文章编号：1006-4354 (2004) 05-0029-02

浅谈计算机病毒的特征与防御

傅 献 华

(陕西省气象台，陕西西安 710014)

中图分类号：TP393 文献标识码：B

随着计算机在社会生活各个领域的广泛运用，计算机病毒攻击与防御技术也在不断拓展。据报道，世界各国遭受计算机病毒感染和攻击的事件数以亿计，严重地干扰了正常的人类社会生活，给计算机网络和系统带来了巨大的潜在威胁和破坏。如“SQL 蠕虫王”病毒，仅仅数小时就使全球主干网陷入瘫痪，在病毒发作的一周时间内就对全球造成了 12 亿美元的直接经济损失。“冲击波”病毒给整个互联网带来了几十亿美元的直接经济损失，感染计算机超过了 100 万台。可以预见，随着计算机、网络应用的不断普及和深入，防御计算机病毒也将越来越受到各个领域的高度重视。

1 计算机病毒的现象特征

计算机病毒是通过复制自身来感染其它软件的程序。具有：(1) 攻击隐蔽性强。病毒可以无声无息地感染计算机系统而不被察觉，待发现时，往往已造成严重后果。(2) 繁殖能力强。电脑一旦染毒，可以很快“发病”。目前的三维病毒还会产生很多变种。(3) 传染途径广。病毒可以通过软盘、光盘、网络和硬件设备等多渠道自动侵入计算机中，并不断蔓延。(4) 潜伏期长。病毒可以长期潜伏在计算机系统而不发作，待满足一定条件后，就激发破坏。(5) 破坏力大。计算机病毒一旦发作，轻则干扰系统的正常运行，重则破坏磁盘数据、删除文件，导致整个计算机系统的瘫痪。(6) 针对性强。计算机病毒的效能可以准确地加以设计，满足不同环境和时机的要求。

1.1 计算机病毒发作前常见的表现

运行正常的计算机经常无缘无故地死机；操作系统无法正常启动；运行速度明显变慢；正常运行的软件经常发生内存不足的错误；打印和通讯发生异常；要求对软盘进行写操作；以前能正常运行的应用程序经常发生死机或者非法错误；系统文件的时间、日期、大小发生变化；打开 Word 文档后，该文件另存时只能以模板方式保存；没有安装新的应用程序而磁盘空间迅速减少；网络驱动器卷或共享目录无法调用；基本内存明显减少；陌生人发来的标题具有诱惑力的电子函件；自动链接到陌生的网站等。

1.2 计算机病毒发作时常见的表现

提示一些不相干的话；发出一段音乐；产生特定的图像；硬盘灯不断闪烁；进行游戏算法；Windows 桌面图标发生变化；计算机突然死机或重启；自动发送电子函件；鼠标自己在动等。

1.3 计算机病毒发作后的表现

计算机病毒发作后都会给计算机系统带来破坏性的后果。“恶性”计算机病毒发作后会给用户造成的损失更大，其后果：硬盘无法启动，数据丢失；系统文件丢失或被破坏；文件目录发生混乱；部分文档丢失或被破坏；部分文档自动加密码；导致计算机重新启动时格式化硬盘；主板被破坏；网络瘫痪，无法提供正常的服务。

2 计算机病毒的防御措施

2.1 时刻保持警惕性

使用计算机时要提防病毒的侵入，不要随便打开来历不明的电子函件中夹带的附件文件；不要随意从不可靠的渠道下载软件；不要轻易将硬盘共享；往外传送的附件也要仔细检查，确定无

收稿日期：2004-06-01

作者简介：傅献华 (1952-)，女，山西阳泉人，高级工程师，从事气象信息网络系统管理与维护。

文章编号：1006-4354 (2004) 05-0030-02

小型局域网共享 ADSL 宽带上网的设置

王 鹏

(洋县气象局，陕西洋县 723300)

中图分类号：TP393 文献标识码：B

洋县气象局共有电脑 7 部，有 WIN98 和 WIN2000 操作系统。计算机都安装有 100 MB 网卡，网卡有 3COM (3C905B-TX) (原单收站微机所配) 和 TP-LINK 两种型号。交换机使用 TP-LINK16 口 10-100 MB 自适应交换机，选用其中一台配置较高的计算机做代理上网的服务器，操作系统为 WIN98，申请了中国电信的 ADSL 宽带上网服务，带宽为 2 MB，由电信商提供一块 PCI 接口的 ADSL MODEM 上网卡。

1 组建网络

1.1 ADSL MODEM 网卡的安装

打开计算机机箱，找到空闲的 PCI 插槽，将 ADSL MODEM 网卡插入，固定后盖上机箱，将电话线接入网卡的 LINE 接口(将电话线的进户线接入网卡，网卡上的 PHONE 口接入电话机)。启动计算机，用该网卡提供的光盘安装 ADSL MODEM 网卡的驱动程序，安装过程中按要求分别填入电信服务商所提供的 IP 地址、网关、子网掩码、DNS，安装完成后重新启动，任务栏右下角出现网络连通标志，点击“状态”，显示连接速度为：下行：2 048 KB，上行：640 KB，此时网卡安装完成，点击服务器 IE 浏览器，可以上网浏览网页。

1.2 客户机安装网卡，配置网络设置

对计算机用其网卡所带的驱动程序盘安装驱

收稿日期：2004-03-03

作者简介：王 鹏 (1965-)，男，陕西洋县人，助工，从事气象业务和服务工作。

计算机病毒后才能发送。只要防护得当，是可以避免感染上计算机病毒的。

2.2 建立有效的计算机病毒防护体系

首先要在计算机中建立病毒防护体系，安装最新版本的、有实时监控文件系统功能的防杀计算机病毒软件；其次坚持定期查、杀病毒。如开机时就启用计算机杀毒软件，对计算机进行扫描“体检”。第三要关注新版本杀毒软件报告，及时对杀毒软件升级更新，确保对新生病毒检测和杀毒的有效性。第四是使用别人的软件、软盘和光盘前先进行病毒检测，严把“入口”关。

防火墙能极大地提高内部网络的安全性，并通过过滤不安全的服务而降低风险，所以在局域网络中应安装防火墙。

2.3 有应急措施

计算机病毒是客观存在的，每台计算机都存在感染病毒危险。因此，必须有应急措施和思想准备。一旦出现计算机病毒，能正确应对，不要手忙脚乱，忙中出错容易使损失扩大。

2.4 重要数据文件定期进行备份

对系统文件、重要数据等要经常备份。不要等到计算机病毒破坏使计算机硬件或软件出现故障、使数据受到损坏时再去急救。平时要尽可能将数据和应用程序分别保存。

2.5 限制访问权限

在不影响系统正常工作的情况下对系统文件设置最低的访问权限，以防止计算机病毒的侵害。

2.6 通过给系统打补丁的方式防范病毒的侵害

有些病毒如“冲击波”、“震荡波”病毒攻击 WIN2000/2003/XP 等操作系统，使用这些操作系统的用户，要经常到专业网站下载补丁程序，通过给系统打补丁的方式防范病毒的侵害。