揭开计算机病毒的面纱

万先军

（重庆市奉节职业教育中心 重庆 奉节 404600）

[摘 要] 在计算机广泛使用的今天，相信都遇到过病毒给我来带来的困惑，那么计算机病毒就是一种程序，属于人为恶意编写的，是编制者在计算机程序中插入的破坏计算机功能或者数据代码，能影响计算机死机，能自我复制的一组指令或者程序代码。它会对计算机软硬件造成较大的危害。病毒的种类非常多，而不同类型的病毒其危害程度和感染方式也不尽相同。

[关键词] 计算机病毒；分类；表现与预防

一、计算机病毒的分类

按照病毒的存在媒体进行分类，一般可以分为引导型、文件型和混合型三种类型。引导型病毒一般来说主要藏匿于磁盘引导区，当电脑启动之后，隐藏在磁盘的病毒便会开始传播；文件型的病毒常常会对计算机中的可执行文件进行感染，例如com、exe、doc文件；而混合型病毒属于上述两种病毒的混合型，其算法复杂，传播的途径和危害更大，甚至导致瘫痪。

二、计算机病毒的危害和表现

1、对计算机数据进行破坏。病毒极有可能篡改计算机系统设置或者对计算机系统进行加密的方法，从而引起计算机系统的混乱，更严重的时候会破坏计算机的硬盘引导区，造成计算机无法正常启动等。

2、病毒会大量占用系统内存以及计算机磁盘空间。当计算机感染某些病毒之后，硬盘会自动开始持续性的读取，虽然用户并未执行操作，但是硬盘却处于高速运转状态，计算机内存也被大量的占用。

3、破坏用户的各种隐私。很多计算机用户对于木马病毒已经是深恶痛绝。有关调查显示，当前木马病毒占据了计算机病毒的60%左右，其中大部分木马病毒的传播目的都是为了破坏用户的个人信息，从而帮助病毒制造者获取非法利益。用户信息一旦泄露，将会给用户带来不可估量的损失。

4、导致计算机运行缓慢。计算机程序设计没有错误的情况下是可以正常打开运行的。但是如果是感染了病毒，很多程序需要使用的文件无法使用，甚至导致死机的现象。比如一些聊天软件和IE浏览器等均无法打开。很多程序在运行过程中突然死机，过会儿好像系统又在自行启动等等。

三、计算机病毒的防范措施

（一）切断病毒传播途径

在当今的网络时代，工作站是网络中的一个节点，大多数的病毒都是通过工作站传播到整个网络中去的。所以防范病毒必须从工作站入手。首先通过软件防范，这种防范方法相对简单，它通过在工作站上安装最新的杀毒软件就能够起到预防病毒入侵的目的。第二是在工作站上插入病毒卡，选择这种病毒防范措施的有点是可以实现对病毒入侵的实时监测，进一步的增强工作站病毒防范能力。第三是在网络接口上装病毒防御芯片，它可以把工作站与服务器的存储控制和病毒防御结合在一起，进一步增强计算机病毒的实时防御。因此当前选择最多的防范措施依旧是安装杀毒软件，方便快捷的起到防范作用。

（二）提升网络管理技术

对于计算机病毒的防范，单单依靠技术手段是不能彻底解决问题的，因此必须要把技术和管理结合在一起。因为计算机病毒的防范措施，从目前的实际情况来看依旧是非常被动的。而就网络管理来说，我们可以主动的出击，按照计算机病毒的感染机制，对计算机进行正确的操作和使用，制定完善的网络访问规范，对于服务器进行定期的杀毒和维护，最大限度的预防病毒的侵害。通过对计算机使用的规范化，可以在很大程度上避免用户对不良网站、信息的点击，可以有效的避免一些利用诱惑性图片来吸引用户点击的非法网站，从而预防病毒对计算机的入侵。

综上所述，计算机用户必须要树立正确的病毒防范观念，应该对目前互联网上的病毒传播手段有一定的了解，对病毒防范知识要有一定的掌握。比如在网上下载的各种资料数据，在打开和使用之前应该用杀毒软件进行扫描，不去访问来历不明的链接与网站；养成良好的计算机操作习惯，不把自己的电脑当作公用产品，定期扫描查杀U盘，移动硬盘等，这样一来病毒会被我们拒之千里，省去很多麻烦。虽然计算机病毒危害大，传播快，但是只要我们能够树立正确的防范意识，积极做好各种计算机病毒防范措施，还是可以在很大程度上避免病毒对计算机造成的危害。虽然说新病毒层出不穷，病毒也越来越隐蔽，现有的计算机操作系统本身也还存在着一定的缺陷和漏洞，很多新型的病毒能够利用这些漏洞在互联网中传播。但是只要每一个用户都能够提高反病毒的警惕性，通过科学有效的病毒防御方法，新出现的各种病毒就不会对用户造成大的威胁。当我们的计算机发现病毒之后，我们所安装的反病毒防御系统能够第一时间展开防御。我们有理由相信，随着病毒防御技术的不断提升以及用户病毒防范意识的提升，计算机病毒的生存空间必然会越来越小。

参考文献

[1]计算机基础（第二版），重庆大学出版社，主编：张小毅