我国计算机病毒的特点和发展趋势

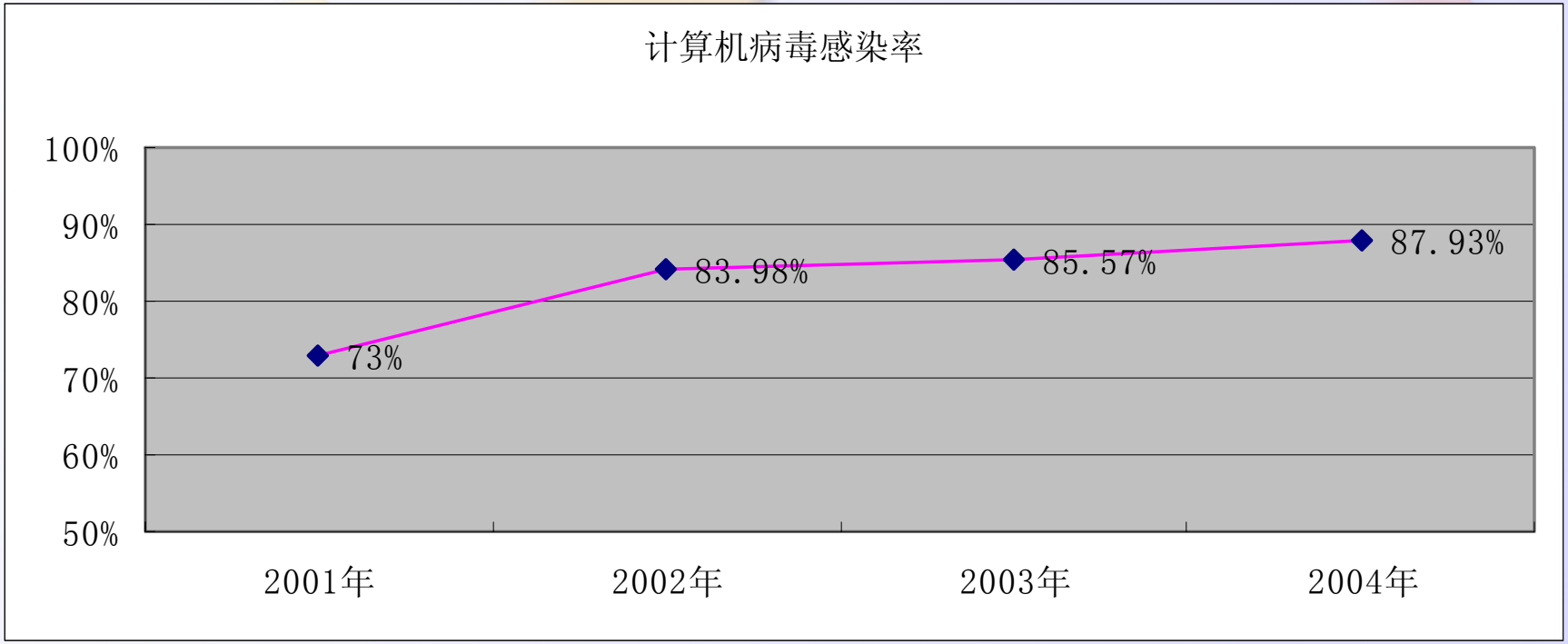
广西 桂林

张健
Zhang Jian
国家计算机病毒应急处理中心
National Computer Virus Emergency Response Center
计算机病毒防治产品检验中心
Anti-Virus Products Testing and Certification Center
Http://www.antivirus-China.org.cn
Zj@antivirus-China.org.cn

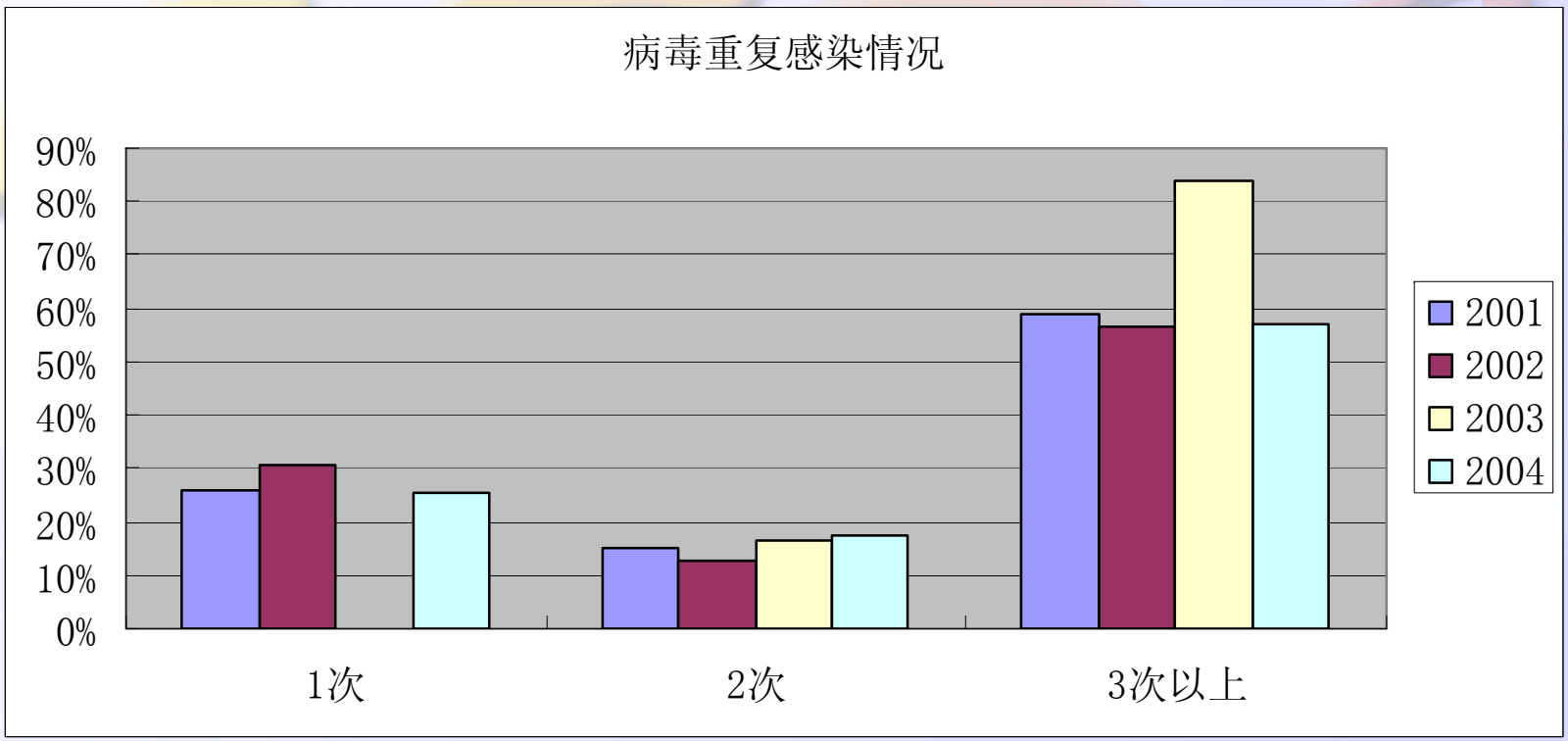
我国计算机病毒疫情调查活动简介

- 2001年4月-5月，由国信安办与公安部共同主办了我国首次计算机病毒疫情网上调查工作
- 2002年4月-5月，由公安部主办我国第二次计算机病毒疫情调查工作
- 2003年4月-6月，由公安部主办我国第三次计算机病毒疫情调查工作
- 2004年4月-5月，由公安部主办我国第四次计算机病毒疫情调查工作

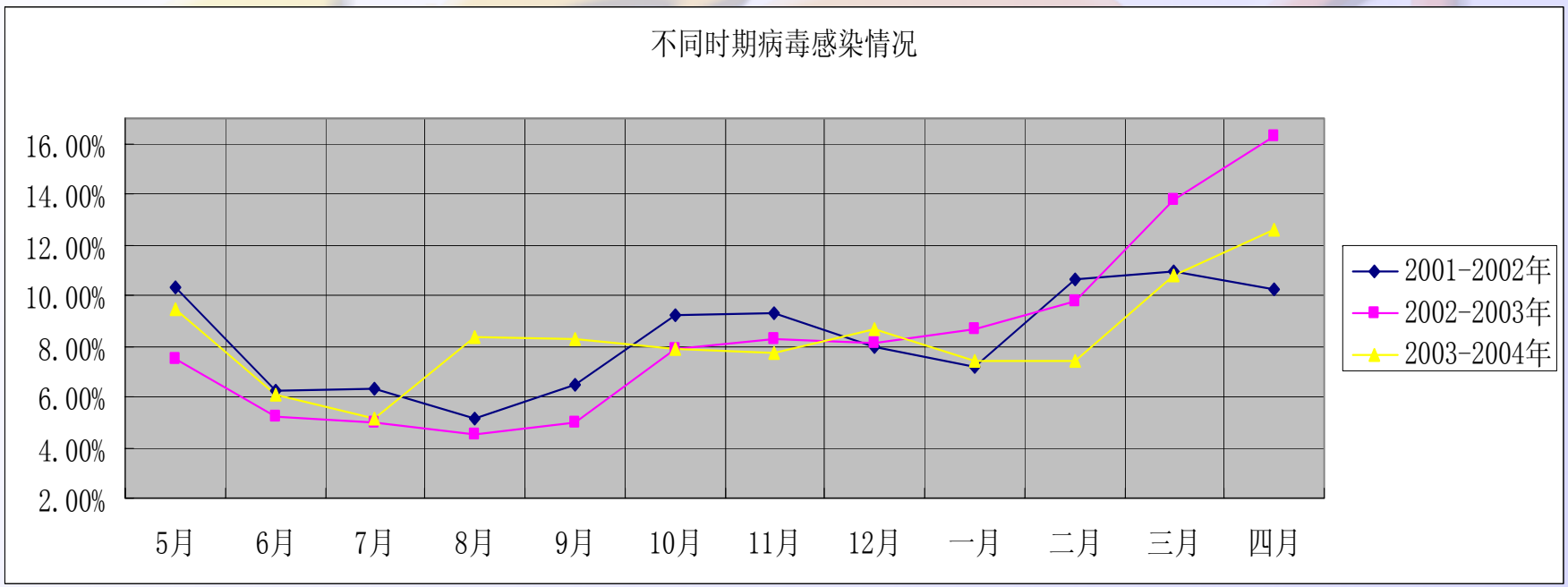
我国计算机用户病毒感染情况



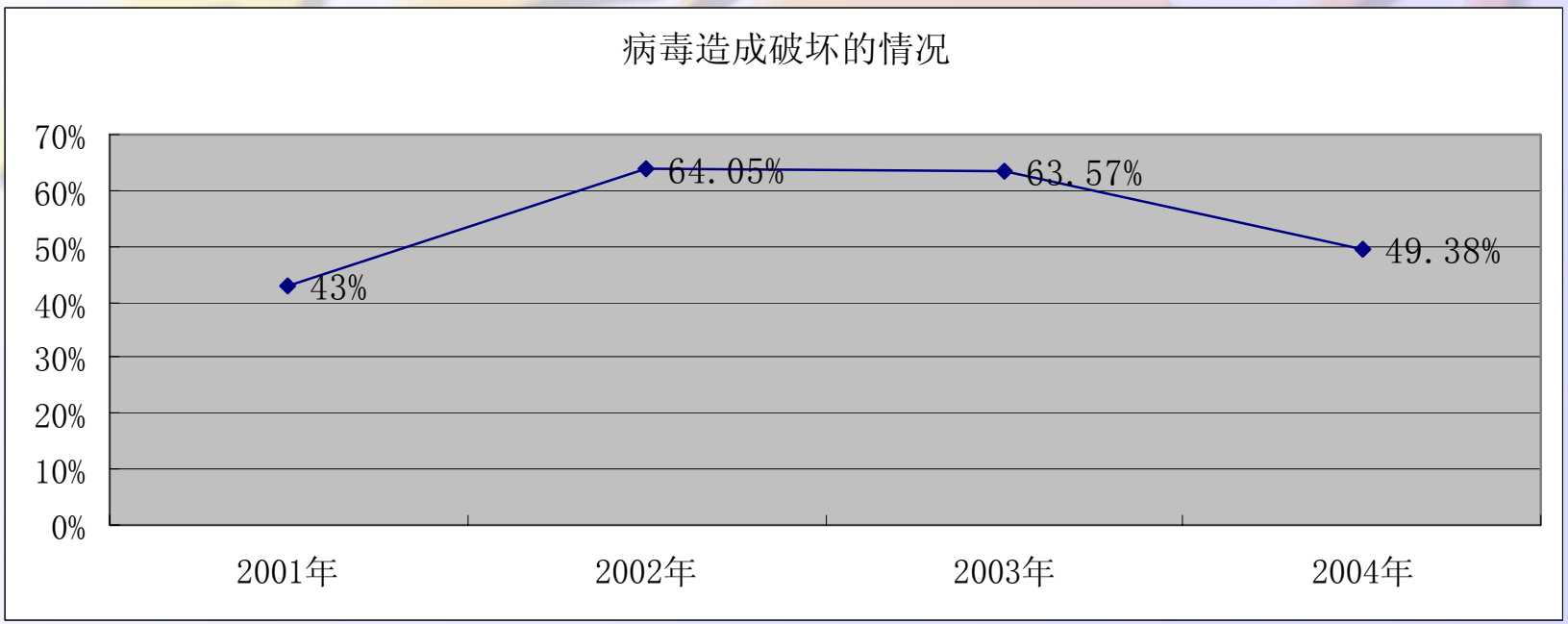
计算机用户感染病毒的次数



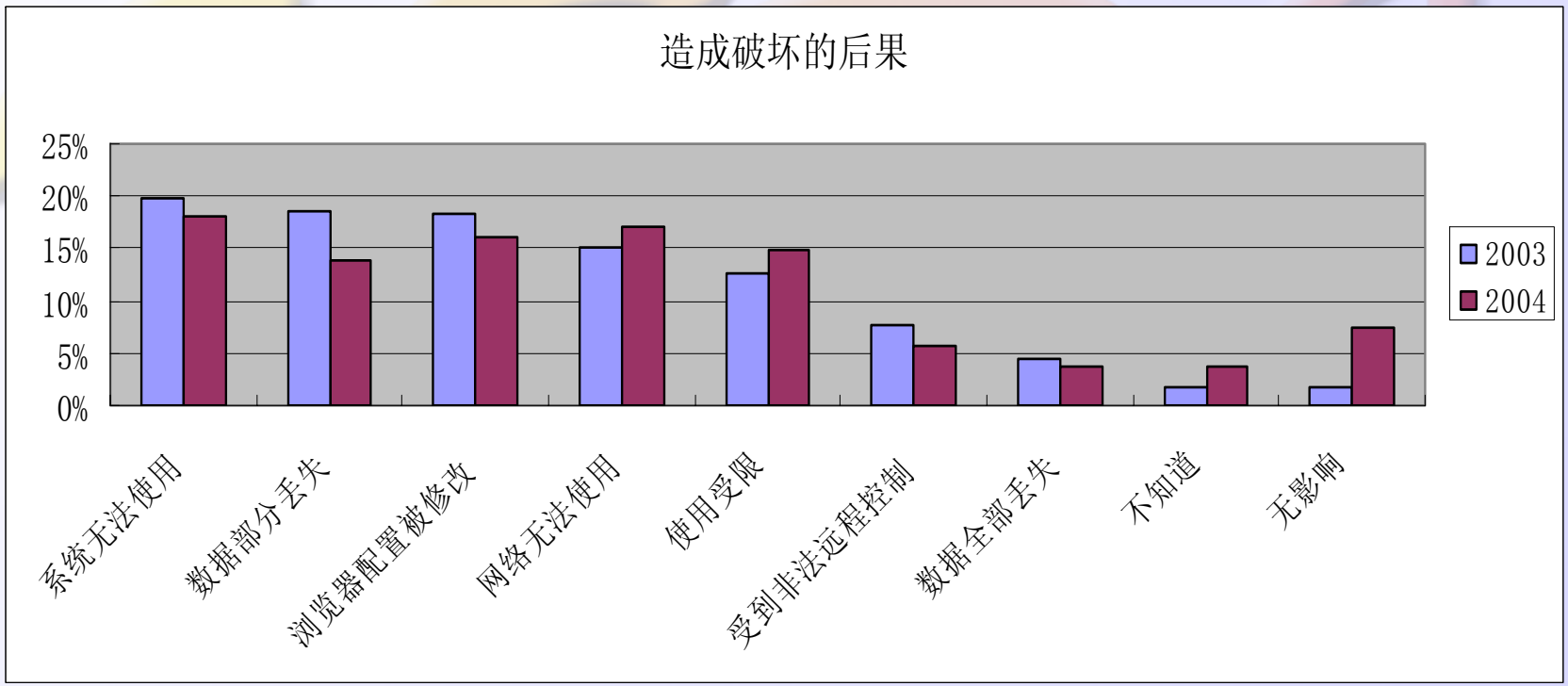
不同时期的病毒感染情况



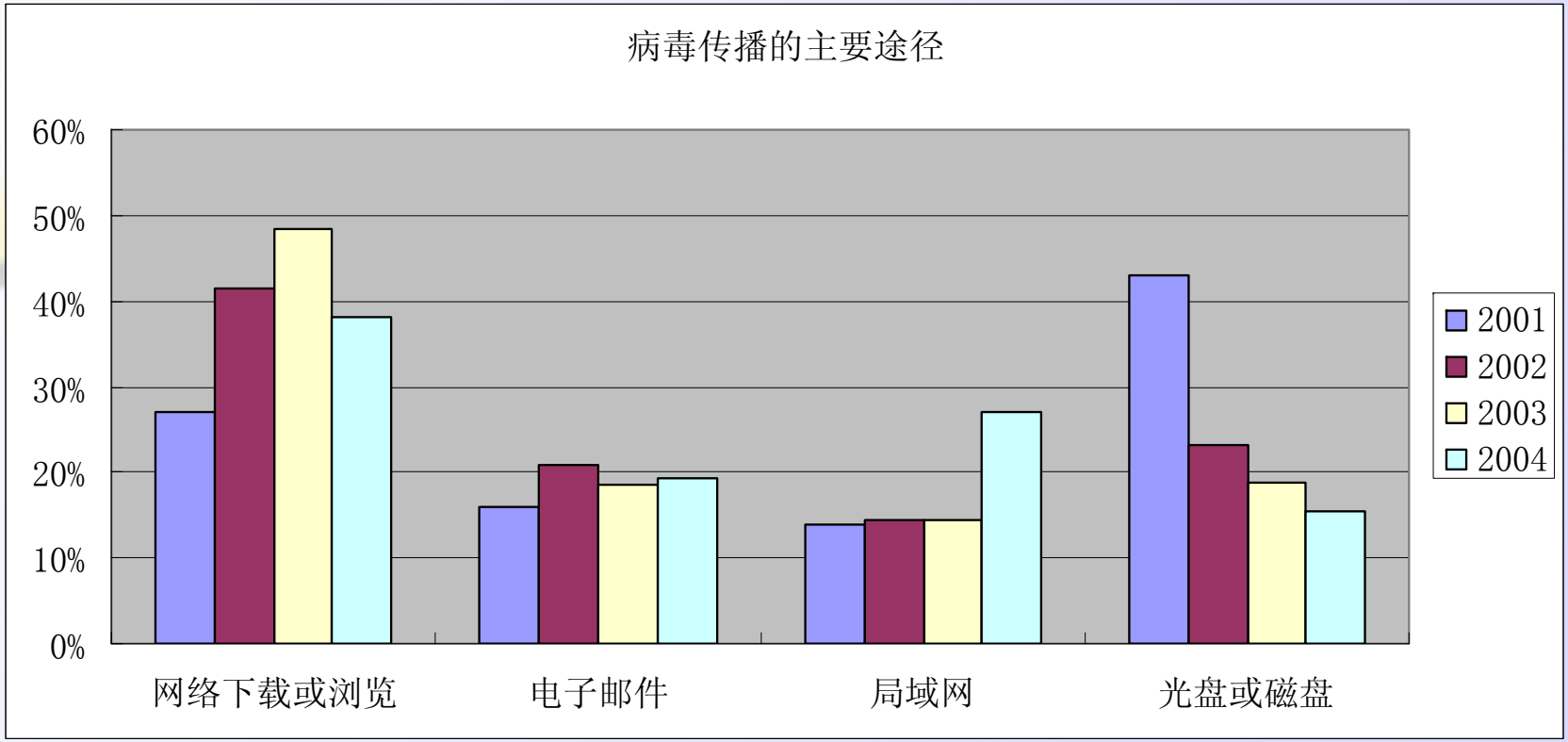
病毒造成破坏的情况


病毒造成破坏的情况
70%
60%
50%
40%
30%
20%
10%
0%
43%
64.05%
63.57%
49.38%
2001年
2002年
2003年
2004年

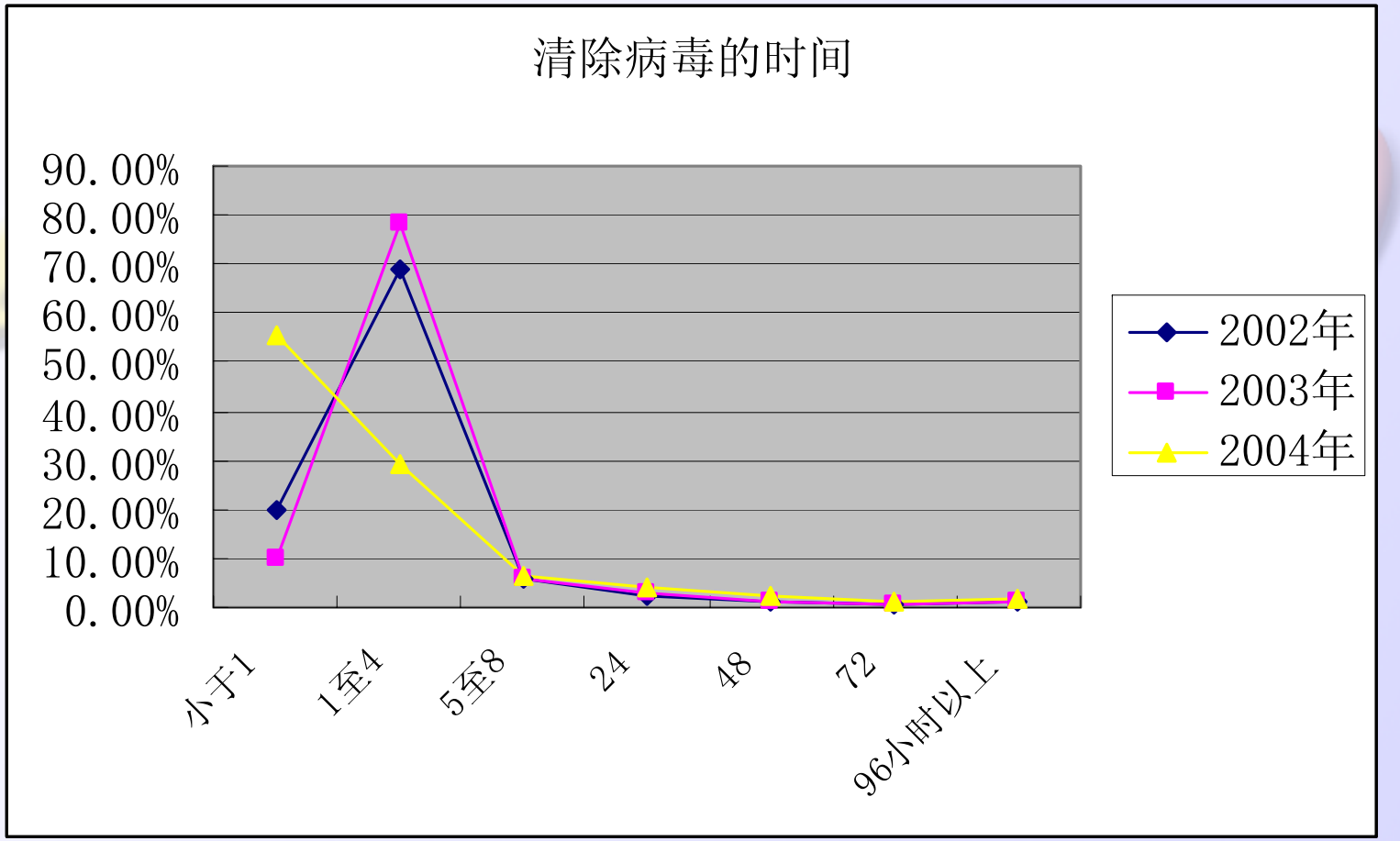
病毒破坏的后果


造成破坏的后果
25%
20%
15%
10%
5%
0%
2003
2004
系统无法使用
数据部分丢失
浏览器配置被修改
网络无法使用
使用受限
受到非法远程控制
数据全部丢失
不知道
无影响

病毒传播的主要途径


病毒传播的主要途径
60%
50%
40%
30%
20%
10%
0%
网络下载或浏览
电子邮件
局域网
光盘或磁盘
2001
2002
2003
2004

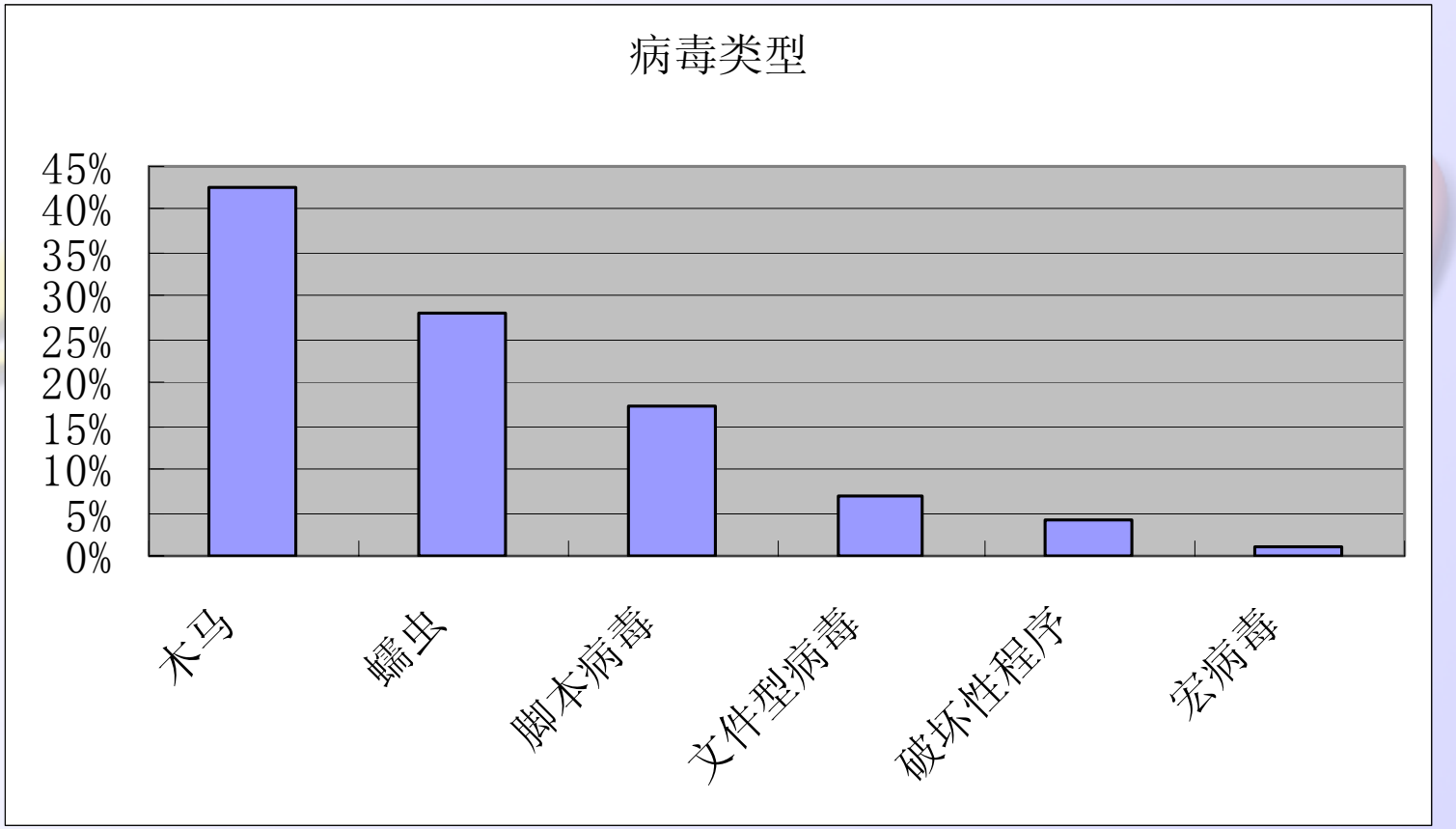
清除病毒的时间


清除病毒的时间
90.00%
80.00%
70.00%
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
小于1
1至4
5至8
24
48
72
96小时以上
2002年
2003年
2004年

我国最流行的十种病毒

时间 / 排名	(2001, 5)	(2002, 5)	(2003, 5)	(2004，5)
1	CIH	Exploit	Redlof	Netsky
2	Funlove	Nimda	Spage	Redlof
3	Binghe	Binghe	Nimda	Homepage
4	W97M.marker	JS.Seeker	Trojan.QQKiller6.8.ser	Unknown mail
5	MTX	Happytime	Klez	Lovegate
6	Troj.erase	Funlove	Funlove	Funlove
7	BO	Klez	JS.AppletAcx	htadropper
8	YAI	CIH	Mail.virus	Webimport
9	wyx	Gop	Script.exploit.htm.page	activeXComponent
10	Troj.gdoor	Troj.netthief	Hack.crack.foxmail	wyx

感染病毒的类型



近期安全事件回顾

- 英国警方的国家高科技犯罪小组破获一起网上银行“抢劫”案，有人侵入日本三井住友银行英国分行的电脑系统，利用一种能够记录键盘输入活动的病毒软件，盗取银行账号和密码。试图将**2.2**亿英镑**(**约合**4.23**亿美元**)**转移至他们分别在不同国家开设的**10**个账户。

黑客操控六万台电脑制造攻击网络 近日落网

- 德国计算机安全专家警告，全球至少有**100**万部个人电脑受控于黑客成为“肉机”。

- 通过IM(即时通讯)传播的病毒每月以50%的速度递增
- 理论上，可以在30秒内感染50万台电脑

病毒的发展趋势

- 黑客、木马和间谍软件数量大幅度增长
- Botnet日益严重
- IM和P2P软件成为传播病毒主要途径
- Phishing成为新的网络公害
- 病毒的目的性愈来愈强
- 手机病毒提高防范程度
- 警惕利用IM等应用软件漏洞自动传播的病毒

计算机病毒破坏方式

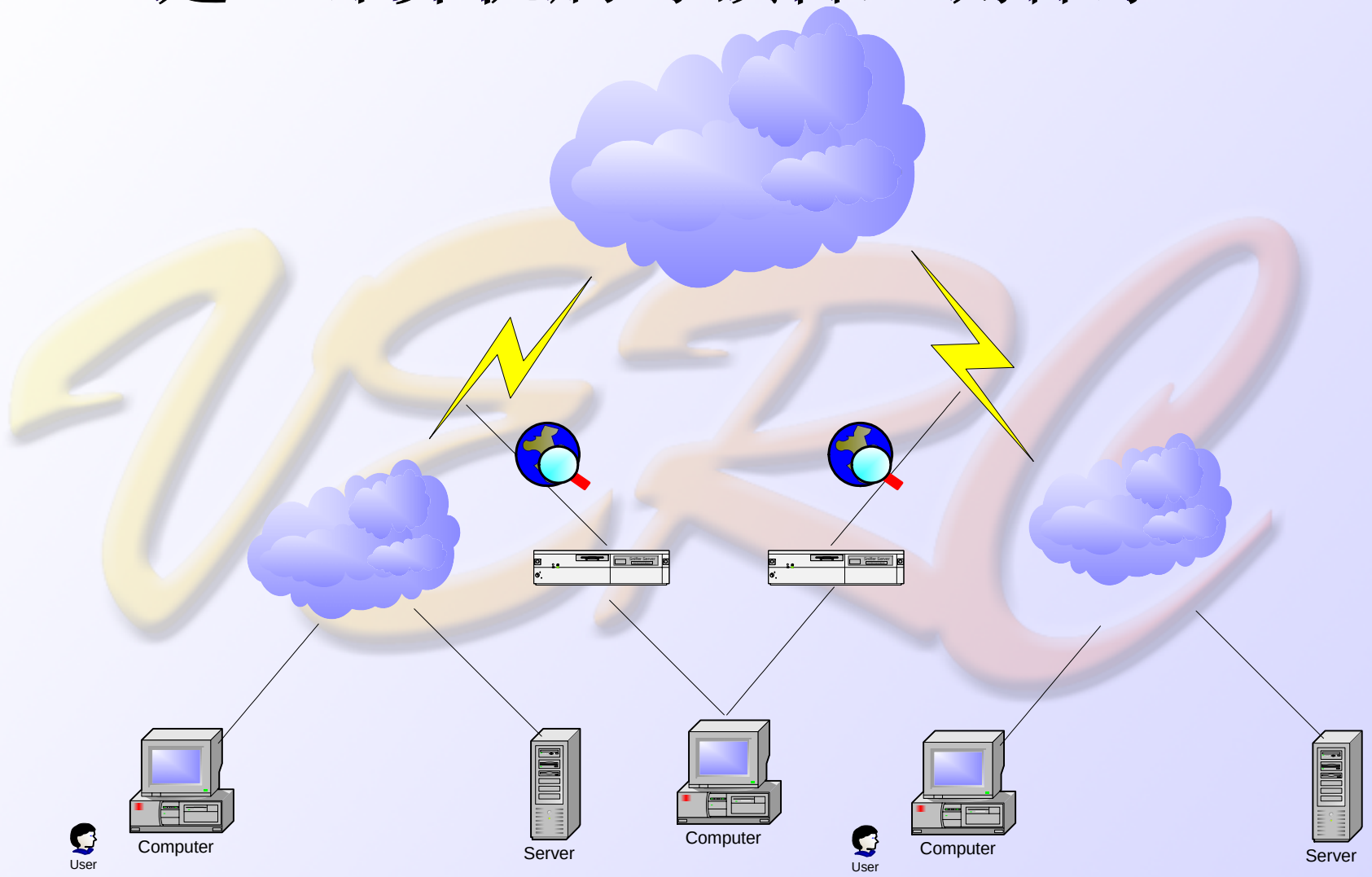
- 显性的破坏方式
  - 以破坏网络通讯为目的，大量消耗网络资源，造成网络阻塞瘫痪
  - 以破坏系统为目的，造成数据丢失、系统瘫痪、崩溃

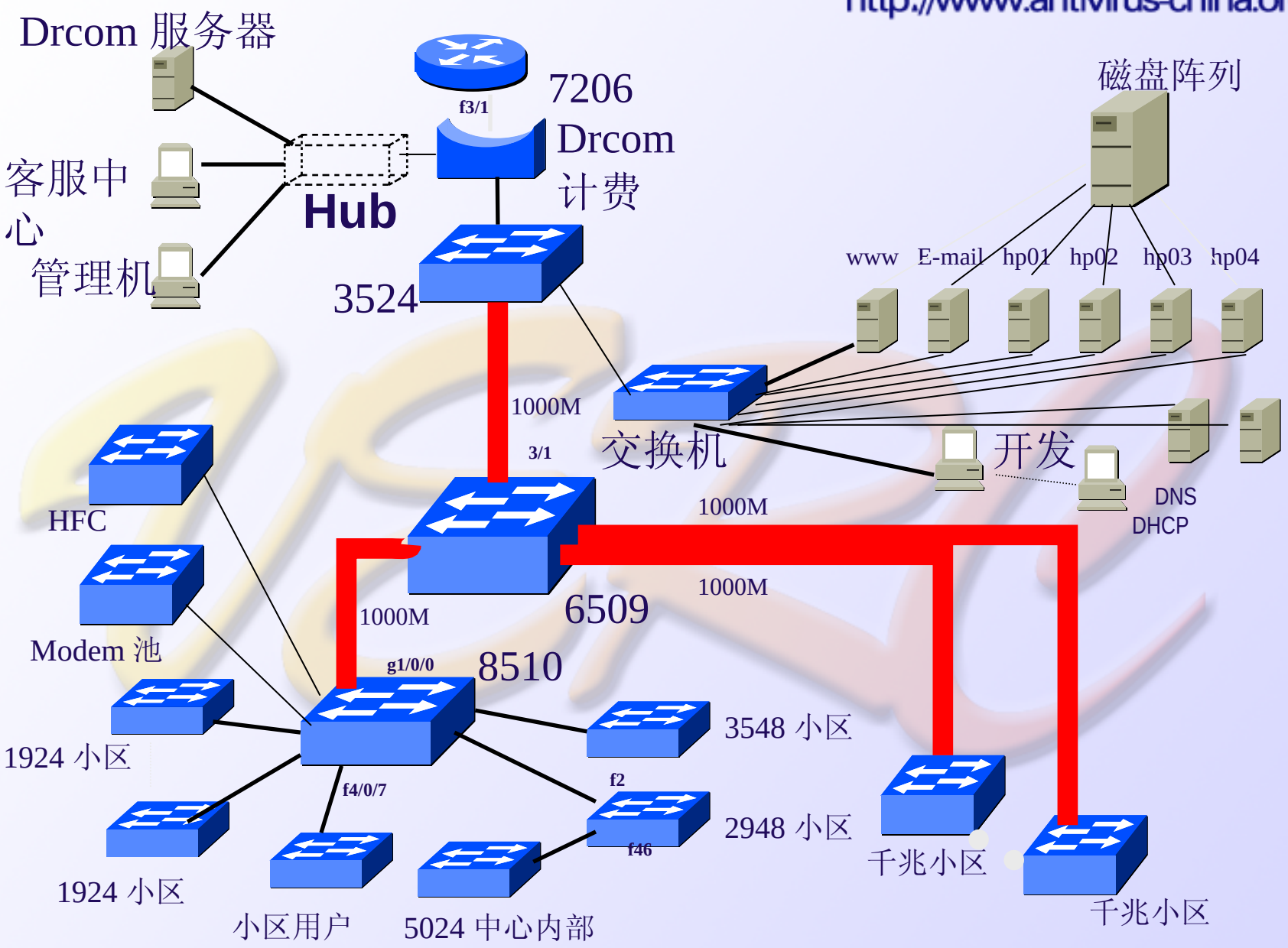
- 隐性的破坏方式
  - 感染、植入病毒程序，以便能够长期控制和滥用系统，成为犯罪分子进行网络攻击破坏的工具
  - 收集情报、敏感信息、窃取计算机资产
  - 沦为进行各种反动宣传的工具

两种破坏方式的特点和区别

- 显性破坏
  - 容易发现
  - 容易处置
  - 容易评估损失
  - 时间短
  - 破坏目标具有广泛性
- 隐性的破坏方式
  - 难于发现
  - 难于评估损失
  - 周期长
  - 攻击目标具有针对性

建立计算机病毒预警监测体系




Drcom 服务器
客服中心
管理机
Hub
f3/1
7206
Drcom
计费
3524
磁盘阵列
www
E-mail
hp01
hp02
hp03
hp04
1000M
3/1
交换机
开发
DNS
DHCP
HFC
1000M
1000M
1000M
6509
Modem 池
g1/0/0
8510
1924 小区
3548 小区
f4/0/7
f2
2948 小区
千兆小区
1924 小区
小区用户
f46
5024 中心内部
千兆小区

网络示意图

病毒监测结果（3月21日—24日）

提供计算机病毒预警服务

- 发布计算机病毒预警信息
  - 2004年共发布50期计算机病毒监测周报
  - 2004年共发布52期计算机病毒预报
- 建立病毒防治宣传阵地
  - 与中央电视台合作开辟计算机病毒播报节目
  - 与新华社合作发布病毒预告
  - 4月将开通手机短信预警服务
    - 中国移动用户
      - 病毒预报　　XFD到3721
      - 反病毒公告栏　XED到3721

加强国际交流

AVAR 2005国际反病毒大会2005年11月17-18日
将在天津开发区泰达万丽酒店召开

我国当前计算机病毒防治策略

- 依法加强对网络安全监督检查力度，遏制计算机病毒传播蔓延，净化网络空间
- 严厉打击制造、传播计算机病毒等有害程序的犯罪活动
- 加强管理措施，建立、健全严格的病毒防治规章制度和动态的技术防控策略，并坚决贯彻执行
- 加快我国计算机病毒预警监测体系建设
- 进一步规范我国计算机病毒信息发布工作
- 建立快速、有效的计算机病毒应急救援体系
- 加大对病毒防治新技术、新产品的研发力度
- 加强对计算机病毒防治产品的质量监督工作
- 加强对各类网上交易系统的安全保障措施
- 加强信息安全培训，普及提高安全防范意识和病毒防治技术
- 建立动态的计算机病毒危害性评估制度
- 建立专业化安全咨询和服务体系
- 加强国际间的交流合作

技术防范措施

- 及时从软件供应商下载、安装安全补丁程序和升级杀毒软件
- 新购置的计算机和新安装的系统，一定要进行系统升级，保证修补所有已知的安全漏洞
- 必须使用高强度的口令，并经常变更各种口令
- 关闭不必要的端口和服务
- 选择、安装经过认证的防病毒软件，定期对整个系统进行病毒检测、清除工作
- 加强对内网的整体安全防范措施，如使用防火墙、防病毒网关
- 加强对内网内部各系统的安全防护措施，如安装使用个人防火墙、防病毒软件
- 空闲的计算机不要接入互联网
- 注意保护各类敏感信息，防止发生失泄密
- 加强对各类帐号的管理，可采用键盘保护产品，防止通过截获键盘盗取敏感信息
- 下载软件时，要登陆大型的门户网站和专业网站，一些小的网站缺乏正规的管理和维护，成为病毒传播的温床

- 经常备份重要数据
- 去掉不必要的网络共享
- 设置显示所有文件和已知文件类型的扩展名
- 定期检查系统配置和关键文件是否正确
- 不要打开来历不明的电子邮件，尤其是含有诱人的标题或者可执行程序的附件
- 正确配置、使用计算机病毒防治产品
- 正确配置系统和各类应用程序，减少病毒侵害事件
- 重要的计算机系统和网络一定要严格与互联网物理隔离

谢谢！

国家计算机病毒应急处理中心
计算机病毒防治产品检验中心
Http://www.antivirus-China.org.cn
86-22-66211487
Zj@antivirus-China.org.cn