计算机病毒分析与处理

主讲人：张天庆

2010年

计算机病毒的特征

非法性

隐藏性

潜伏性

可触发性

表现性

破坏性

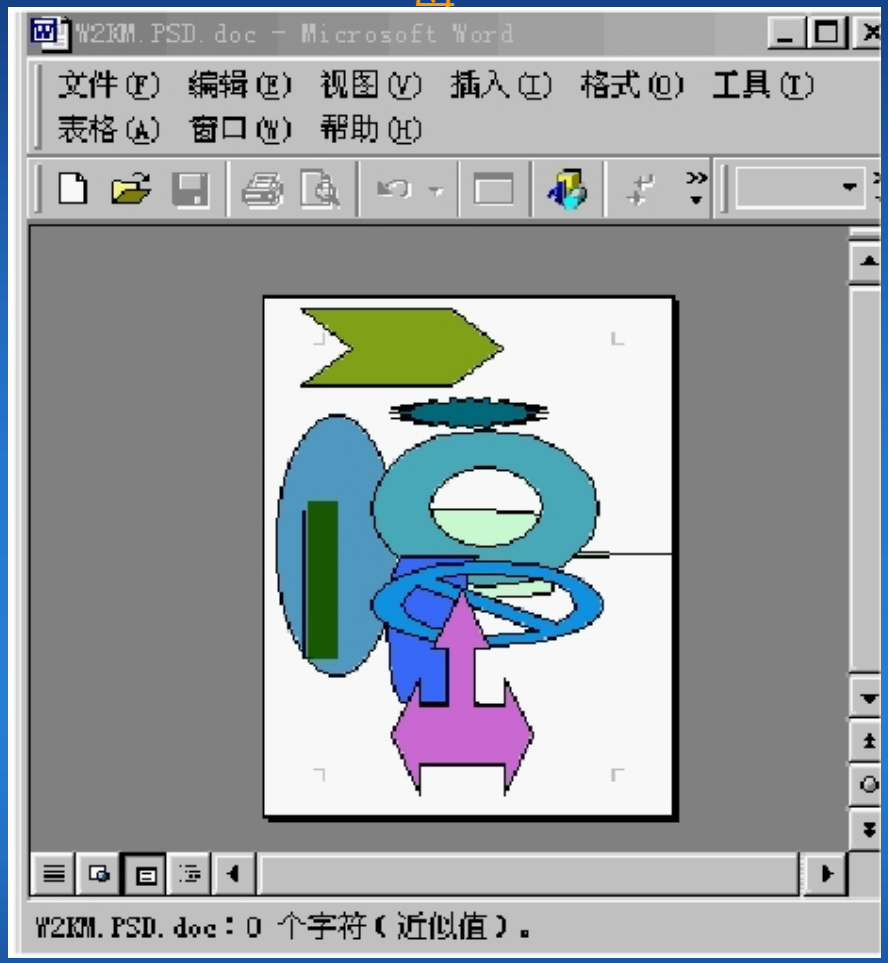
传染性

针对性

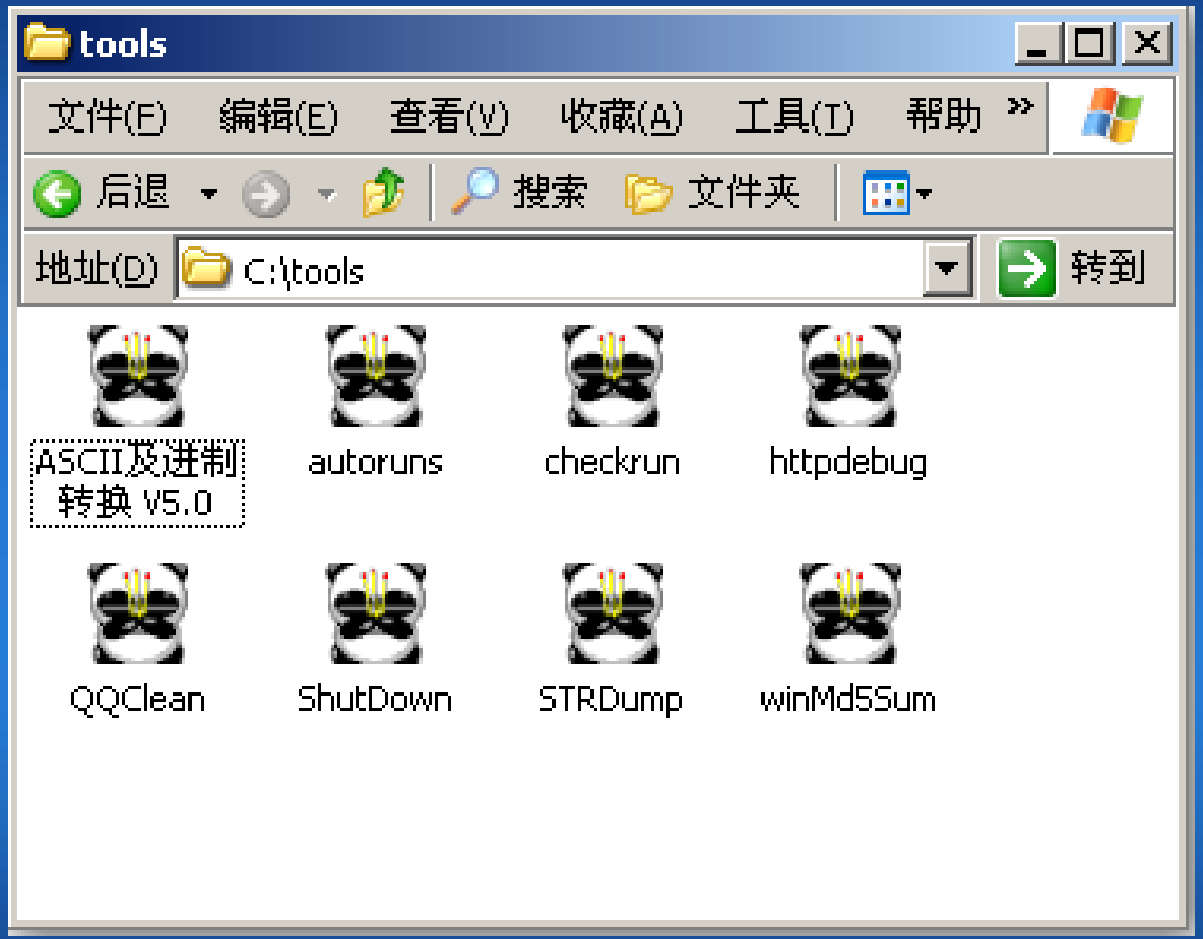
变异性

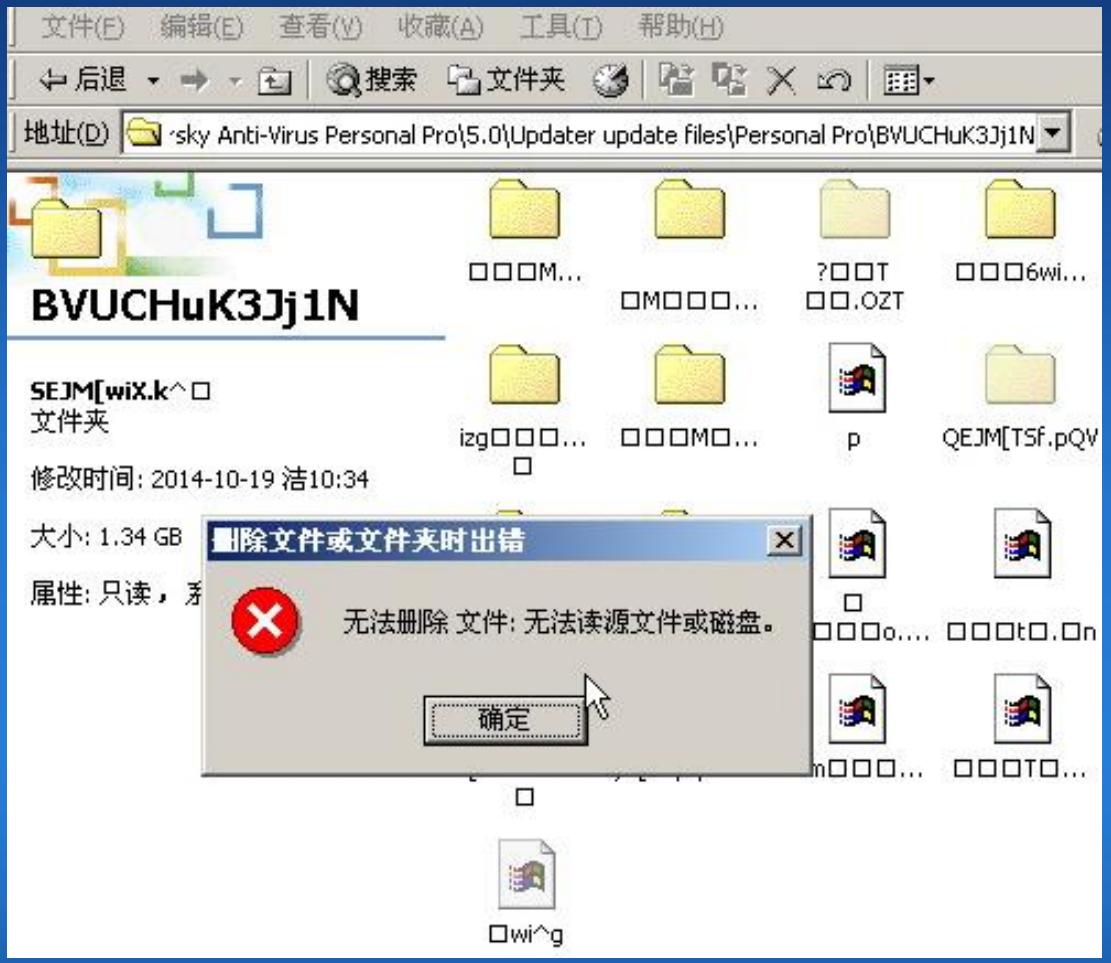
不可预见性

计算机病毒的表现性体现：“七月杀手”病毒



计算机病毒的表现性体现：“熊猫烧香”病毒




文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 文件夹
地址(D) ·sky Anti-Virus Personal Pro\5.0\Updater update files\Personal Pro\BVUCHuK3Jj1N
BVUCHuK3Jj1N
SEJM[wiX.k^□
文件夹
修改时间: 2014-10-19 洁10:34
大小: 1.34 GB
属性: 只读，
□□□M...
□M□□□...
?□□T
□□.OZT
□□□6wi...
izg□□□...
□
□□□M□...
p
QEJM[TSf.pQV
□
□□□o....
□□□t□.□n
m□□□...
□□□T□...
□
□wi^g
删除文件或文件夹时出错
无法删除 文件: 无法读源文件或磁盘。
确定

常见病毒分类

- 引导型病毒 - - MBR病毒、 BR病毒
  软（U)盘→硬盘→软（U)盘
- 文件型病毒
- 源码型病毒
- 嵌入型病毒
- 外壳型病毒
- 混合型病毒（又称复合型）

具有代表性的病毒类型

- 宏病毒：感染word、excel文件，驻留Normal模板
- 蠕虫病毒
- 特洛伊木马病毒
- 流氓软件

计算机病毒的传播途径

- 网络
- 移动存储介质
- 硬盘
- 光盘
- 点对点通信系统和无线通道

木马的出现

- 特洛伊木马（Trojan）病毒（也叫黑客程序或后门病毒）是指隐藏在正常程序中的一段具有特殊功能的恶意代码，具备破坏和删除文件、发送密码、记录键盘和攻击等功能，会使用户系统破坏甚至瘫痪。

- 1986年第一例计算机木马

木马病毒的分类

- 针对网游的木马
- 针对网上银行的木马病毒
- 针对即时通讯工具的木马病毒
- 给计算机开后门的木马病毒
- 推广广告的木马病毒

蜜蜂大盗（Win32.Troj.MiFeng70）

- 偷窃传奇游戏的密码
- 盗窃以下软件的密码:QQ、奇迹、千年、红月、倚天、决战、大话西游、石器时代、遗忘传说、DVAQ
- 木马运行后会将自身复制到系统目录生成文件：isUn0404.exe、isUn0804.exe、isUninst.exe
- 修改注册表实现自启动

修改注册表：

在注册表主键HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run下添加键值“internet”=“%SYSTEM%”\%VIRUSNAME%“；

对注册表主键HKLM\SOFTWARE\Classes\xtfile\shell\open\command修改键值"默认"="%SYSTEM%"\%VIRUSNAME%" "%1"；

修改系统文件：

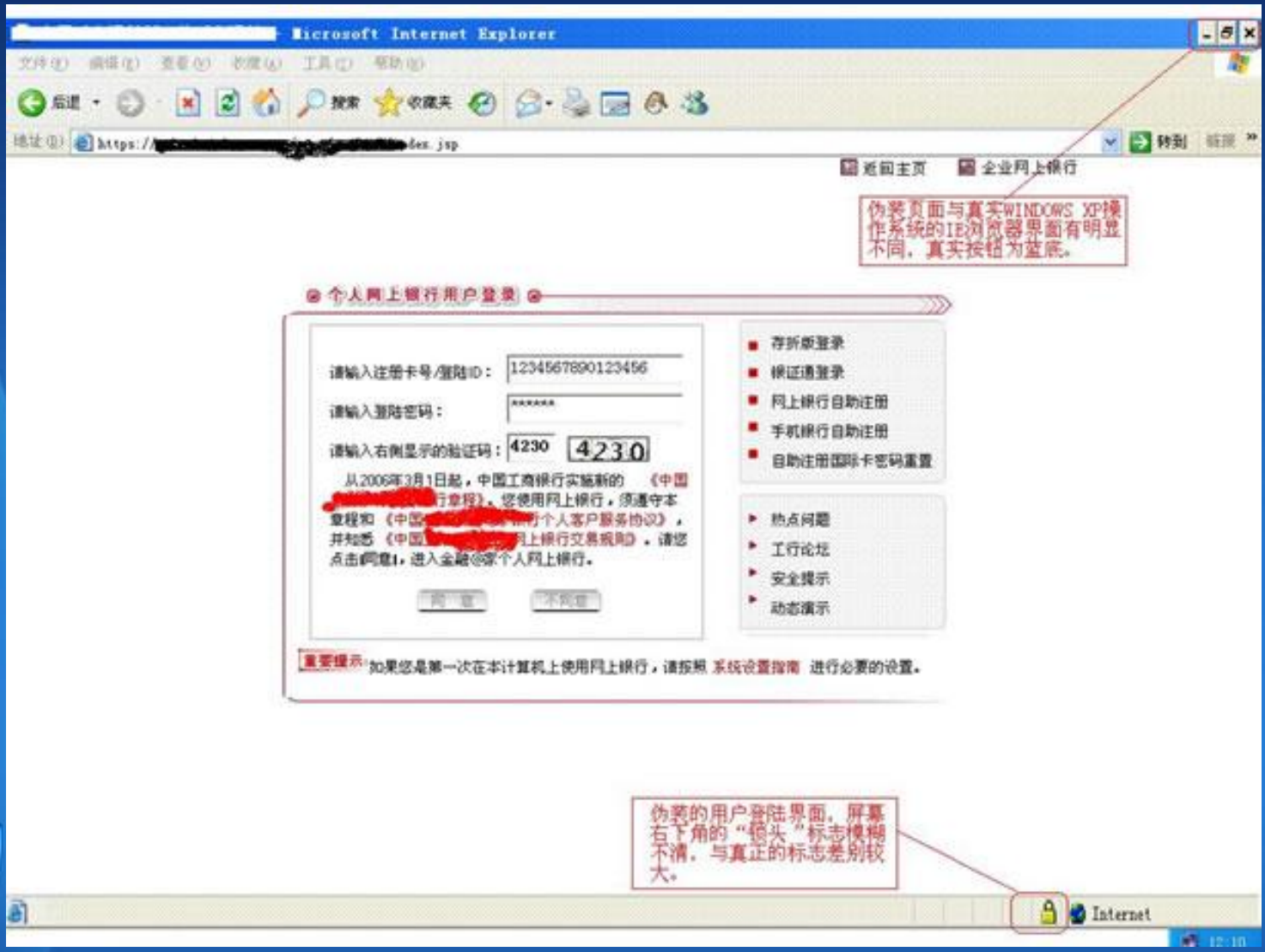
在C:Autoexec.bat中添加内容

net stop "Internet Connection Firewall(ICF)/Internet Connection Sharing(ICS)">C:BOOTEX.LOG

木马运行后硬盘会狂运作，监听UDP2222端口，监视杀毒软件木马克星、瑞星。

木马病毒的分类

- 针对网游的木马
- 针对网上银行的木马病毒
- 针对即时通讯工具的木马病毒
- 给计算机开后门的木马病毒
- 推广广告的木马病毒


Microsoft Internet Explorer
后退
搜索
收藏夹
转到
返回主页
企业网上银行
伪装页面与真实WINDOWS XP操作系统的IE浏览器界面有明显不同，真实按钮为蓝底。
个人网上银行用户登录
请输入注册卡号/登陆ID：
1234567890123456
请输入登陆密码：
******
请输入右侧显示的验证码：
4230
4230
从2006年3月1日起，中国工商银行实施新的 《中国
行章程》，您使用网上银行，须遵守本
章程和 《中国
个人客户服务协议》，
并知悉 《中国
网上银行交易规则》，请您
点击同意1，进入金融@家个人网上银行。
同 意
不同意
存折版登录
银证通登录
网上银行自助注册
手机银行自助注册
自助注册国际卡密码重置
热点问题
工行论坛
安全提示
动态演示
重要提示
如果您是第一次在本计算机上使用网上银行，请按照 系统设置指南 进行必要的设置。
伪装的用户登陆界面，屏幕右下角的“锁头”标志模糊不清，与真正的标志差别较大。
Internet


网上银行 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹 媒体
https://[redacted]/index.jsp
转到
个人网上银行
金融@家
个人网上银行用户登录
请输入注册卡号/登录ID：
请输入登录密码：
请输入右侧显示的验证码：
5810
从2006年3月1日起，中国工商银行实施新的《中国[redacted]电子银行章程》，您使用网上银行，须遵守本章程和《中国[redacted]电子银行个人客户服务协议》，并知悉《中国[redacted]人网上银行交易规则》。请您点击“同意”，进入金融@家个人网上银行。
同意
不同意
存折版登录
银证通登录
网上银行自助注册
手机银行自助注册
自助注册国际卡密码重置
国际汇款
热点问题
工行论坛
安全提示
动态演示
重要提示：如果您是第一次在本计算机上使用网上银行，请按照系统设置指南进行必要的设置。
与伪造的对比
此标志为ssl安全套接字，伪造的页面标志粗糙
完毕
Internet

木马病毒的分类

- 针对网游的木马
- 针对网上银行的木马病毒
- 针对即时通讯工具的木马病毒
- 给计算机开后门的木马病毒
- 推广广告的木马病毒

即时通讯木马病毒

可以利用即时通讯工具进行传播。中了木马后电脑会下载病毒作者指的任意程序，其危害不可确定。会造成恶作剧，比如“MSN我要结婚”病毒，中毒者会向联系人发送“我今天要结婚”的恶作剧消息。

木马病毒的分类

- 针对网游的木马
- 针对网上银行的木马病毒
- 针对即时通讯工具的木马病毒
- 给计算机开后门的木马病毒
- 推广广告的木马病毒

后门木马病毒

病毒本身不具有传播的功能，都是被恶意者种植。该木马病毒采用反弹端口技术绕过防火墙，对被感染的系统进行远程文件和注册表的操作,可以捕获被控制的电脑的屏幕,可远程重启和关闭计算机, 可以禁用系统热键和注册表编辑器，中了该木马后，被感染的系统将完全暴露于黑客手中。

木马病毒的分类

- 针对网游的木马
- 针对网上银行的木马病毒
- 针对即时通讯工具的木马病毒
- 给计算机开后门的木马病毒
- 推广广告的木马病毒

广告木马病毒

此类木马采用各种技术隐藏于系统内，修改IE等网页浏览器的主页，禁用多种系统功能，收集系统信息发送给传播广告木马的网站。更恶毒的是修改网页定向，导致一些正常的网站不能登录。最近闹的沸沸扬扬的MSN病毒就是这种木马病毒，它诱使点击一个可执行文件导致了937个网站不能正常访问。

木马病毒的工作方式

木马病毒一般分为客户端（控制端）和服务端（被控端）

利用控制端向服务端发出请求，服务端收到请求后会根据请求执行相应的动作，其中包括：

- 查看文件系统，修改、删除、获取文件；
- 查看系统注册表，修改系统设置；

通过修改系统实现自启动：

利用Autoexec.bat和Config.sys进行加载；

修改注册表；

修改Win.ini文件；

感染Windows系统文件

计算机病毒的命名

- 组成病毒名称的六个字段：
- 主行为类型.子行为类型.宿主文件类型.主名称.版本信息.主名称变种号

主名称

病毒的主名称是由分析员根据病毒体的特征字符串、特定行为或者所使用的编译平台来定的，如果无法确定则可以用字符串”Agent”来代替主名称，小于10k大小的文件可以命名为“Small”。

计算机病毒主名称

Backdoor

Dropper

Hack

Worm

Harm

Binder

Trojan

Virus

病毒名称	病毒中文名称	病毒介绍
Backdoor	后门	指在不知道也不允许的情况下，在被感染的系统上以隐蔽的方式运行。可以对被感染的系统进行远程控制，而且无法通过正常的方法禁止其运行。“后门”其实是木马的一种特例，它们之间的区别在于“后门”可以对被感染的系统进行远程控制（如：文件管理、进程控制等）。
Worm	蠕虫	指利用系统的漏洞、外发邮件、共享目录、可传输文件的软件（如：MSN、OICQ、IRC等）、可移动存储介质（如：U盘、软盘），这些方式传播自己的病毒。这种类型的病毒其子型行为类型用于表示病毒所使用的传播方式。
Trojan	木马	指在不知道也不允许的情况下，在被感染的系统上以隐蔽的方式运行，而且无法通过正常的方法禁止其运行。这种病毒通常都有利益目的，它的利益目的也就是这种病毒的子行为。
Virus	感染型病毒	指将病毒代码附加到被感染的宿主文件（如：PE文件、DOS下的COM文件、VBS文件、具有可运行宏的文件）中，使病毒代码在被感染宿主文件运行时取得运行权的病毒。
Harm	破坏性程序	指那些不会传播也不感染，运行后直接破坏本地计算机（如：格式化硬盘、大量删除文件等）导致本地计算机无法正常使用的程序。
Dropper	释放病毒的程序	指不属于正常的安装或自解压程序，并且运行后释放病毒并将它们运行。
Hack	黑客工具	指可以在本地计算机通过网络攻击其他计算机的工具。
Binder	捆绑病毒的工具	
Constructor	病毒生成器	指可以生成不同功能的病毒的程序。
Joke	玩笑程序	指运行后不会对系统造成破坏，但是会对用户造成心理恐慌的程序。
Rootkit	越权执行	设法让自己达到和内核一样的运行级别，甚至进入内核空间，这样它就拥有了和内核一样的访问权限，因而可以对内核指令进行修改。
Packer		加了某类专门针对杀毒软件免杀的壳的文件。这种壳专门针对杀毒软件作变形免杀，逃避查杀。

Trojan 的子行为类型

- Spy
- PSW
- DL
- IMMSG
- MSNMSG
- QQMSG
- ICQMSG
- UCMSG
- Proxy
- Clicker
- Dialer

主名称变种号

确为是同一家族病毒的条件:

病毒的主行为类型、行为类型、宿主文件类型、主名称均相同.

举例说明

- Trojan.DL.VBS.Agent.cgk
- Trojan.PSW.ZhengTu.afl
- Worm.Mail.Bagle.ld
- Worm.MSN.Kelvir.i
- Backdoor.Agobot.ius
- Hack.DDoSer.Boxed.bc

瑞星每月(11月)病毒疫情排TOP 5排名趋势病毒名称百分比

- 01↑3Worm.Win32.MS08-067.c
- 02↑5AdWare.Win32.Fsutk.a
- 03↑12Worm.Win32.MS08-067.a
- 04↓2Trojan.DL.Giframe.a
- 05↑1Trojan.Win32.ACAD.r

计算机病毒分析与处理

常用病毒分析方法

1. 进程和常规启动项
2. 服务项和驱动项
3. 查看劫持项和钩子，开机引导等
4. 实时分析和抓包

计算机病毒处理

1. 清理内存中的病毒
2. 清理启动项、服务项、驱动项等
3. 重启，后处理
4. 使用杀毒引擎遍历全盘

典型病毒分析

- 文件隐藏者

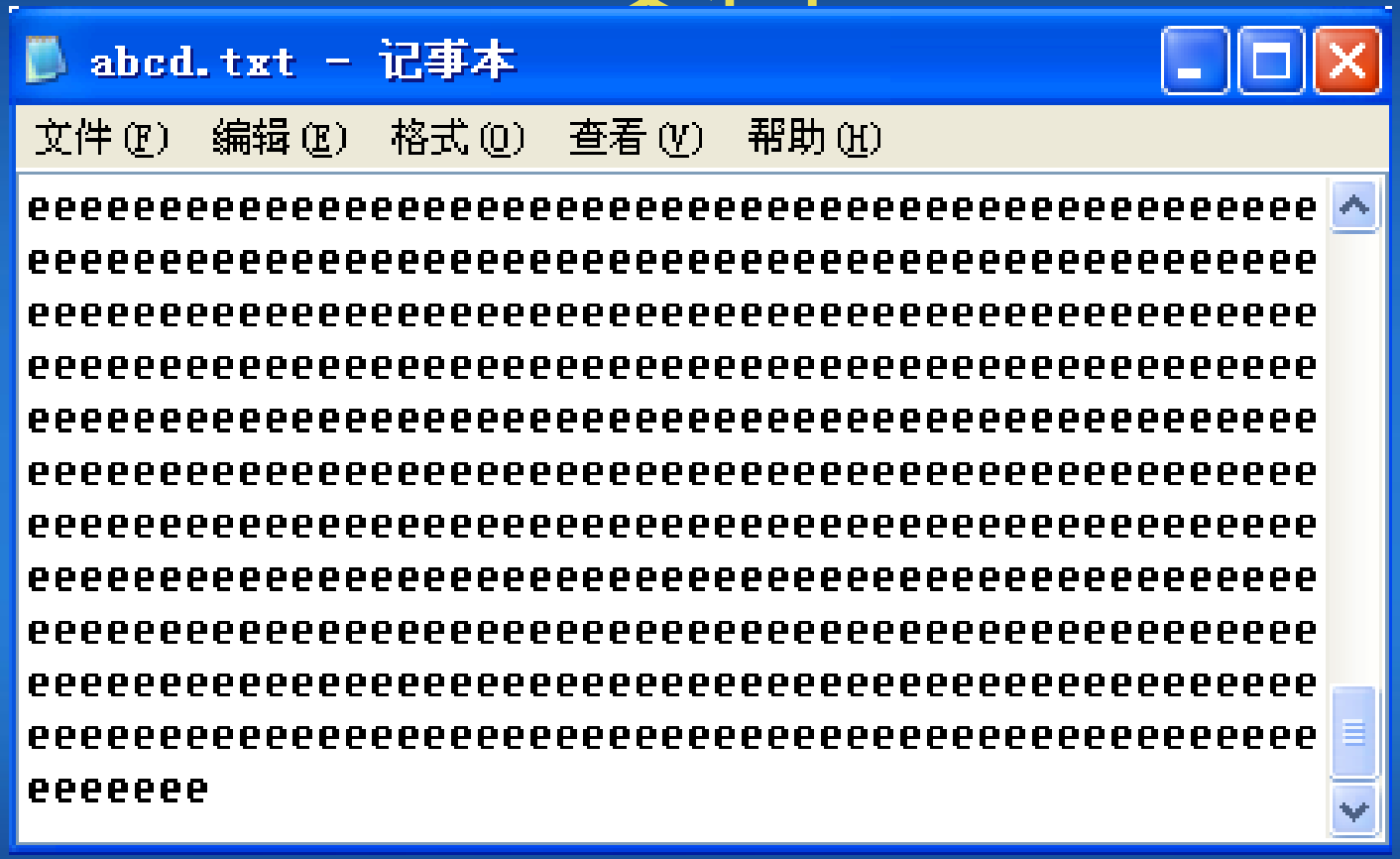
数据保密——安全删除

文件粉碎：

通过向指定磁盘区域反复填写垃圾代码的方式，使粉碎后的文件无法恢复。

瑞星杀毒软件文件粉碎功能演示

新建一个文本文档


abcd.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
eeee

分别在#575和#607扇区中看到的文件名称和文件内容

```
sector 575 (cylinder 0, head 9, sector 9)
D0 C2 BC D3 BE ED 20 20 20 20 20 08 00 00 00 00   ð┬╝Ë¥Ý      .....
00 00 00 00 00 00 A9 78 B7 38 00 00 00 00 00 00   ......©xÀ8......
E5 B0 65 FA 5E 20 00 87 65 2C 67 0F 00 D2 87 65   Õ°e·^ .çe,g..Êçe
63 68 2E 00 74 00 78 00 74 00 00 00 00 00 FF FF   ch..t.x.t.....
E5 C2 BD A8 CE C4 7E 31 54 58 54 20 00 19 B0 78   Õ┬¢¿╬─~1TXT ..°x
B7 38 B7 38 00 00 B1 78 B7 38 00 00 00 00 00 00   À8À8..±xÀ8......
41 42 43 44 20 20 20 20 54 58 54 20 18 19 B0 78   ABCD    TXT ..°x
B7 38 B7 38 00 00 D9 78 B7 38 02 00 99 68 65 00   À8À8..┘xÀ8..Öhe.
```

```
Absolute sector 607 (cylinder 0, head 9, sector 41)
0000:   65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65   eeeeeeeeeeeeeeee
0010:   65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65   eeeeeeeeeeeeeeee
0020:   65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65   eeeeeeeeeeeeeeee
0030:   65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65   eeeeeeeeeeeeeeee
0040:   65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65   eeeeeeeeeeeeeeee
0050:   65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65   eeeeeeeeeeeeeeee
0060:   65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65   eeeeeeeeeeeeeeee
0070:   65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65   eeeeeeeeeeeeeeee
0080:   65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65   eeeeeeeeeeeeeeee
0090:   65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65   eeeeeeeeeeeeeeee
```

进行常规删除后，对应扇区的变化

Absolute sector 575 (cylinder 0, head 9, sector 9)

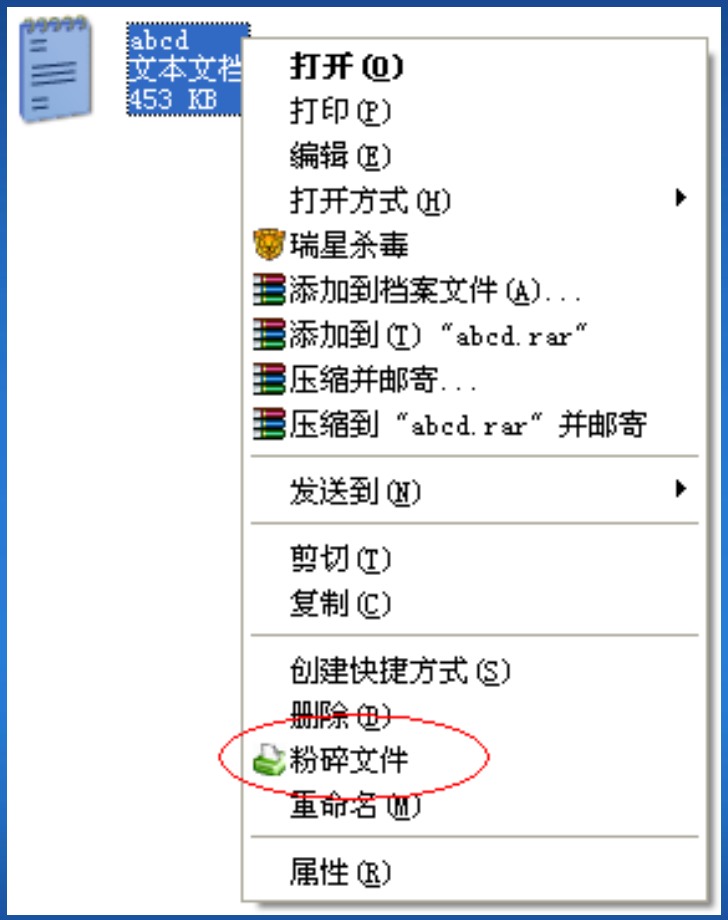
```
0000:  D0 C2 BC D3 BE ED 20 20 20 20 20 08 00 00 00 00  ð┬╝Ë¥Ý     ....
0010:  00 00 00 00 00 00 A9 78 B7 38 00 00 00 00 00 00  ......©xÀ8.....
0020:  E5 B0 65 FA 5E 20 00 87 65 2C 67 0F 00 D2 87 65  Ö▒e·^ .çe,g..Êçe
0030:  63 68 2E 00 74 00 78 00 74 00 00 00 00 00 FF FF  ch..t.x.t.....
0040:  E5 C2 BD A8 CE C4 7E 31 54 58 54 20 B0 78        Õ┬½┐╬─~1TXT ..▒x
0050:  B7 38 B7 38 00 00 B1 78 B7 38 00 00 00 00 00 00  À8À8..▒xÀ8.....
0060:  E5 42 43 44 20 20 20 20 54 58 54 20 18 19 B0 78  ÕBCD    TXT ..▒x
0070:  B7 38 B7 38 00 00 D9 78 B7 38 02 00 99 68 65 00  À8À8..┘xÀ8..Öhe
```

注意文件名称的变化

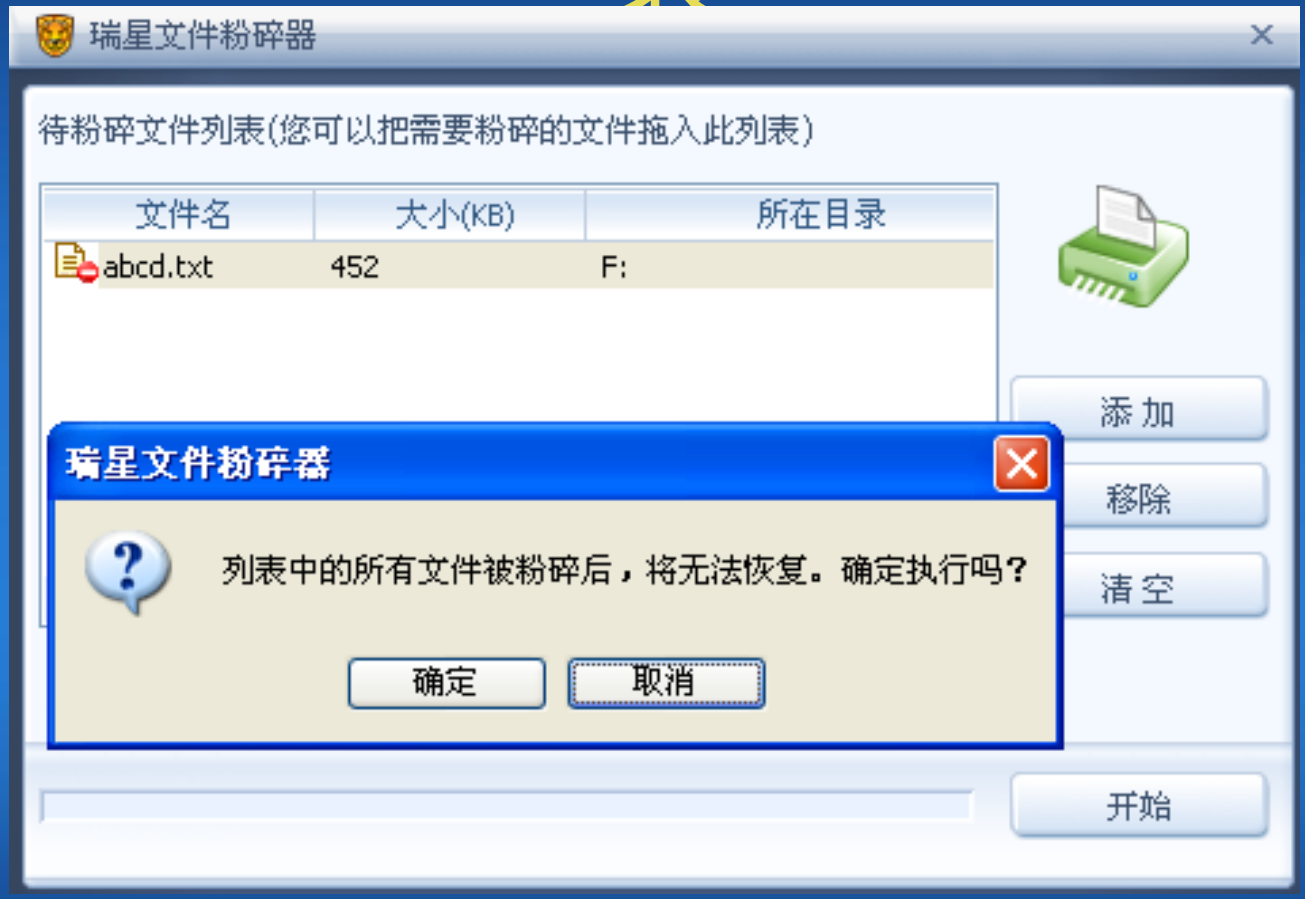
Absolute sector 607 (cylinder 0, head 9, sector 41)

```
0000:  65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65  eeeeeeeeeeeeeeee
0010:  65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65  eeeeeeeeeeeeeeee
0020:  65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65  eeeeeeeeeeeeeeee
0030:  65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65  eeeeeeeeeeeeeeee
0040:  65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65  eeeeeeeeeeeeeeee
0050:  65 65 65 65 65 65 65 65 65 65 65 65 65 65 65 65  eeeeeeeeeeeeeeee
```

使用瑞星“文件粉碎”功能对文件进行删除



待粉碎文件列表


瑞星文件粉碎器
待粉碎文件列表(您可以把需要粉碎的文件拖入此列表)
文件名
大小(KB)
所在目录
abcd.txt
452
F:
添 加
移除
清 空
瑞星文件粉碎器
列表中的所有文件被粉碎后，将无法恢复。确定执行吗？
确定
取消
开始

文件粉碎后#575、#607的扇区情况

Absolute sector 575 (cylinder 0, head 9, sector 9)

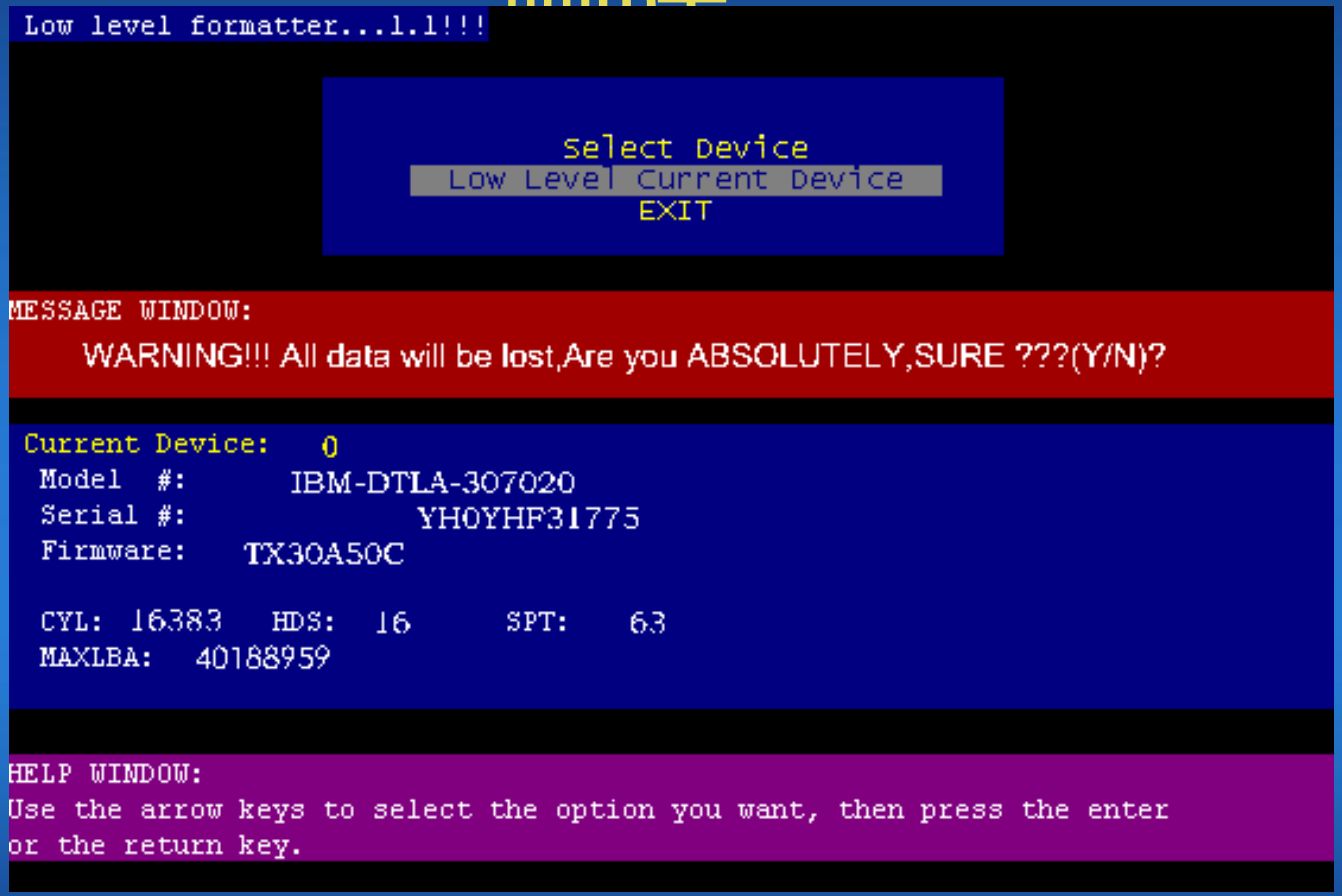
```
0000:  D0 C2 BC D3 BE ED 20 20 20 20 20 08 00 00 00 00  ð┬╝Ë¥Ý     .....
0010:  00 00 00 00 00 00 DB 7D B7 38 00 00 00 00 00 00  ......Û}·8......
0020:  E5 B0 65 FA 5E 20 00 87 65 2C 67 0F 00 D2 87 65  õ°eú^ .‡e,g..Ò‡e
0030:  63 68 2E 00 74 00 78 00 74 00 00 00 00 00 FF FF  ch..t.x.t.....ÿÿ
0040:  E5 C2 BD A8 CE C4 7E 31 54 58 54 20 00 1F E3 7D  õ┬½¨╬─~1TXT ..ã}
0050:  B7 38 B7 38 00 00 E4 7D B7 38 00 00 00 00 00 00  ·8·8..ä}·8......
0060:  E5 42 43 44 20 20 20 20 54 58 54 20 18 1F E3 7D  õBCD    TXT ..ã}
0070:  B7 38 B7 38 00 00 18 7F B7 38 02 00 74 11 07 00  ·8·8....·8..t...
```

Absolute sector 607 (cylinder 0, head 9, sector 41)

```
0000:  EF 04 00 00 FF 37 00 00 68 28 00 00 8C 0D 00 00  ï... ÿ7..h(..Œ...
0010:  74 01 00 00 73 28 00 00 43 25 00 00 97 2B 00 00  t...s(..C%..—+..
0020:  C0 6B 00 00 87 15 00 00 5F 6E 00 00 7D 62 00 00  Àk..‡... n..}b..
0030:  A4 46 00 00 56 63 00 00 BC 51 00 00 4B 19 00 00  ¤F..Vc..¼Q..K...
0040:  CB 29 00 00 73 24 00 00 ED 4A 00 00 59 03 00 00  Ë)..s$..íJ..Y...
0050:  F9 48 00 00 23 14 00 00 7A 64 00 00 22 0C 00 00  ùH..#...zd.."...
0060:  90 00 00 00 C9 00 00 00 84 48 00 00 52 35 00 00  ....É....„H..R5..
0070:  58 0B 00 00 A1 3A 00 00 A7 44 00 00 21 1B 00 00  X...¡:..§D..!...
0080:  7F 45 00 00 B1 5A 00 00 25 45 00 00 E0 12 00 00  .E..±Z..%E..à...
```

数据保密——安全删除

低级格式化



数据保密——安全删除

扇区覆盖

```
DD 0B 1F 67 7E C2 6F 97 36 43 E1 01 23 E5 D0 AF
8F 3B A1 BC 39 53 4D 24 49 17 C0 F8 25 75 09 DF
E7 A4 AF C4 35 B3 AF D9 FA 25 FF D6 A2 5D D2 42
D6 0C 10 8B A6 4A 34 0A 0A 71 A3 40 76 74 5F 6C
58 D1 27 14 16 57 E4 6D 8E 5E C3 38 74 14 13 60
C3 37 3C B1 4C C8 B5 3F E0 52 2A 54 13 06 9C CE
87 87 BD 94 A0 E6 05 3A 64 54 96 71 37 0A 60 FA
F1 D1 41 D9 5C B5 36 0E 88 42 03 A7 10 66 AB E0
66 7B AF 4D 8F 8B 22 8C B7 EC 70 FE 92 FB 5E ED
```

存储数据的扇区

```
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

被覆盖后的扇区

数据保密——消磁

硬盘消磁：

硬盘消磁机是一款能够快速彻底销毁“硬盘、磁带、软盘和磁卡”等上面所有信息的设备。