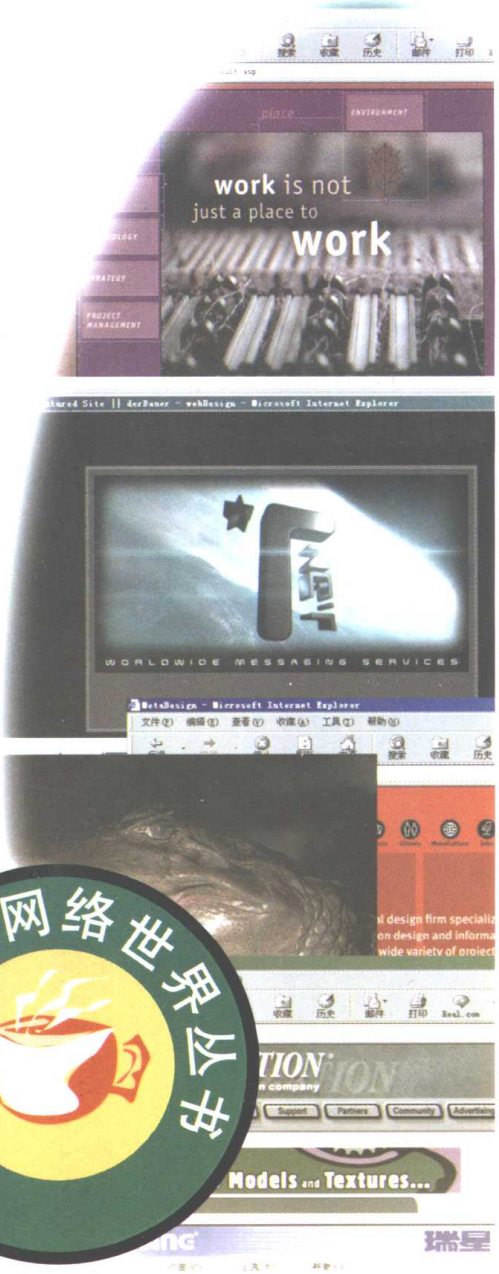
跟我学

网络病毒防治



轻松走遍网络世界丛书

左志刚　程勇刚　编著

机械工业出版社
China Machine Press

轻松走遍网络世界丛书

跟我学网络病毒防治

左志刚　程勇刚　编著

机 械 工 业 出 版 社

本书介绍了计算机网络病毒的相关知识、防治计算机病毒常用软件的特点及其使用方法，并对流行的计算机病毒进行了详细的分析。全书由浅入深地讲述了网络病毒的有关知识，详细介绍了多种防范病毒的软件，如Norton、瑞星和McAfee等，不仅可以作为一本计算机病毒知识的基础教程，使读者循序渐进地了解计算机病毒，而且也可以作为一本计算机病毒的手册使用。

本书主要是针对想了解计算机网络病毒的相关知识及防治计算机病毒的网络用户而编写，对广大网络爱好者和使用者亦均有很好的参考价值。

图书在版编目（CIP）数据

跟我学网络病毒防治/左志刚，程勇刚编著.—北京：机械工业出版社，2002.1
（轻松走遍网络世界丛书）
ISBN 7-111-09823-4

Ⅰ.跟… Ⅱ.①左…②程… Ⅲ.①计算机网络—安全技术②计算机病毒—基本知识 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2002）第001571号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）
责任编辑：边 萌
责任印制：付方敏
北京铭成印刷有限公司印刷·新华书店北京发行所发行
2002年2月第1版第1次印刷
1000mm×1400mm B5·5.625印张·218千字
0001—5000册
定价：20.00元 (含1CD)

前　言

互联网正在渗透到各行各业并逐渐走入普通人的日常生活中。在未来的几年内，互联网将极大地改变人们的生活方式。网上邮箱、网上购物、网上旅游、网上受教育、网上娱乐、网上交易、网上拍卖等。都会改变人们传统的工作方法和生活方式。因此，尽快地掌握网络工具，从而利用网络寻找自己所需要的资源就成为人们迫切的愿望。由于计算机技术的飞速发展，计算机硬件产品不断更新换代，计算机软件及其功能也不断升级和增强，特别是网络的应用将无处不在。为了满足读者的需求，我们重新组织了《轻松走遍网络世界丛书》，在原有基础上，更新并扩展了内容。这套丛书包括：《跟我学网络基础知识》、《跟我学使用网络工具》、《跟我学制作个人主页》、《跟我学网页动画制作》、《跟我学网络编程技术》、《跟我学网络病毒防治》、《跟我学网络黑客防范》和《跟我学网络布线与组网》共八本。该套丛书主要面向广大普通家庭用户，以及想进入互联网而又不知如何操作的网络爱好者。丛书所介绍的有关互联网的内容为：（1）计算机网络基础知识及Novell局域网、Internet和拨号上网的过程。（2）当前网络应用中流行的WWW浏览器、离线浏览器、下载工具、各种聊天软件(OICQ)、Telnet软件、E-mail软件和网络娱乐软件。（3）使用超文本标识语言HTML，JavaScript与VBScript、CGI语言，ASP、Perl、PHP等服务器端脚本语言来制作个人主页的相关知识。（4）动态网页设计软件Flash 5.0、Fireworks 4.0和专门用于制作网页动画的COOL 3D 3.0，比较系统地讲述了网页动画的制作方法。（5）网络编程的基本方法，包括HTML、Perl等语言，以及CGI编程、VBScript编程、JavaScript编程、Active Server Pages（ASP）编程、JavaServer Pages（JSP）编程等基本知识。（6）计算机网络病毒的相关知识、计算机病毒防治常用软件的特点及其使用方法，计算机流行病毒的分析。（7）黑客的内幕，向读者讲述网络自我防护方面的知识，以对用户的网络和计算机实现安全保护。（8）组建局域网及其布线。阅读本书后，读者可以独自完成网络的布线和组网工作。

通过这套丛书的学习，网络初学者将敲开网络的大门；已掌握一定知识的网络爱好者，将会获取更多、更新的内容，并学会如何创建自己的动态网页。

清源科技

编 者 的 话

自从第一例计算机病毒出现以来，随着计算机以及网络技术的迅猛发展，计算机病毒也日益猖狂，成为危害计算机和网络安全的幽灵。目前全世界流行的病毒共有 20 000 余种，这个数量正在以每月 300～500 种的速度攀升。

据 ICSA（International Computer Security Association，国际计算机安全协会）1998 年对 581 458 台桌面机和 12 122 台应用/文件服务器进行抽样调查的结果显示，几乎所有计算机(>99%)都有过被计算机病毒感染的经历。

而网络的发展又使计算机病毒找到了新的更为有效的传播方式。以前通过磁盘等有形媒介传播的病毒，从国外发现到国内流行，据统计，一个病毒的传播周期平均需要 6～12 个月；而网络的普及，使得病毒的传播已经没有国界，计算机病毒通过网络，在短短几天就传遍整个世界。网络和电子邮件使计算机病毒的传播已经没有了时间和空间的限制。

而且，由于网络资源的共享以及人们对计算机和网络的日益依赖，计算机病毒所造成的危害就越来越惊人。像 CIH 一类破坏主板 BIOS 和硬盘数据的恶性病毒，使得用户不得不更换主板以及造成硬盘数据的不可恢复性丢失，曾给中国用户带来巨大损失；COMPAT、DELTREE 等宏病毒随机修改数据文件的数据和删除文件；探索蠕虫、美丽杀手等特洛伊木马型病毒，在短时间内造成世界范围内的网络瘫痪和数据丢失。所有这些病毒给我们的生产和生活带来了极大的麻烦，而且进入网络时代，计算机病毒仍然猖獗、肆虐。

因此，了解一些计算机病毒的相关知识，懂得如何选择和使用防治计算机病毒的软件，注意流行的计算机病毒，对于我们安全地在网上冲浪，安全地使用计算机处理日常事务，是十分有必要的。

本书前 4 章介绍了有关计算机病毒的知识，包括计算机病毒的起源、种类、特点，计算机病毒发作的表象，以及网络病毒的诊断。第 5～6 章着重介绍常用的防治病毒软件以及防治网络病毒的相关知识。第 7 章则对典型的网络病毒进行了比较详细的分析。相信通过阅读本书，您一定能够了解现在计算机病毒与反病毒的发展现状，使您能够远离计算机病毒的困扰。

本书由左志刚、程勇刚负责编写，张涛、阴向阳、胡毅、李晓城等也参与了本书的部分章节的编写或资料的准备和收集工作。由于水平有限，时间仓促，书中缺点和不足在所难免，敬请广大读者批评指正。

目　录

第 1 章　认识计算机病毒

1.1　计算机病毒

什么是计算机病毒？一般来说，凡是能够引起计算机故障、破坏计算机数据的程序统称为计算机病毒。依据此定义，诸如逻辑炸弹、蠕虫等均可称为计算机病毒。

一种较为广泛的定义是：计算机病毒就是能够通过某种途径潜伏在计算机存储介质（或程序）里，当达到某种条件时即被激活的，具有对计算机资源进行破坏作用的一组程序或指令集合。

1994 年 2 月 18 日，我国正式颁布实施《中华人民共和国计算机信息系统安全保护条例》（以下简称《条例》），在《条例》第二十八条中明确指出："计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。"

这个定义具有法律性、权威性。

1.2　计算机病毒的起源

计算机病毒并非是最近才出现的新产物，事实上，早在 1949 年，距离第一部商用计算机的出现还有好几年时，计算机的先驱者冯·诺依曼（John Von Neumann）在他的一篇论文《复杂自动机组织论》中，提出了计算机程序能够在内存中自我复制，即已把病毒程序的蓝图勾勒出来。

但当时绝大部分计算机专家都无法想象这种会自我繁殖的程序是可能的，只有少数几个科学家默默地研究冯·诺依曼所提出的概念。

1975 年，美国科普作家约翰·布鲁勒尔(John Brunner)写了名为《震荡波骑士》(《Shock Wave Rider》)一书，该书第一次描写了在信息社会中，计算机作为正义和邪恶双方斗争的工具的故事，成为当年最佳畅销书之一。

1983 年 11 月 3 日，弗雷德·科恩(Fred Cohen)博士研制出一种在运行过程中可以复制自身的破坏性程序，伦·艾德勒曼(Len Adleman)将它命名为计算机病毒(Computer Viruses)，并在每周一次的计算机安全讨论会上正式提出，8 小时后专家们在 VAX11/750 计算机系统上运行，第一个病毒实验成功，一周后又获准进行 5 个实验的演示，从而在实验上验证了计算机病毒的存在。

1986 年初，在巴基斯坦的拉合尔(Lahore)，巴锡特(Basit)和阿姆杰德(Amjad)

两兄弟经营着一家 IBM-PC 机及其兼容机的小商店，他们编写了 Pakistan 病毒，即 Brain，在一年内流传到了世界各地。

1988 年底，在我国的国家统计部门发现小球病毒。

1.3 计算机病毒的传播途径

计算机病毒具有自我复制和传播的特点，因此，研究计算机病毒的传播途径是极为重要的。

根据美国国际计算机安全协会（ICSA）1999 年计算机病毒传播媒介的统计报告显示，电子邮件已经成为最重要的计算机病毒传播途径。此外，传统的软盘、光盘等传播方式也占据了相当的比例，而其他通过互联网的计算机病毒传播途径近年来也呈快速上升趋势。传播途径的比例大致如图 1-1 所示。

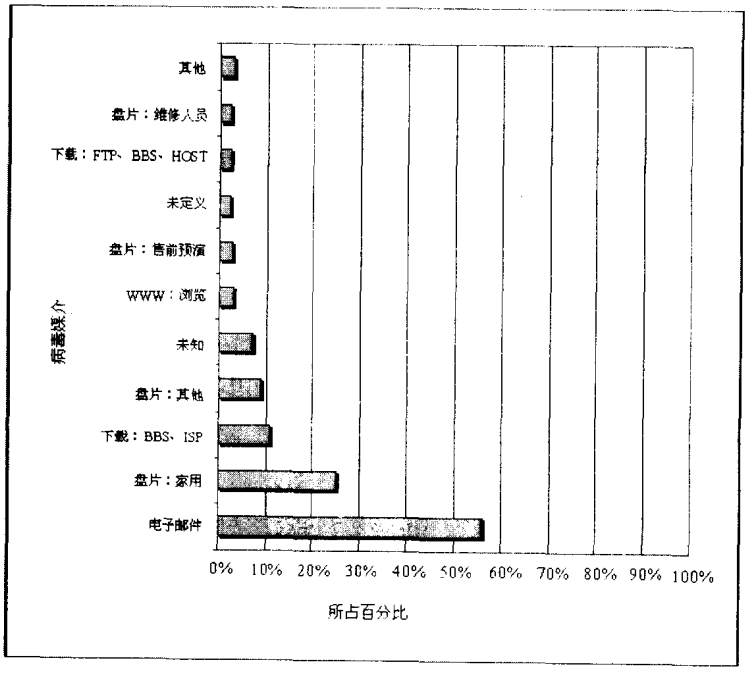


图 1-1 计算机病毒的传播途径

下面就来分析这些传播途径。

1.3.1 不可移动的计算机硬件设备

计算机病毒可以通过不可移动的计算机硬件设备，即利用专用集成电路芯片（ASIC）进行传播。这种计算机病毒虽然极少，但破坏力却极强，目前尚没有较好的检测手段。

1.3.2 可移动的存储设备

计算机病毒可以通过移动存储设备进行传播，包括软盘、光盘、ZIP 和 JAZ 磁盘，后两者仅仅是存储容量比较大的特殊磁盘。

软盘是使用广泛、移动频繁的存储介质，因此也成了计算机病毒寄生的“温床”。

光盘因为容量大，存储了大量的可执行文件，大量的病毒就有可能藏身于光盘中。对只读式光盘，不能进行写操作，因此光盘上的病毒不能清除。在以谋利为目的非法盗版软件的制作过程中，不可能为病毒防护担负专门责任，也决不会有真正可靠、可行的技术保障避免病毒的传入、传染、流行和扩散。

随着大容量可移动存储设备如 ZIP 盘、可擦写光盘、磁光盘（MO）等的普遍使用，这些存储介质也将成为计算机病毒寄生的场所。

1.3.3 网络

计算机病毒可以通过网络进行传播。随着因特网的高速发展，计算机病毒也走上了高速传播之路，网络已经成为计算机病毒的第一传播途径，其感染计算机病毒的方式有以下几种。

1. 电子邮件

计算机病毒主要是以附件的形式进行传播的。

由于人们可以将任何类型的文件作为附件发送，而大部分计算机病毒防护软件在这方面的功能也不是十分完善，因此使得电子邮件成为当今世界上传播计算机病毒最主要的媒介。

2. BBS（电子布告栏系统）

BBS 作为深受大众欢迎的栏目存在于网络中已经有相当长的时间。在 BBS 上，用户除了可以讨论问题，还能够进行各种文件的交换；加之 BBS 一般没有严格的安全管理，甚至有专门讨论和传播计算机病毒技术的 BBS 站点，使之成为计算机病毒传播的场所。

3. WWW 浏览

您可能已经发现，现在的网页比起过去要漂亮得多，这全要感谢 Java Applets 和 ActiveX Control 所赐，Java 或 ActiveX 可以让我们欣赏动感十足的网页。

但是，只要是任何可执行的程序，都可能被计算机病毒编制者利用，上述二者也没有能逃脱，目前互联网上已经有一些利用 Java Applets 和 ActiveX Control 编写的计算机病毒，因此，通过 WWW 浏览感染计算机病毒的可能性也在不断地增加。

4. FTP 文件下载

FTP 的含义是文件传输协议（File Transfer Protocol）。通过这一协议，您可以将文件放置到世界上的任何一台计算机上，或者从这些计算机中将文件复制到您本地的计算机中，这一过程就称为下载。当然，这些下载文件可能会被恶意的计算机病毒代码所感染。

1.3.4 点对点通信系统和无线通信系统

计算机病毒也可以通过点对点通信系统和无线通信系统进行传播。

目前已出现通过发布短信息来传播病毒的手机概念病毒（所谓概念病毒是指已经实现潜伏、传播、感染和破坏等病毒特性的病毒雏形）。一旦用户接收到带有病毒的短信息，阅读后便会出现手机键盘被锁死的现象，随后可能出现手机内存储的信息被破坏，直至手机 IC 卡被彻底破坏等恶性手机病毒。

随着 WAP 等技术的发展和无线上网的普及，通过这种途径传播的计算机病毒也将占有一定的比例。

1.4 计算机病毒的危害和特点

1.4.1 计算机病毒的危害

计算机病毒的程序代码包含一套特殊的指令，与其他的威胁不同，它可以不需要人们的介入就能由程序或系统传播出去。

计算机病毒也是程序，对于计算机的危害取决于计算机病毒编制者的意图，它们能够做任何程序作用于计算机的操作。任何计算机病毒只要侵入系统，都会对系统及应用程序产生程度不同的影响。轻者会降低计算机工作效率，占用系统资源，重者可导致系统崩溃，这些都取决于计算机病毒编制者的意愿。

下面分析一下计算机病毒的危害。

1. 计算机病毒激发对计算机数据信息的直接破坏作用

大部分病毒在激发的时候直接破坏计算机的重要数据信息，所利用的手段有格式化磁盘、改写文件分配表和目录区、删除重要文件或者用无意义的“垃圾”数据改写文件、破坏 CMOS 设置等。

2. 计算机病毒占用磁盘空间和对信息的破坏

寄生在磁盘上的病毒总要非法占用一部分磁盘空间。

引导型病毒的一般侵占方式是由病毒本身占据磁盘引导扇区，而把原来的引导区转移到其他扇区，也就是引导型病毒要覆盖一个磁盘扇区。

文件型病毒利用一些DOS功能进行传染，这些DOS功能能够检测出磁盘的未用空间，把病毒的传染部分写到磁盘的未用部位去。所以在传染过程中一般不破坏磁盘上的原有数据，但非法侵占了磁盘空间。

3. 计算机病毒抢占系统资源

大多数病毒在动态下都是常驻内存的，这就必然抢占一部分系统资源。病毒所占用的基本内存长度大致与病毒本身长度相当。病毒抢占内存，导致内存减少，一部分软件不能运行。

除占用内存外，病毒还抢占中断，干扰系统运行。计算机操作系统的很多功能是通过中断调用技术来实现的。病毒为了传染激发，总是修改一些有关的中断地址，在正常中断过程中加入病毒的“私货”，从而干扰子系统的正常运行。

4. 计算机病毒影响计算机运行速度

病毒进驻内存后不但干扰系统运行，还影响计算机速度，主要表现在：

（1）病毒为判断传染激发条件，总要对计算机的工作状态进行监视，这相对于计算机的正常运行状态既多余又有害。

（2）有些病毒为了保护自己，不但对磁盘上的静态病毒加密，而且进驻内存后的动态病毒也处在加密状态，CPU每次寻址到病毒处时都要运行一段解密程序，把加密的病毒解密成合法的CPU指令再执行；而病毒运行结束时再用一段程序对病毒重新加密，这样，CPU就要额外执行数千条以至上万条指令。

（3）病毒在进行传染时同样要插入非法的额外操作。

5. 计算机病毒的兼容性对系统运行的影响

兼容性是计算机软件的一项重要指标。兼容性好的软件可以在各种计算机环境下运行；反之兼容性差的软件则对运行条件“挑肥捡瘦”，对机型和操作系统版本等有要求。病毒的编制者一般不会在各种计算机环境下对病毒进行测试，因此病毒的兼容性较差，常常导致死机。

1.4.2 计算机病毒的特点

计算机病毒与生物病毒有许多相似之处，同样有以下一些特点。

1. 计算机病毒的传染性

传染性是计算机病毒最重要的特性，计算机病毒在这一点上与生物病毒是一致的。

传染性是生物病毒的一个重要特征。通过传染，生物病毒从一个生物体扩散到另一个生物体。在适宜的条件下，它得到大量繁殖，进而使被感染的生物体表现出病症甚至死亡。同样，计算机病毒也会通过各种渠道从已被感染的计算机扩

散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。

是否具有传染性被作为判别一个程序是否为计算机病毒的最重要的条件。

2. 计算机病毒的隐蔽性

计算机病毒通常附在正常程序中或磁盘较隐蔽的地方，目的是不让用户发现它的存在。

正是由于这种隐蔽性，计算机病毒得以在用户没有察觉的情况下游荡于世界上百万台计算机中。

计算机病毒的隐蔽性表现在两个方面：

（1）计算机病毒程序传染的隐蔽性　大多数计算机病毒在进行传染时速度是极快的，一般不具有外部表现，不易被人发现。

（2）计算机病毒程序存在的隐蔽性　被计算机病毒感染的计算机在多数情况下仍能维持其部分功能，不会由于一感染上计算机病毒，整台计算机就不能启动了，或者某个程序一旦被计算机病毒所感染，就被损坏得不能运行了。如果出现这种情况，计算机病毒也就不能流传于世了。正常程序被计算机病毒感染后，其原有功能基本上不受影响，计算机病毒代码附于其上而得以存活，不断地得到运行的机会，去传染出更多的复制体，与正常程序争夺系统的控制权和磁盘空间，不断地破坏系统，直至使整个系统瘫痪。

3. 计算机病毒的潜伏性

大部分的计算机病毒感染系统之后一般不会马上发作，它可长期隐藏在系统中，只有在满足其特定条件时才启动其表现（破坏）模块，在此期间，它就可以对系统和文件进行大肆传染。潜伏性愈好，其在系统中的存在时间就愈久，计算机病毒的传染范围就愈大。

4. 计算机病毒的破坏性

所有的计算机病毒都是一种可执行程序，而这一可执行程序又必然要运行，所以对系统来讲，所有的计算机病毒都存在一个共同的危害，即降低计算机系统的工作效率，占用系统资源。其具体情况取决于入侵系统的病毒程序。

同时，计算机病毒的破坏性主要取决于计算机病毒设计者的目的。如果病毒设计者的目的在于彻底破坏系统的正常运行的话，那么这种病毒对于计算机系统进行攻击造成的后果是难以设想的，它可以毁掉系统的部分数据，也可以破坏全部数据并使之无法恢复。但并非所有的病毒都对系统产生极其恶劣的破坏作用。有时几种本没有多大破坏作用的病毒交叉感染，也会导致系统崩溃等重大恶果。

5. 计算机病毒的针对性

计算机病毒一般都是针对某一种或几种计算机和特定的操作系统进行攻击

的。例如，有针对 PC 及其兼容机的，有针对 Macintosh 的，还有针对 UNIX 和 Linux 操作系统的。

只有一种计算机病毒几乎是与操作系统无关的，那就是宏病毒，所有能够运行 Office 文档的地方都有宏病毒的存在。

6. 计算机病毒的衍生性

计算机病毒的衍生性是指，计算机病毒编制者或者其他人将某个计算机病毒进行一定的修改后，使其衍生为一种与原先版本不同的计算机病毒。后者可能与原先的计算机病毒有很相似的特征，这时称其为原先计算机病毒的一个变种；如果衍生的计算机病毒已经与以前的计算机病毒有了很大甚至根本性的差别，则此时就会将其认为是一种新的计算机病毒。新的计算机病毒可能比以前的计算机病毒有更大的危害性。

7. 计算机病毒的寄生性

计算机病毒的寄生性是指，一般的计算机病毒程序都是依附于某个宿主程序中，依赖于宿主程序而生存，并且通过宿主程序的执行而传播。

8. 计算机病毒的不可预见性

计算机病毒的不可预见性体现在以下两个方面：

（1）计算机病毒的侵入、传播和发作是不可预见的　有时即使安装了计算机病毒实时防火墙，也会由于各种原因不能完全阻隔某些计算机病毒的侵入。事实上，任何软件都不能完全确保整个系统在任何时候没有任何计算机病毒，所以，对于计算机病毒防护人员而言，永远没有高枕无忧的时候。

（2）计算机病毒的发展速度远远超出了我们的想象　根据国际权威机构 ICSA(国际计算机安全协会)的统计报告显示，1999 年第一季度的计算机病毒数量是 1998 年同期的两倍，更是 1997 年的三倍。而且，计算机病毒的编制技术也是日新月异，各种新计算机病毒的出现不断给计算机病毒防范软件提出新的挑战。从这一点上看，计算机病毒防范软件似乎永远滞后于计算机病毒的发展，因此，新计算机病毒也许会永远不断地涌现，这一点它在人们的预料之中；但是病毒如何出现以及如何防范却永远是不可预料的。

1.5 计算机病毒的分类

从第一个病毒出世以来，究竟世界上有多少种病毒，说法不一。无论多少种，病毒的数量仍在不断增加。据国外统计，计算机病毒以 10 种/周的速度递增，另据我国公安部统计，国内计算机病毒以 4～6 种/月的速度递增。给病毒分类是为了更好地了解它们。按照计算机病毒的特点及特性，计算机病毒的分类方法有许

多种。因此，同一种病毒可能被分到许多不同的类别中。

1.5.1 按计算机病毒攻击的系统分类

1. 攻击 DOS 系统的病毒

这类病毒出现最早、最多，变种也最多。如 Stone、大麻病毒。

2. 攻击 Windows 系统的病毒

由于 Windows 的图形用户界面（GUI）和多任务操作系统深受用户的欢迎，因此 Windows 已经逐渐取代 DOS，从而成为病毒攻击的主要对象。如 CIH 病毒。

3. 攻击 UNIX 系统的病毒

当前，许多大型的操作系统均采用 UNIX 作为其主要的操作系统，所以 UNIX 病毒的出现，对人类的信息处理也是一个严重的威胁。

4. 攻击 OS/2 系统的病毒

世界上已经发现第一个攻击 OS/2 系统的病毒，它虽然简单，但却是一个不祥之兆。

1.5.2 按计算机病毒攻击的机型分类

1. 攻击微型计算机的计算机病毒

这是世界上传染最为广泛的一种病毒。

2. 攻击小型机的计算机病毒

小型机的应用范围是极为广泛的，它既可以作为网络的一个节点机，也可以作为小的计算机网络的主机。起初，人们认为计算机病毒只有在微型计算机上才能发生，而小型机则不会受到病毒的侵扰。但自 1988 年 11 月份 Internet 网络受到 worm 程序的攻击后，使得人们认识到小型机也同样不能免遭计算机病毒的攻击。

3. 攻击工作站的计算机病毒

近几年，计算机工作站有了较大的进展，并且应用范围也有了较大的发展，所以我们不难想象，攻击计算机工作站的病毒的出现，也是对信息系统的一大威胁。

1.5.3 按计算机病毒的链接方式分类

计算机病毒本身必须有一个攻击对象，才可以实现对计算机系统的攻击。计算机病毒所攻击的对象是计算机系统可执行的部分。