一个实用的计算机病毒检测程序

云南保山建设银行 江 文

目前检测计算机病毒的方法多种多样，对计算机用户而言动手自己编写个检测计算机病毒的程序，加入自动批处理中做“看门狗”，无疑是一件爽心悦目的事情。笔者在本文中给出一个用 TURBO C2.0 编写的实用检测程序 SVR.EXE，该检测程序能对内存性病毒及文件性病毒进行检测并将每次检测的时间和检测结果登记在案。SVR.EXE 的检测原理如下：

1.利用 DOS INT12H 得到计算机的实际内存大小，扫描被检测计算机的内存，获取计算机是否被病毒感染的信息。

2.对文件性病毒的检测，笔者没用剖析病毒内码的办法进行检测，而是用一种既简单又直观的“笨”办法进行检测，计算机每次开机首先运行 COMMAND.COM，故 COMMAND.COM 是病毒攻击的第一对象，判断 COMMAND.COM 的大小便能得知文件性病毒是否侵入的信息。笔者在程序中给出了 DOS 2.11 至 DOS 3.31 及目前流行的 DOS 5.00 的 COMMAND.COM 文件长度，同时考虑到 MS-DOS 同 PC-DOS 的差别及其它问题，用检测得到的 COMMAND.COM 文件长度除 100 得到的数进行判断。

经检测，如果实际内存小于 64KB 或 COMMAND.COM 文件长度不满足判断条件时，程序将拉响警笛进行报警，提示发现计算机病毒。检测后 SVR.EXE 将检测日期及检测结果备案在 RECORD 文件中，SVR.EXE 没发现计算机病毒，备案文件中只登记检测日期，发现计算机病毒，在日期后备注一条“Found computer virus”。

SVR.EXE 的用户界面采用彩色立体画面，用户将其放入 AUTOEXE.BAT 中，SVR.EXE 便将每次开机的日期时间及检测结果存入 RECORD 文件中，为用户提供一种管理的手段（黑匣子）。原程序见附录 SVR.C

```
/*计算机病毒检测程序 SCR.C 1993 年 1 月 江文*/
#include<stdio.h>
#include<ctype.h>
#include<dos.h>
#include<dir.h>
#include<string.h>
#include<sys\stat.h>
#include<io.h>

min(argc)
{
struct ffblk f;
struct date today;
struct time now;
FILE *fp;
register long int dfv;
char pat[80];
char *p;
int disk, so1, so2;
int virus=0, vsize=0;

if(argc>1)
exit(0);
getcwd(pat, 80);
chdir(pat);
gotoxy(18,6);
textbackground(10);
cprintf(" ");
for so1=7;so1<15;so1++)
{
gotoxy(18,so1);
textbackground(10);
cprintf(" ");
textbackground(15);
cprintf(" ");
}
gotoxy(20,15);
cprintf(" ");
textcolor(14);
textbackground(10);
```

```
gotoxy(20,7);
cprintf("SVR(tm) version 2.0 (C)Copyright
  by JIANCWEN 1993.01");
textcolor(15);
gotoxy(30,8);
cprintf("SVR.EXE scan your Computer
  and Record");
gotoxy(33,9);
cprintf("%-4dKB total conventional
  memory",nc());
textcolor(14);
gotoxy(30,12);
cprintf("The People's Construction
  Bank of China");
gotoxy(33,13);cprintf("BaoShan Central
  Subbranch YunNan");
textcolor(0);
gotoxy(20,14);
cprintf("Addr:BanShan YunNan
  Tel:0875-20436 PostCode:678000");
textcolor(15);
if(nc()<640)    /*检测计算机内存*/
{
gotoxy(37,10);
cprintf("SVR Found Computer Virus");
virus=1;
}
dfv=findfirst("\\*.*",&f,23);
while(!dfv)
{
if(!strcmp(f.ff_name,l"COMMAND.COM"))/
  *扫描 COMMAND.COM 文件,获取文件长度*/
vsize=f.ff_fsie/100;
dfv=findnext(&f);
}
if(vsize!=0&&vsize!=478&&vsize!
  =232&&vsize!=253&&vsize!=237&&vsize!=159&&vsize!=2
52)
{
vsize=0;
gotoxy(37,10);
cprintf("SVR Found Computer Virus");
virus=2;
}
if(virus!=0)    /*警笛报警部分*/
{
for (so1=0;so1<800;so1=so1+4)
{
sound(100+so1);
delay(40);
}
for (so1=0;so1<20;so1++)
{
for(so2=0;so2<600;so2++)
{
sound(600+so2);
delay(1);
}
}
nosound();
}
if(virus=0)
{
gotoxy(33,10);
cprintf("SVR have not find Computer Virus");
}
if((fp=fopen("record","a"))==NULL)/*
  在 RECORD 文件中记录检测时间及检测结果*/
{
puts("can not open file");
exit(0);
}
getdate(&today);
gettime(&now);
if(virus!=0)
fprintf(fp,"%d-%d-%d  %0.2d:%02d  Found computer
  virus\n",today.da_year,today.da_mon,
  today.da_day,now.ti_hour,now,ti_min);
else
fprintf(fp,"%d-%d-%d %02d:%02d:%02d\n",
  today.da_year, today.da_mon, today.da_day,
  now.ti_hour,now.ti_min);
fclose(fp);
gotoxy(1,16);
}
/*获取计算机的实际内存大小*/
nc()
{
union REGS regs;
int86(0X,&regs,&regs);
```