电脑操作指南

电脑防毒杀毒手册

崔永普　主编

经■济■管■理■出■版■社

图书在版编目（CIP）数据

电脑防毒杀毒手册 / 崔永普主编. —北京：经济管理出版社，2004
（电脑操作指南）
ISBN 7-80162-808-X

Ⅰ. **电**... Ⅱ. **崔**... Ⅲ. **计算机病毒—防治** Ⅳ. TP309.5

中国版本图书馆 CIP **数据核字（**2004**）第** 012489 **号**

出版发行：经济管理出版社

北京市海淀区北蜂窝 8 **号中雅大厦** 11 **层**

邮编：100038

印刷： **经销：新华书店**

责任编辑：张丽生
技术编辑：晓 成

责任校对：郭红生

850mm×1168mm/32 11.75 **印张** ■ 241 **千字**
2004 **年** 3 **月第** 1 **版** ■ 2004 **年** 3 **月第** 1 **次印刷**

印数：1—6000 **册** ■ **定价：**20.00 **元**

书号：ISBN 7-80162-808-X/F·727

电脑操作指南编委会名单

主 编：史俊杰　孙一林

编 委：贺　林　邵　丹　张　丽　刘文生

张世青　柳子文　乌　丹　沈　淞

郭　涛　笑　浓　李小旭　王浩君

窦　宏　岳小雨　江凌翔　楼小梅

曹　宁　康　强　白　勇　邢　聪

李　琳

前　言

“我的电脑中毒了!”

网络时代，人人“谈毒色变”。我们已经离不开网络带来的方便，但伴随而来的病毒泛滥却成了一个最头痛的问题，计算机病毒的威胁使广大用户终日忐忑不安。因此，怎样成功地预防各种病毒的侵袭，使计算机免遭病毒的破坏；又怎样在计算机不幸感染病毒之后，快速地检测和杀毒，就成了电脑用户的迫切需求。《电脑防毒杀毒手册》正是基于这些要求编写的。

本手册包括如下几个方面的内容：

1. 病毒的概念。通过一些介绍，使读者对电脑病毒有一个初步的认识，比如，计算机病毒的特征、分类、传播途径，电脑病毒的命名、破坏级别等。

2. 最新病毒档案室。主要包括最新的病毒档案，如“冲击波”病毒、“SQL 服务器”蠕虫病毒、“QQ 木马”病毒等。

3. 病毒的检测和清除。比如，怎样清除“恶邮差”病毒？怎样清除“红色代码”新变种蠕虫病毒？如何检测和清除“QQ 窃手”病毒？等等，包括手工方法和软件方法。

4. 病毒的防范和急救措施。比如，服务器如何防毒？

终端用户如何防毒？文件丢失后如何恢复？等等。

5. 常用杀毒软件及其使用技巧。比如，瑞星软件的使用技巧、金山毒霸的使用技巧等。

本书由崔永普主编，黄丹霞参加编写。在编写过程中得到了彭波、胡治国和李兵等同志的大力帮助，在此表示衷心的感谢！

由于电脑技术的飞速发展，加上时间紧迫，书中的错误和不足之处在所难免，恳请广大读者给予批评和指正。

编　　者

2003 年 10 月

第一章　电脑病毒的概念

1. 初识电脑病毒

首先，与医学上的病毒不同，电脑病毒即电脑病毒，它不是天然存在的，是某些人利用电脑软、硬件所固有的脆弱性，编制具有特殊功能的程序。由于它与生物医学上的病毒同样有传染和破坏的特性，因此，这一名词是由生物医学上的病毒概念引申而来。

从广义上讲，凡能够引起电脑故障，破坏电脑数据的程序统称为电脑病毒。依据此定义，诸如“逻辑炸弹”、“蠕虫”等均可称为电脑病毒。

1994 年 2 月 18 日，我国正式颁布实施了《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》第二十八条中规定：“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。”此定义具有法律性和权威性。

自从 Internet 盛行以来，含有 Java 和 ActiveX 技术的网页逐渐被广泛使用，一些别有用心的人于是利用 Java 和 ActiveX 的特性来编制病毒。以 Java 病毒为例，Java 病毒并不能破坏储存媒介上的资料，但若用户使用浏览器来浏览含有 Java 病毒的网页，Java 病毒就可以强迫你的 Windows 不断的开启新窗口，直到系统资源被耗尽，而你也不得不重新启动电脑。所以只要是对使用者造成不便的程序代码，就可以被归类为电脑病毒。

2. 电脑病毒的衡量标准

电脑病毒的最大特点是具有“主动传染性”。病毒可以侵入到整个系统，使其受到感染，而每个受感染的程序又可能成为新的病毒，继续将病毒传染给其他程序。一个病毒程序的关键性质在于，它能够传染给别的程序，并且具有传染性。这使它有别于同样具有隐蔽性、激发性和攻击性的逻辑炸弹、特洛伊木马等。传染性成为判定一个程序是否为病毒的首要条件。

3. 谁是电脑病毒的制造者

给人类进步带来严重危害的电脑病毒的制造者是人类自己。制造病毒的人有各种各样的动机,大致有如下几种：

(1)“电脑迷”的恶作剧。这类人多以青少年、大学生为主。他们缺乏法制观念和社会责任感，出于对电脑系统的好奇和兴趣，或为了显示自己的“聪明”，而制造病毒。

（2）出于报复心理。对单位领导或同事不满的软件开发人员，他们为了报复而编写电脑病毒程序，使憎恨对象遭受损害。例如，某国一家电脑公司的一名程序员被辞退后，决定对公司进行报复，离开前向公司电脑系统中输入了一个病毒程序，“埋伏”在公司电脑系统里。结果这个病毒潜伏了3年多才发作，造成整个电脑系统的崩溃，给公司造成了巨大损失。

（3）出于经济目的。利用电脑病毒从事经济犯罪，或窃取竞争对手的电脑系统中的机密信息，或修改电脑中的数据从而挪用款项，或破坏竞争对手的电脑系统。如日本某公司聘请病毒专家编制了专门对付竞争对手的病毒，以破坏对方电脑系统中的数据。

（4）出于军事目的。1990年5月8日纽约消息，美国军队悬赏研制摧毁敌人电子系统的电脑病毒。这种病毒能传递有意错报敌人命令的消息，也可以用来改变敌人向战斗部队传递信息的通信卫星软件，病毒可以通过无线电通信系统潜入敌方的电脑系统。

（5）出于政治目的。如“6·4”病毒就是一个以政治宣传和攻击为目的而传播的病毒，其政治影响远远大于其破坏能力，我国公安部已严令各省、市公安计算机监察机关追查该病毒。还有一些黑社会组织、恐怖分子，如国际上的“红色恐怖旅”、“消灭电脑委员会”、“制造电脑混乱俱乐部”等，他们都是以电脑作为攻击的对象。1988年，制造电脑混乱俱乐部专门召开了以病毒为主题的秘密会议，参加者数百人，会上不仅交换了已渗透到世界各地的大型电脑网络系统的口令和其他敏感信息，还交换了制造更高级病毒的

思想和技术。据预测，21 世纪国际恐怖活动采取的 5 种新武器中，电脑病毒名列第二。

4. 电脑病毒是看不见摸不着的吗

许多人以为电脑病毒也像生物病毒一样，是肉眼看不见的。其实，多数电脑病毒有自己的病毒现象。下面的纪实片段也许会让你想起，你曾经也看到过病毒现象。

1988 年底，一位旅美学者从美国带回来一台电脑，他在电脑里安装了一个称为 VirusGuard 的防病毒程序，人们好生兴趣地问：“ 电脑病毒什么时候才会光临中国 ?” 他认真地回答：“ 也许就在明年。” 在这之前，国内的一些报刊也曾报道过国外的电脑病毒，但都是在通信网络上传播的，不少人以为我国的通信网络发展才刚刚开始，电脑病毒离我们还远着呢。半年之后，那是 1989 年 4 月的一天，某计算中心发出了求救信号，那里的 7 台 PC/AT 电脑相继出现了圆点“ 小球 ” 在屏幕上不停地弹跳。后来的报道证实，这就是入侵我国的第一个电脑病毒。

1990 年 8 月，某县城一个工厂从省城购买了一套 386 系统设备用于工厂的 MIS 管理。不久之后，发现了一个怪现象，只要一发送打印命令，就提示“ . . . error writing device PRN ”，无法连机打印。工厂的技术人员详细检查了打印机接口和信号电缆，也检查了汉字操作系统和汉字打印驱动程序，甚至还把汉字操作系统卸掉，都无法连机打印。他们怀疑是打印机故障，就把打印机送去省城维修，检查结果是打印机没有故障。可是，他们将这个没有故障的打印机带回县

城连接在自己的386系统上，却仍然不能打印。他们只好将整套设备送到省城维修。经检查分析，原来是“Unprint”病毒在作怪。

所以说，多数电脑病毒都有自己的病毒现象，并不是看不见摸不着的。

5. 电脑病毒的传播途径

电脑病毒侵入一个系统，主要通过一个从磁盘装入的带病毒的程序，或者通过一个从网络通信交换的带病毒的程序。

电脑用户共享软件或使用来历不明的软盘是病毒传播的主要途径。尤其是PC电脑采用开放式系统，电脑病毒很容易在其间传播。更严重的是，在网络上大家共享服务器上的软件，一旦病毒通过任何一台工作站侵入服务器，那么另一工作站调用执行服务器上的带病毒的程序时，病毒就传播出去了。

另外，电子布告栏（BBS）也是病毒传播的一种途径，情况与网络相似。

6. 电脑病毒由哪些部分组成

电脑病毒大体上可以分为病毒引导程序、病毒传染程序和病毒病发程序三个部分。

7. 电脑病毒是如何运作的

电脑病毒的运作，可分为引导、传染和病发三个阶段。

（1）病毒引导阶段：电脑病毒被执行并开始活动。由于一个人不会故意去执行一个明知是病毒的程序，所以电脑病毒势必要附着（寄生）在其他可执行的程序（即宿主程序）上，以便在宿主程序被执行时，顺便执行自身。对于需要驻留内存的病毒，引导时会将病毒主体程序引导到内存的适当位置，并设置必要的参数。

（2）病毒传染阶段：病毒被引导之后，开始以各种方式将自身复制并附着到更多其他宿主程序上。这是电脑病毒的最大特色，也是技巧最难的部分。病毒的传染方式基本可分为两大类，一是立即传染，即病毒在被执行的瞬间，抢在宿主程序开始执行前，立即感染磁盘上的其他程序，然后再执行宿主程序；二是驻留内存并伺机传染，内存中的病毒检查当前系统环境，在执行一个程序或 DIR 等操作时传染磁盘上的程序，驻留在系统内存中的病毒程序在宿主程序运行结束后，仍可活动，直至关闭电脑。

（3）病毒病发阶段：潜伏在系统中的病毒处于发作就绪状态，一旦引发病毒，系统就会执行病毒发作所需的操作。

8. 电脑病毒的破坏级别

（1）无害型。这类病毒除了传染时减少磁盘的可用空

间外，对系统没有其他影响。

（2）无危险型。这类病毒仅仅是减少内存，显示图像，发出声音及同类音响。

（3）危险型。这类病毒在电脑系统操作中造成严重的错误。

（4）非常危险型。这类病毒删除程序、破坏数据、清除系统内存区和操作系统中重要的信息。

这些病毒对系统造成的危害，并不是本身的算法中存在危险的调用，而是当它们传染时会引起无法预料的和灾难性的破坏。由病毒引起其他程序产生的错误也会破坏文件和扇区，这些病毒也按照他们引起的破坏能力划分。一些现在的无害型病毒也可能会对新版的 DOS、Windows 和其他操作系统造成破坏。例如，在早期的病毒中，有一个“ Denzuk ”病毒在 360K 磁盘上可以很好地工作，不会造成任何破坏，但是在后来的高密度软盘上却能引起大量的数据丢失。

9. 电脑病毒的特征

（1）传染性。这是病毒的基本特征。在生物界，通过传染生物病毒从一个生物体扩散到另一个生物体。在适当的条件下，它可以大量繁殖，并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。与生物病毒不同的是，电脑病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它会搜寻其他符合其传染条件的程

序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。如果一台计算机染毒后不及时处理，那么病毒会在这台机器上迅速扩散，其中的大量文件（一般是可执行文件）会被感染。而被感染的文件又成了新的传染源，当与其他机器进行数据交换或通过网络接触，病毒会继续进行传染。

正常的计算机程序一般是不会将自身的代码强行连接到其他程序之上的。而病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。计算机病毒可通过各种可能的渠道，如软盘、计算机网络去传染其他计算机。当你在一台机器上发现了病毒时，往往曾在这台计算机上用过的软盘也已感染上了病毒，而与这台计算机联网的其他计算机也许已被该病毒传染上了。是否具有传染性是判别一个程序是否为电脑病毒的最重要条件。

未经授权而执行。一般正常的程序是由用户调用，再由系统分配资源，完成用户交给的任务。其目的对用户是可见的、透明的。而病毒具有正常程序的一切特性，它隐藏在正常程序中。当用户调用正常程序时，它窃取系统的控制权，先于正常程序执行。病毒的动作、目的是用户未知的，当然也是未经用户允许的。

（2）隐蔽性。病毒一般是具有很高编程技巧、短小精悍的程序。通常附在正常程序中或磁盘较隐蔽的地方，也有个别的以隐含文件形式出现。目的是不让用户发现它的存在。如果不经过代码分析，病毒程序与正常程序是不容易区别开来的。一般在没有防护措施的情况下，计算机病毒程序取得系统控制权后，可以在很短的时间里传染大量程序。而且在

受到传染后，计算机系统通常仍能正常运行，使用户不会感到任何异常。试想，如果病毒在传染到计算机上之后，机器马上无法正常运行，那么它本身便无法继续进行传染了。正是由于隐蔽性，计算机病毒得以在用户没有察觉的情况下扩散到上百万台计算机中。

大部分病毒的代码之所以设计得非常短小，也是为了隐藏。病毒一般只有几百或 1K 字节，而 PC 机对 DOS 文件的存取速度可达每秒几百 KB 以上，所以，病毒转瞬之间便可将这短短的几百 KB 附带到正常程序之中，非常不易察觉。

（3）潜伏性。大部分的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，这样它才可广泛地传播。如“ PETER－2 ”在每年 2 月 27 日会提三个问题，答错后会将硬盘加密。著名的“ 黑色星期五 ”在逢 13 号的星期五发作。国内的“ 上海一号 ”会在每年 3、6、9 月的 13 日发作。当然，最令人难忘的便是 26 日发作的“ CIH ”。这些病毒在平时会隐藏得很好，只有在发作日才会露出本来面目。

（4）破坏性。任何病毒只要侵入系统，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。据此可将病毒分为良性病毒与恶性病毒。良性病毒可能只显示一些画面或出点音乐、无聊的语句，或者根本没有任何破坏动作，但会占用系统资源。这类病毒较多，比如，“ GENP ”、“ 小球 ”、“ W－BOOT ”等。恶性病毒则有明确的目的，或破坏数据、删除文件，或加密磁盘、格式化磁盘，有的对数据造成不可挽回的破坏。这也反映出病毒编制者的险恶用心。

（5）不可预见性。从对病毒的检测方面来看，病毒还有不可预见性。不同种类的病毒，它们的代码千差万别，但有些操作是共有的（如驻内存，改中断）。有些人利用病毒的这种共性，制作了声称可查所有病毒的程序。这种程序的确可查出一些新病毒，但由于目前的软件种类极其丰富，且某些正常程序也使用了类似病毒的操作甚至借鉴了某些病毒的技术。使用这种方法对病毒进行检测势必会造成较多的误报情况。而且病毒的制作技术也在不断的提高，病毒对反病毒软件永远是超前的。

简言之，病毒的特征可以概括为：人为的特制程序，具有自我复制能力，很强的感染性，一定的潜伏性，特定的触发性，很大的破坏性。

10. 电脑病毒是硬件故障或编程失误吗

电脑病毒都是一组精心编制的指令，不可能随机地自然产生，也不可能由偶然的硬件故障或软件编程失误造成。所有的电脑病毒都是人为地有意制造出来的。

11. 电脑病毒是如何命名的

正像生物病毒一样，每一种电脑病毒都有自己的名字；同时，也正像生物病毒一样，每一种电脑病毒的名字也是人定的。从目前的情况看，电脑病毒有两种来源：一种是本地的电脑病毒；另一种是国外传进来的电脑病毒。而电脑病毒的定名则有三种情况：一是国人对电脑病毒的定名；二是援

引国外对病毒的英文定名；三是病毒国外定名的中文译名。

需要提出的是，一种名称神秘的病毒并不意味着这种病毒神秘且不可攻破，也并不一定意味着这种病毒的破坏力就很大。

12. 电脑病毒的分类

电脑病毒以依托对象来分类，可分为大、中、小型机和微机病毒，微机病毒可分为依托 Intel 系列指令系统的 PC 病毒和依托 MOTOROLA 6800 指令系统的 APPLE II 、Macintosh 机病毒等。IBM PC 电脑及其各种兼容机，包括我国的长城、联想、浪潮等各种国产兼容机，其总数在世界上已超过几千万台，仅我国就有几百万台，因而这类病毒的产生机会和传播途径都是很可观的。目前在我国流行的病毒包括国产病毒几乎都是 PC 病毒。本书所述的电脑病毒机制、杀毒与防毒技术都是基于 PC 病毒。

电脑病毒以传播媒介来分类，可分为单机病毒和网络病毒。单机病毒的载体是磁盘，常见的是病毒从软盘传入硬盘，感染系统，然后再传染其他软盘，软盘又传染其他系统。网络病毒的传播媒介不再是移动式载体，而是网络通道，这种病毒的传染能力更强，破坏力更大。

电脑病毒以病发的危害程度来分类，可分为良性病毒、恶性病毒和中性病毒。一般良性病毒是指那些具有攻击性质并无恶意的病毒程序，它不破坏电脑系统的数据，只是干扰人—机界面，如屏幕出现小球滚动，键盘接收速度减慢，程序执行中断必须输入指定字符才可继续等。恶性病毒是指那

些具有破坏性的病毒程序，它破坏电脑系统或软、硬盘上的数据，如修改文件分配表，更改盘上数据，或对盘格式化等。中性病毒是指那些具有恶意攻击性质而没有破坏性的病毒程序，它往往是向电脑用户挑战，好像是机器出毛病，但并不破坏电脑系统的数据，如修改引导程序，使硬盘引导失败，或把文件分配表隐藏起来等。

电脑病毒以病毒寄生嵌入方式来分类，大体可分为：

① 操作系统病毒。它用自己的程序意图加入或取代部分操作系统进行工作，这种病毒具有很强的破坏力，可以导致整个系统的瘫痪。

② 源码病毒。这类病毒在程序被编译之前插入到 FORTRAN、C 或 Pascal 等语言编制的源程序，完成这一工作的病毒程序一般是在语言处理程序或连接程序中，或者随系统隐蔽在内存中。

③ 外壳病毒。这种病毒较常见，常附在主程序的头尾，对原程序不做修改，易于编写，也易于发现，一般测试可执行文件的大小即可知。

④ 入侵病毒。这种病毒侵入到主程序之中，并替换主程序中部分不常用到的功能模块或堆栈区，一般是针对某些特定程序而设计的，较难编写，一旦入侵程序体后也较难消除。

根据病毒特有的算法来分类，又可以分为如下几类：

① 伴随型病毒。这类病毒并不改变文件本身，它们根据算法产生 EXE 文件的伴随体，具有同样的名字和不同的扩展名（COM），例如，XCOPY. EXE 的伴随体是 XCOPY. COM。病毒把自身写入 COM 文件并不改变 EXE 文