恶意代码发展与校园安全管理论坛

段海新

duanhx@tsinghua.edu.cn

2008年9月21，大连理工大学

提纲

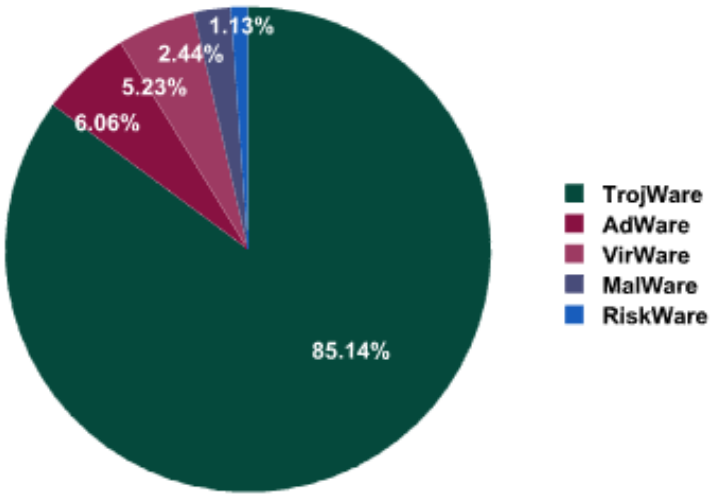
- 恶意代码发展现状
- 恶意代码对抗的思考
- 校园网安全管理论坛

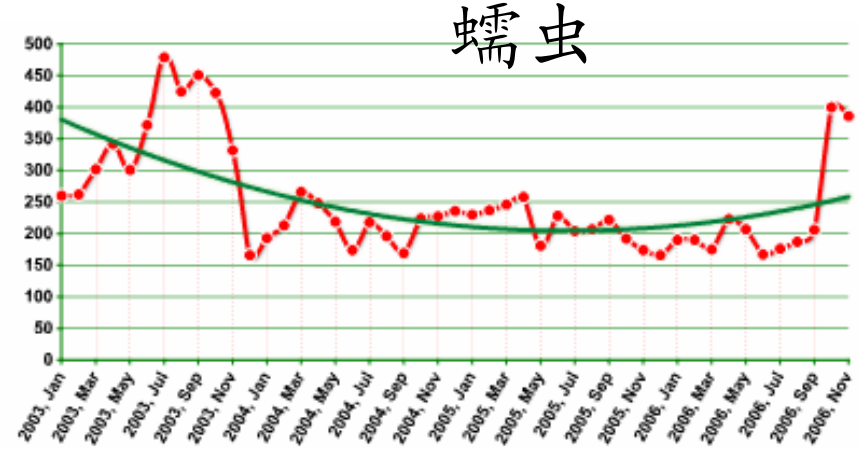
近年来网络攻击的趋势

- 影响主干网的大规模安全事件有所减少
  - 蠕虫攻击有所下降
  - 大规模DDoS攻击减少
- 安全技术发挥了很大作用
  - 补丁更新、防病毒软件及更新
  - 防火墙、入侵检测与防护？ 其他
- 网络管理者的努力
  - 常用端口、站点的封堵
- 用户安全意识和技能的提高

近年来恶意代码类型与趋势

- 大多数是木马
- 传统病毒大为减少
- 蠕虫影响下降





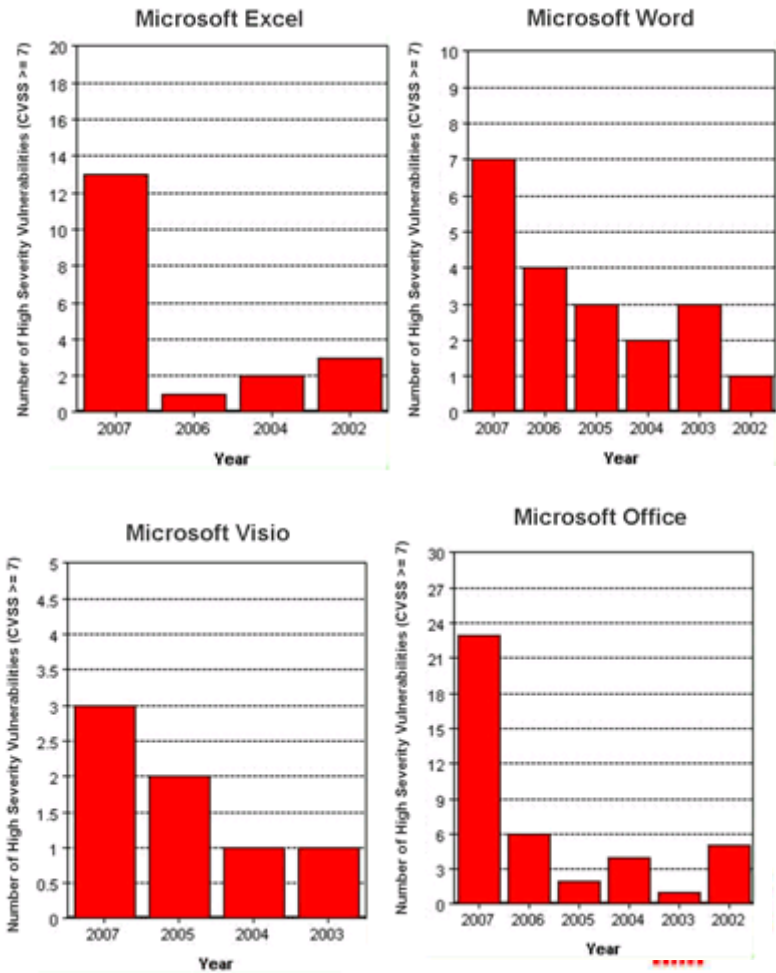
"Kaspersky Lab"

http://www.viruslist.com/en/analysis?pubid=204791924

http://www.viruslist.com/en/analysis?pubid=204791987

利用办公软件文件格式的攻击

Microsoft Excel Remote Code Execution (MS07-002)
Microsoft Outlook Remote Code Execution (MS07-003)
Microsoft Word Remote Code Execution (MS07-014)
Microsoft Office Remote Code Execution (MS07-015)
Microsoft Excel Remote Code Execution (MS07-023)
Microsoft Word Remote Code Execution (MS07-024)
Microsoft Office Remote Code Execution (MS07-025)
Microsoft Outlook Express and Windows Mail (MS07-03
Microsoft Excel Remote Code Execution (MS07-036)
Microsoft Excel Remote Code Execution (MS07-044)
Adobe Reader and Acrobat Remote Code Execution (APSB07-18)
Adobe Reader and Acrobat Cross Site Scripting (APSA0 01)



基于Web的攻击增多

- 利用Web浏览器的漏洞
  - ActiveX control，脚本
  - 第三方的Plugins，BHO（Browser Help Object）
- 基于Web服务器漏洞的攻击
  - SQL注入问题
  - 基于开源软件的内容管理软件，如
    - 网站管理软件、内容发布
    - 论坛（BBS）软件，Wiki软件，Blog软件…
- 应用层内容的检测：防火墙、入侵检测

利用媒体播放器的攻击

- **RealPlayer**
  CVE-2007-2497, CVE-2007-3410, CVE-2007-5601
- **Apple iTunes**
  CVE-2007-3752
- **Adobe Flash Player**
  CVE-2007-3457, CVE-2007-5476
- **Apple Quicktime**
  CVE-2007-0462, CVE-2007-0588, CVE-2007-0466, CVE-2007-0711, CVE-2007-0712, CVE-2007-0714, CVE-2007-2175, CVE-2007-2295, CVE-2007-2296, CVE-2007-0754, CVE-2007-2388, CVE-2007-2389, CVE-2007-2392,
- **Windows Media Player**
  CVE-2006-6134, CVE-2007-3035, CVE-2007-3037, CVE-2007-5095

第三方软件的更新问题值得关注

ARP欺骗攻击

- 几乎所有园区网管理者都会头痛的问题
  - 网络不稳定或彻底不通
  - 流量劫持，敏感信息泄漏
  - HTTP流量的劫持，注入恶意代码
- ARP协议, 1982年的RFC，没有补丁；
- 不是一种恶意代码，而是一种方法，防病毒软件没有统一的方法
- 影响局限于一个广播域，主干网看不到，入侵检测和防火墙不起作用

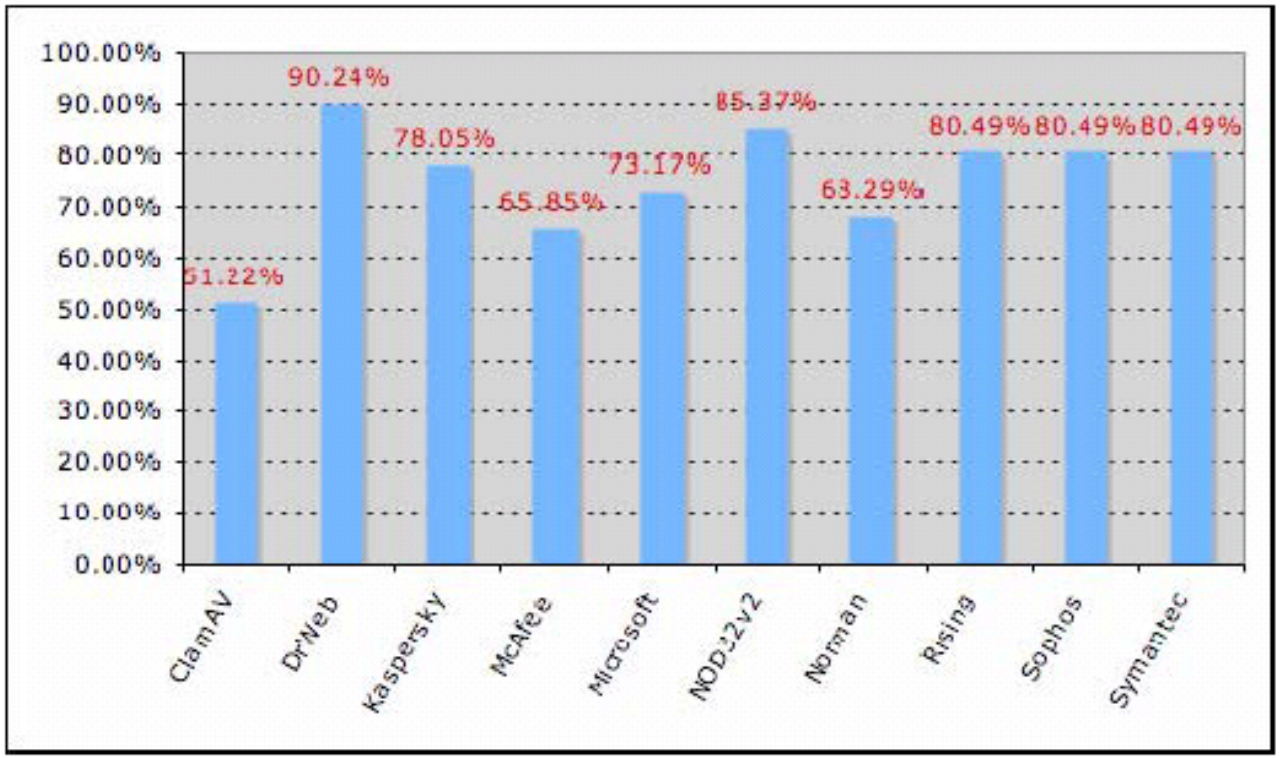
恶意代码的趋势

- 黑客以赢利为目的，黑色产业链
- 恶意代码的模块化，如DiskGen
- 一种病毒多种传播手段
- 传播的隐蔽性，长期隐藏
- 影响的本地化，主干网无法检测

恶意代码对抗技术及反思

- 针对防病毒技术
  - 变形与多态：加密、加壳
  - 虚拟机：更加复杂的壳
  - 主动防御：内核级的Rootkit
- 针对入侵检测
  - 变形与多态，动态端口
- 防火墙技术
  - 反向链接，动态端口，线程注入

07’9-10提交VirusTotal 41个样本首次提交检出率

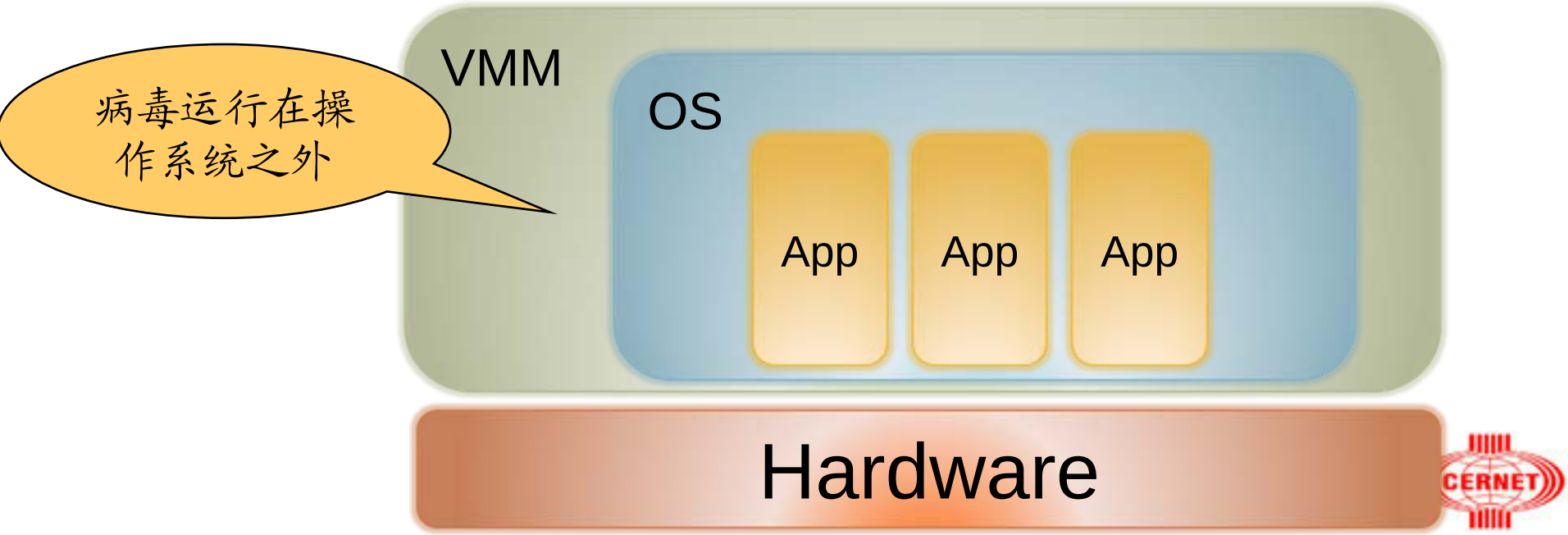


2007年9月-10月收集的41个病毒样本首次提交检出率统计

来源：商尔从 SYSU-CSIRT，中山大学信息与网络中心

针对虚拟计算的RootKit

- 硬件虚拟化的出现使得Rootkit可以
  - 在OS中运行的一切，包括安全软件，都在其控制之中
- 两个实例： BluePill， Vitriol



关于恶意代码对抗的思考

- **安全产品不作为吗？**
  - 不用防病毒、防火墙，你试试？
- **校园网安全，存在彻底的解决方案吗？**
  - 你的方案能解决所有问题吗？
  - 你能保证以后不发生安全问题吗？
- **我们应该信赖谁？**
  - 我们自己
  - 不断学习，不断提高
  - 集众人所长，形成自己的方案

校园网安全管理论坛的宗旨

- 运行CCERT的体会
  - 技术发展变化：如，攻击的局域化
  - 管理体制的变化：主干网转移到赛尔公司
  - 服务定位的变化：校园网
  - 自己认识的变化：知识分布在每个人的头脑中，不可能集中到一个人的脑子里
- 独立的校园网安全管理需要共享信息，不可能集中控制或者管理
- 需要平等、自由、开放的信息交流平台

论坛的组织和活动

- 对校园网运行管理人员完全开放、免费
- 由自愿者组织相关的技术交流活动
- 关注校园网关注的运行、安全问题
- 交流平台：
  - 网站：http://forum.ccert.edu.cn
  - 论坛（BBS）、邮件列表、Blog
  - 视频会议，QQ群

CERNET COMPUTER EMERGENCY RESPONSE TEAM

CCERT

校园网安全与管理论坛

近期病毒案例分析及清华校园网病毒防范_清华郑先伟

本文从近期病毒案例（磁碟机）分析切入，引出新形势下病毒对校园网运维带来的挑战，最后阐述了清华大学校园网病毒防范所采取的举措：
1、局域网部署监测设备
2、统一部署的防病毒软件
3、用户的安全培训

下载

最新活动信息 2008/04/8

1	技术沙龙第二期:校园网防病毒软件选型和近期病毒动态分析	2008-03-26 15:32:00	查看详情
2	技术沙龙第一期：校园网中802.1X准入控制的利与弊	2008-01-02 11:54:00	查看详情

近日更新文档 2008/04/8

1	近期病毒案例分析及清华校园网病毒防范_清华郑先伟	2008-04-02 15:55:00	查看详情
2	北大校园网安全服务与ARP病毒防治_北大钱杰	2008-04-02 15:52:00	查看详情

近日更新软件 2008/04/8

1	Windows清理助手	2008-02-01 08:10:00	查看详情

关于ARP的多次研讨会总结

- 使用交换机的功能
  - 检测IP与MAC对应表，自动报警（石油大学网管软件）
  - Anti ARP spoofing （集美大学，锐捷设备）
  - DAI和DHCP Snooping （cisco 设备，上海交大）
- 客户端ARP过滤软件
  - Anti-ARP
  - ARPFix (清华）
  - 360卫士, …
- 网关上IP-MAC的绑定
  - 北大：利用DHCP信息配置网关上的静态绑定
- 细粒度划分VLAN

校园网防病毒软件选型及ARP防范技术沙龙
4月1日，北京大学

安全意识的教育：中山大学

信息安全指南

个人计算机安全改善（1）

本指南适用于普通办公及住宅环境下的个人计算机

前 言

安全意识已公认为计算机信息安全的第一道防线。在有了良好的信息安全意识后，我们需要进行具体的信息安全改善工作。

本指南主要针对使用Windows XP和Vista操作系统的个人计算机使用者，就几个关键方面作出指引，指导使用者进行安全改善。

本小册子供本校教职工、学生免费索取

不要随便开启不明来历的邮件或即时信息

不明来历的邮件或即时信息可能含有恶意代码或含有病毒，一旦开启有可能受到病毒或木马的感染。因此，一般不要随便开启不明来历的邮件或即时信息。即使认识的人发过来的邮件中如果含有附件，在打开前也应该得到对方的确认。垃圾邮件还是"网络钓鱼(Phishing)"欺骗的重要手段。犯罪者主要利用垃圾邮件配合假冒站银行或电子商务站点进行欺诈，骗取您的银行帐号和密码。因此，随意点击垃圾邮件中的链接是非常危险的，这有可能遭至您直接的金钱损失。

遇到棘手的安全问题应及时向专业人士求助

当今的IT产品，复杂的技术被易用的"外衣"包裹，安全问题往往是非常复杂的问题，一旦您遇到怀疑病毒、入侵等棘手的安全问题时，应及时向专业人士求助与咨询。

实施了恰当的安全措施后，可以将风险降至最低，但就目前技术而言，并无100%可靠的安全措施。客观上，信息安全事故是难以完全避免的，因此我们需要在信息安全事故中学习如何改善信息安全。

信息与网络中心的IT服务帮助台也是各种安全事件的联系点。您可以通过电子邮件、电话语音呼叫和FAQ知识库来获取帮助。帮助台与计算机安全事件响应小组可以为您提供快捷、专业和有礼的服务支持。如果您的棘手问题我们无法解决，我们也会尝试将您的问题提交到更专业的合作伙伴解决。

INFOSECU-GUIDE-01-200711-A

中山大学信息与网络中心

紧急呼吁禁用自动播放功能和对U盘进行查毒

信息与网络中心在风险评估的基础上，基于以下的原因，紧急呼吁立即禁用Windows上的自动播放，并建议大家对自己所使用的U盘进行查毒：

1. 在目前，没有100%可靠的信息安全解决方案，各种信息系统不再追求设计成绝对安全，技术不是万能的，必须使用管理手段并增强人们的意识去保障信息的安全。
2. 开启Windows上的自动播放功能所产生的代价或成本非常的高。开启此功能很有可能在使用移动介质（例如U盘）的时候感染蠕虫病毒，并导致防（杀）毒软件等安全措施失效，从而使蠕虫、木马病毒的泛滥。后果会引致个人及学校的重要信息外泄，引致局部乃至全局网络的不稳定甚至不可用。而关闭Windows上的自动播放功所付出的代价，仅是在使用移动介质时，增加2至3次的鼠标点击操作。
3. 已经有十分充足的证据证明，目前流行的ARP欺骗木马的一个重要传染途径就是利用移动介质蠕虫，通过在使用U盘的过程中传染扩散，开启Windows上的自动播放功能感染及传播这种病毒的机会要远远大于关闭自动播放功能的计算机。

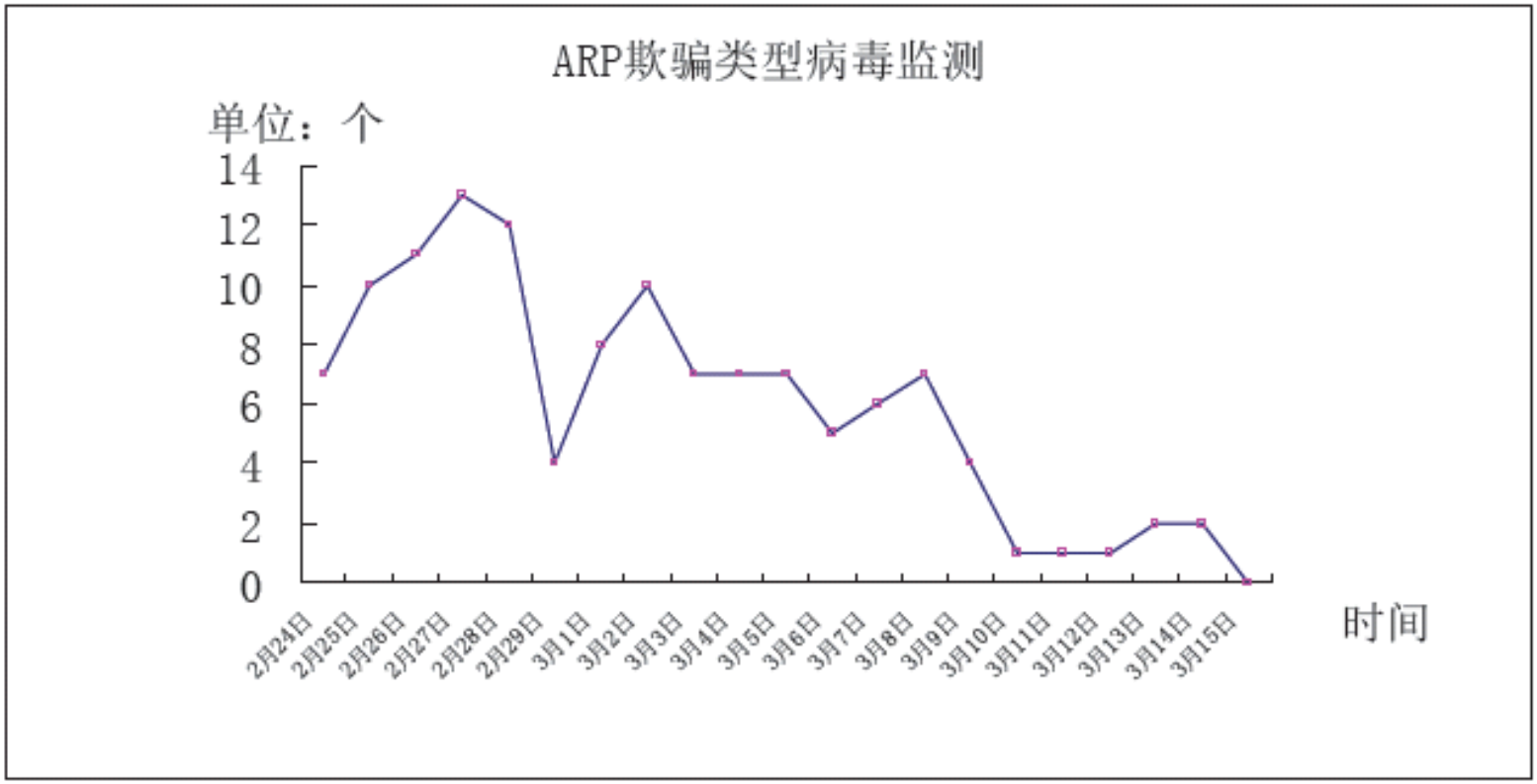
在各单位办公及实验室、多媒体教室、图书馆、公共计算机实验室、乃至个人所拥有的计算机都建议关闭自动播放功能。对于多媒体教室、图书馆、公共计算机实验室的公用的计算机在关闭了自动播放后，建议做好与使用者的沟通工作，提前张贴公告和使用指南。

如何关闭Windows自动播放功能请见《信息安全指南》小册子，更详细的方法也可以参看信息与网络中心帮助台的网站 http://helpdesk.sysu.edu.cn/ 中的 "IT服务FAQ" → "G.信息安全与防病毒" → "Q26. 如何关闭Windows自动播放功能?

另外大家应该对自己所使用的U盘进行一次全面的病毒查杀。在病毒查杀的时候应该使用正版的防（杀）毒软件，使用盗版的防（杀）毒软件与使用假冒伪劣安全产品（例如安全帽、灭火筒）没有区别，是无任何安全保障的。

各单位及个人在关闭自动播放功能及病毒查杀中遇到问题，可与信息与网络中心帮助台及CSIRT联系。

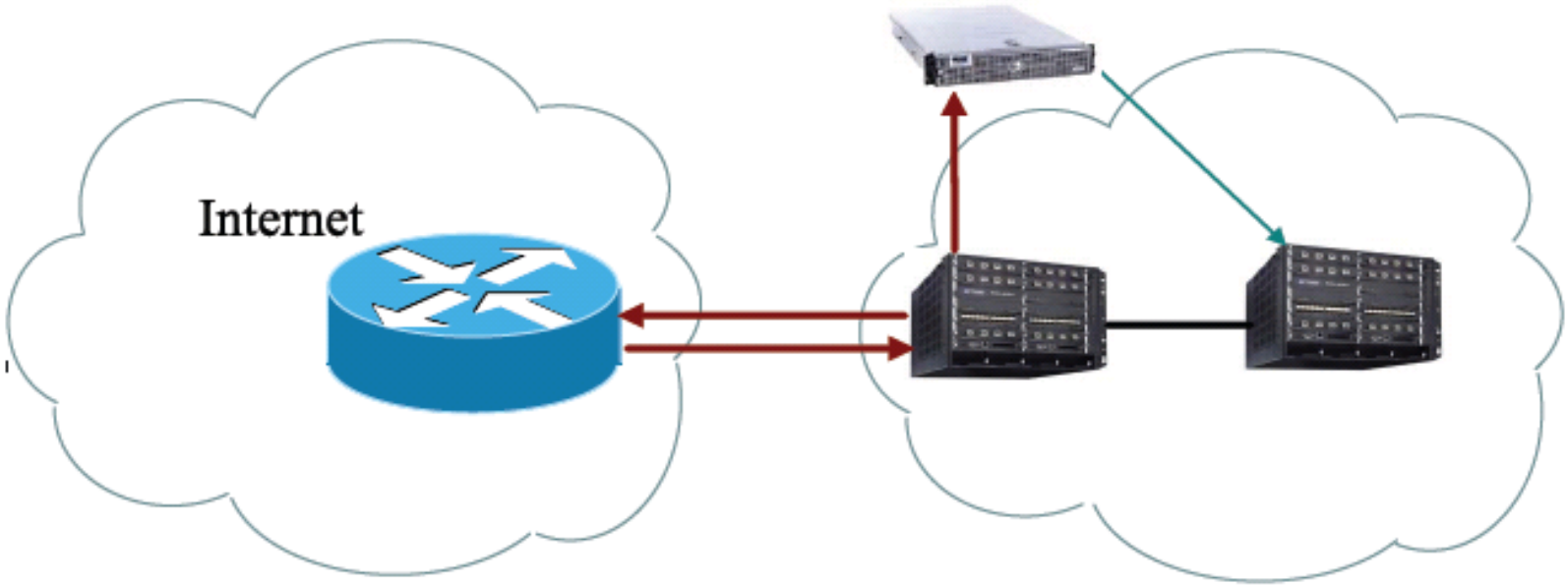
控制磁碟机病毒爆发思路



最近一周校内基本没有发现ARP欺骗现象

自动采取措施（1）

- 对用户在线告警
  - 利用TCP劫持来实现网页重定向
  - 用户端浏览器弹出告警网页



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

地址(D) http://cert.sjtu.edu.cn/black/

转到

SJTU CERT 上海交通大学 计算机紧急响应组

关于我们 | 安全公告 | 安全建议 | 杀毒中心 | 工具补丁 | 病毒库自动更新 | 校内WindowsUpdate自动更新

警告：

您的电脑已经被黑客远程控制

请按下文说明操作清除木马和后门。如果已清除，明天会再提醒一次，后天开始不再提醒。

关于近期清理校内感染木马用户的说明

您的IP地址是 202.120.2.231

校园网禁用/告警用户名单

如果您确认问题已解决并采取有效措施防止此类事件重演，请联系网络信息中心解封，联系方式如下：

电子邮件：cert@sjtu.edu.cn
徐汇校区：临然高科技大厦47网络信息中心 62932944-0
闵行校区：闵行计算中心2F网络信息中心 (地图) 54742547-0

如何参与校园网安全管理论坛？

- 在网站注册，全国各高校同行交流
- 关注、参加论坛的活动
- 在论坛网站上开博客，介绍技术和经验
- 组织交流活动或技术沙龙
- 在本地形成一个交流的圈子，CCERT和《中国教育教育网络》将鼎力协助

参考资料

- 姜开达，上海交通大学校园网近期ARP欺骗分析与控制，http://forum.ccert.edu.cn/upload/files/xxd_2008_042_1400.pdf
- 商尔从，防病毒软件还是防病毒服务？http://forum.ccert.edu.cn/upload/files/zhoud_2008_042_1548.pdf
- 中山大学校园网信息安全意识宣传，http://helpdesk.sysu.edu.cn/content/view/134/
- **校园网安全与管理论坛 http://forum.ccert.edu.cn**

- **Kaspersky Security Bulletin 2006: Malware Evolution，** http://www.viruslist.com/en/analysis?pubid=204791924
- **SANS Top-20 2007 Security Risks (2007 Annual Update)** http://www.sans.org/top20/

http://forum.ccert.edu.cn

duanhx@tsinghua.edu.cn