研究，发现该病毒有个特点，病毒拒绝用户覆盖主引导区时，若用户强行用 DM 手动方式操作，硬盘格式化虽然正常，重建分区也正确，但重新开机启动时，C 盘与 A 盘全部丢失，系统瘫痪。很明显这是硬盘格式化时，病毒再次发作，改写 CMOS，丢失所有硬盘和软盘所致。此时只能将 CMOS 放电，使系统开机时 CMOS 检测失败，从而进入系统设置，恢复 C 盘、A 盘、B 盘。关于如何将 CMOS 放电的方法，许多杂志及报刊上都有论述，在此不再介绍。

另外，当用户用 A 盘启动并执行 A 盘上的 DEBUG 文件时，注意 A 盘应贴上写保护缺口，否则在内存带毒的时候，很容易感染 A 盘。当 DEBUG 程序带毒，则格式化 0 道后仍不能覆盖主引导扇区。

dBASEⅢ数据库的简单加密

李红胜 （随州市第一人民医院）

现在被广泛使用的数据库管理系统 FoxBASE、FoxPRO 以及 Clipper，为了程序的保密，在 FoxBASE 中提供了伪编译功能；FoxPRO 和 Clipper 则完全具备了真正的编译功能。这样无疑是保护了程序设计人员的劳动，也保证了所设计软件的健康运行。但是为保证软件的兼容性和数据的继承性，这些数据库管理系统全都较好地保留了 dBASE Ⅲ 的数据库结构，而 dBASEⅢ 的数据库是可以在 dBASEⅢ、FoxBASE 或 FoxPRO 中直接进行操作的。也就是说，我们使用以上数据库管理系