计算机病毒不容忽视

杜卫平　（测绘学院）

摘　要：本文介绍了计算机病毒的感染机制、测试和防护方法。

一、引　言

1988年11月初，计算机病毒程序使美国Internet网络上的2500多台各种计算机陷于瘫痪，美国政府、科研机构、大学等许多单位的科学研究工作蒙受了巨大损害。虽然在此之前美国已经成立"计算机病毒工业协会(CVIA)"，并开始为销售抗病毒工具提供指导，但仍未避免这次事件的发生。这既说明计算机病毒的危害性还没有受到人们足够的重视，也说明抗计算机病毒的方法和工具还不完善。

网络上计算机病毒的危害是巨大的，而单个PC机受到病毒攻击同样不可忽视。由于现在国内微机的使用已有一定普遍性，所以系统软件、应用软件的相互复制，使病毒程序也有可乘之机，能在很大范围内扩散。目前国内对计算机病毒的研究工作势在必行，刻不容缓。

二、病毒传染机制

计算机感染病毒会使计算机显示无用或杂乱无章的信息或图像，计算机内的文件和硬盘将遭到破坏，从而使计算机本身或网络系统陷于瘫痪。这种病毒的自身作用是破坏以下计算机资源：(1) 文件和数据 (2)占用CPU资源。

计算机病毒的基本特性是感染别的程序。磁盘文件和内存中运行的程序都可能受病毒感染。这有两个含义：一是指对别的程序进行感染，其过程是复制后的病毒代码加在被感染程序的前部或尾部。二是指在内存中病毒程序的繁殖。计算机病毒通过它在运行过程中的自我复制占据内存空间，使CPU速度减慢下来。

下面说明计算机病毒感染的几种机制：

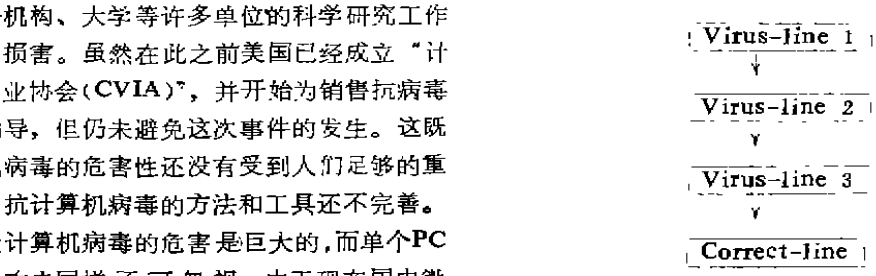
1、运行带病毒的程序时，病毒程序自我复制后加在用户文件（系统文件）之前。

一旦执行带病毒程序，首先病毒被复制在寻找到的可执行文件的前部，然后执行正常程序部分。如果受病毒程序多次感染的文件（程序）运行，则它将多次感染别的可执行文件（程序）。

举例：如果病毒程序部分用Uirut-line n表示，正常程序部分用Correct-line表示。一个受病毒程序三次感染的程序可表示如下：

```
Virus-line 1;
Virus-line 2;
Virus-line 3;
Correct-line;
```

这个带病毒程序运行过程为：



2、病毒程序加在正常程序之后，那么病毒程序的执行是在正常程序执行以后。第一和第二种情况的不同之处是：如果病毒程序加在正常程序之前，那么执行一个多次受病毒感染的程序，它占用较长的CPU时间而无正常结果。病毒程序加在正常程序之后时，执行一个多次受感染的带病毒程序，总能执行正常程序部分，但用户较前者更不易发现病毒的存在。

3、病毒程序除对别的可执行文件进行感染外，运行时还自我复制，彻底扰乱正常程序的执行。这种情况下，如果病毒程序突破操作系统对其运行时所需内存的限制（即破坏了操作系统的内存限制机制），那么它将大量占用内、外存存储空间，并侵占CPU资源，使CPU运行速度大大减慢，最后使系统瘫痪。

对于没有ID识别和口令存取控制等存取机制的操作系统来说，它所管理的文件和数据很容易受病毒感染。对于象UNIX这样的操作系统，病毒要进行感染，就要猜出口令，或者破坏存取机制。

上述几种计算机病毒的传染机制已经得到实验证明。

三、局域网内病毒的感染

在局域网内用户能够共享硬盘等资源，病毒程序对共享硬盘软件包的感染结果也许是致命的。

病毒程序通过对硬盘管理程序发起攻击，使得病毒能对专用体内的文件进行感染。虽然对专用体的使用规定有口令，猜出口令的可能性也是存在