跟我学电脑 丛书

五笔字型发明人　王永民教授　主编

计算机病毒的检测、清除和预防

冯宇彦　蒋平　编著

北京·气象出版社

跟我学电脑

计算机病毒的检测、清除和预防

冯宇彦　蒋平　编著

气象出版社

图书在版编目(CIP)数据

计算机病毒的检测、清除和预防/冯宇彦，蒋平编著. -北京：气象出版社，1997.9
(跟我学电脑/王永民主编)
ISBN 7-5029-2320-9

Ⅰ.计… Ⅱ.①冯… ②蒋… Ⅲ.①计算机病毒-检测②计算机病毒-消除③计算机病毒-预防 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(97)第 09472 号

气象出版社出版
(北京西郊白石桥路 46 号　邮编：100081)
责任编辑：郭彩丽　终审：周诗健
封面设计：陈云峰　责任技编：都平　责任校对：时人
*
北京科技印刷厂印刷
气象出版社发行　全国各地新华书店经销
*
开本：787×1092　1/16　印张：13.25　字数：326 千字
1997 年 9 月第一版　1997 年 9 月第一次印刷
印数：1—5000　定价：22.00 元

难得一套电脑科普书

前天，纽约时报公布了本周内纽约州畅销书的排行榜。名列榜首的书，是一本理论物理学的科普读物《时间简史》(A Brief History of Time)，作者斯蒂芬·霍金(Stephen Hawking)，被誉为自爱因斯坦以来当代最伟大的天才理论物理学家。他以残废之身在轮椅上研究著述了20多个年头。评论文章称，他的这本书是在世界上引起轰动、在纽约连续100个星期销量排名第一的书，发行已超过100万册。

我立即到书店花16美元买了一本，一口气翻完了180页正文。啊！这真是一本我从未见过的令人不忍掩卷的科普书。作者把高深的理论，诸如什么是时间，时间有无头尾，什么是宇宙和黑洞，什么是相对论等等，讲得通俗易懂，趣味盎然！

一本高深理论物理学的科普书居然会如此畅销，的确是发人深省的。

也许，科普书的难点正在于写"深"容易，写"浅"反而难！不是真正精于一门的饱学之士，不是真正了解读者心理的大手笔，便很难写出好的科普书。正所谓"明白不明白的人为什么不明白，才算真明白"。

然而电脑，实在不是一般人容易弄明白的洋机器。

继西方世界全面实现电脑化之后，电脑用于机关，电脑走向民间，在国内已蔚然成风。要让国人明白电脑是怎么一回事，要让普通人学会操作电脑，除了开展正规教育之外，我以为最重要的，恐怕就是编写一套通俗易懂、趣味盎然的自学丛书，满足为数更多的自学者的要求。

事实上，电脑并不高深莫测。不少人对电脑望洋兴叹，常常是因为那些厚厚的叫人眼花缭乱而又枯燥无味的操作手册、用户指南使人望而生畏，不敢问津。

现在，这种情况可望有所改善。我看了中国气象出版社出版的《跟我学电脑》丛书一套11册的初稿，觉得这套丛书具有以下特色：

一、实用性强。书中介绍的都是最基本的电脑知识，着重于实际应用和操作方法，看了就明白，明白了就能用。

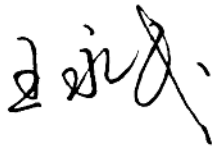
二、图文并茂。书中附有大量的电脑屏幕图，以图解文，直观教学，形象生动，另配有许多漫画，可使读者迅速领会，印象深刻。

三、浅显易懂。丛书为初学者编写，尽量避免抽象概念，自学者不必死记硬背，只管照章操作，即可熟练掌握，无师自通。

这真是一套难得的电脑科普书。对国内读者来说，可谓是雪中送炭。

而且，这是一套具有《时间简史》一书特色的好书！

我相信，这套丛书也会像《时间简史》在美国受到欢迎一样，在中国乃至国外华人界受到欢迎。特此向中国气象出版社表示祝贺和感谢，是为序。



1997 年 5 月 6 日于纽约 Flushing

引　言

1989年以来，在我们日新月异的生活中，又出现了一个新成员——计算机病毒。计算机工作者无不关注计算机病毒；受害的用户忙于收拾残局；计算机应用领域的专家在忙于寻找对策。“病毒”的肆虐弄得人们一时不知所措，有人错把计算机硬件或软件的故障也怪罪成病毒。本书的目的即是让您认识计算机病毒，掌握检测、消除和预防计算机病毒的方法，为计算机更广泛地应用铺平道路。

本书特点

1. 浅显易懂。全书尽量避免晦涩难懂的专业术语，以生动活泼的语言向您介绍了对付计算机病毒的各种方法。

2. 实用性强。本书在向您介绍病毒的生成、消除和预防的原理的同时，辅之以典型的实例，并配有生动形象的漫画帮助您理解，您可以一边学习原理，一边学习上机操作。

本书结构

全书共9章。第1和第2章讲述病毒的表现和来历；第3章介绍DOS的基本知识，为您了解病毒的原理(第4章)做准备；第5章介绍如何检测计算机病毒的存在；第6章便教给您如何杀除病毒；第7章则是有关预防计算机病毒再次捣乱的各种方法，至此您便具备了防治计算机病毒的基本知识和能力；第8章为您提供了您进一步提高反病毒能力的知识、技能和技巧的行动指南；最后，第9章对各种典型的病毒进行了剖析，使您在学习完本书之后，自然而然地就具备了反病毒的重要经验。

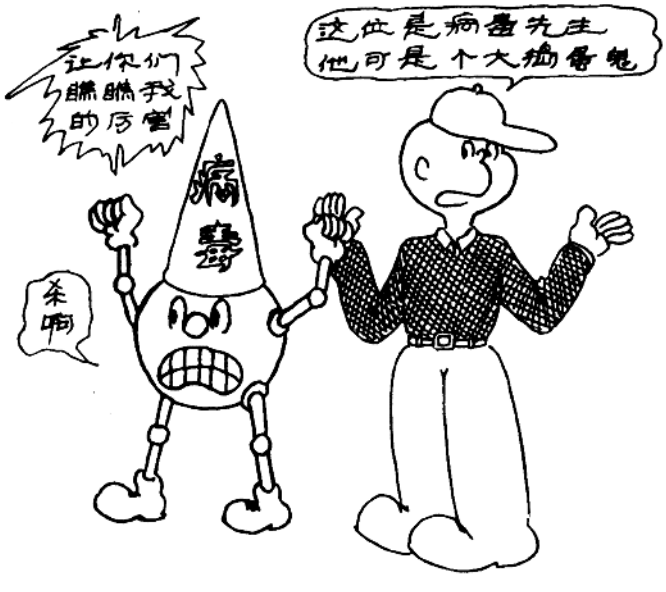
本书的阅读方法

本书是专门为您——计算机的初学者设计和写作的。各章的内容既有其内在的有机联系，又保持了其相对的独立性。您可以按部就班、一章一章地阅读；或者您对其中的某些内容已经比较熟悉，那么也可以跳过不读，拣您最需要的部分阅读。

欢迎您加入反病毒阵营！

目　录

第1章
病毒来了



- 变态的计算机
- 这就是病毒
- 病毒并非很可怕

1.1 变态的计算机

1989年春的一天，厄运突然降临到我心爱的IBM PC原装机身上。

在我依照平常的习惯，先打开显示器的开关，然后启动计算机，一切都如从前。但是，一切微妙的事情都是因为“但是”而发生了根本的变化，当我开始工作了半个小时的时候，显示器上突然出现了一个小圆点，并且来回移动。也许你可以称之为一个小球，因为它不停地弹跳，碰到屏幕显示区的边缘之后就好像碰在墙上一样以一定角度反弹，如此反复，永不知疲倦。如果这个小球仅仅只是在屏幕上窜一窜，那也无所谓，给枯燥的上机还能带来一点点新奇。但是，令我不堪忍受的是，这个小球在运动过程中，一旦碰到了任何的字符，就把那个字符吞掉了。就像一条贪婪的大鲨鱼，吞食着它遇到的一切。这样，我的屏幕很快变得难以辨认，我再也无法进行任何工作。我只有两种选择，要么坐在终端桌前看着小球的弹撞，要么关闭计算机。

后来，总参气象局来了两位同志，说是他们发现了计算机病毒，并且经过分析研究而找到了解决的方法，所以，他们首先来到了同一领域的气象部门。较年轻的一位同志将带来的一片软盘插进我的机器，然后重新启动计算机。机器启动之后，他们运行了一个软盘上的程序，程序输出了一些数据，他们看了数据后，肯定地说：“这台微机感染了计算机病毒。”

这是我第一次听到“计算机病毒”这个词。从那之后，我再也摆脱不了病毒这一阴影的纠缠，我见过各式各样的计算机病毒。我第一次遇到的这个病毒，因为像一只乒乓球一样不停地弹来弹去，故被称为“乒乓病毒”。又因为其圆形的形状，也有人称之为“圆点病毒”或“小球病毒”。

1.2 这就是病毒

提到病毒，许多人会想起造成流行性感冒或是AIDS(爱滋)病这样的生物性病毒。记得在情景剧《电脑之家》中，赵一江家的电脑由于使用盗版软件而染上病毒后，一家人吓得带上了口罩，并在屋内喷上了消毒水。

事实上，我们这本书所说的病毒是“计算机病毒”的简称。我们可以对病毒作出下述定义：

一种传染性的寄生程序，它只在指定的程序或程序包中繁殖，并对计算机系统的正常工作造成影响。

有人更一针见血地说：“一个天生的捣乱者，这就是病毒。”

不过，上述说法只是一个大致的定义，我们将在第3章中给出更严格和更全面的定义。

1.3 病毒并非很可怕

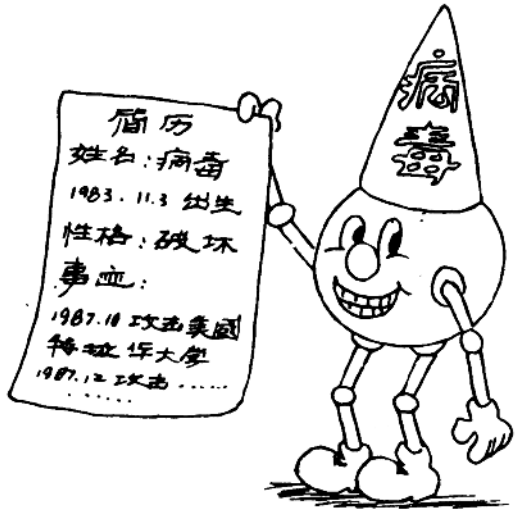
病毒的特点在于隐蔽性、传染性和破坏性。病毒常常在不知不觉中侵入了你的系统，又不知不觉地在有联系的系统中传染开来，当它跳出来展示自己时，计算机系统已经被破坏了。这就是大多数人畏之如虎的原因。

不知诸位见过饲养毒蛇的人没有，在平常人眼中，眼镜王蛇、竹叶青、五步蛇等毒蛇都是杀

人不见血的魔头，而他们却视之无物，可以毫无顾忌地接近它们，甚至戏耍它们。这是为什么呢？

原因很简单，就是因为养蛇人摸透了毒蛇的生活规律，知道它的弱点。如果我们也对计算机病毒了如指掌，知道它的原理、规律及弱点，那么我们还有什么可怕的呢？这就是本书的目的，也是诸位读者继续看下去的理由。

第2章
病毒的来历



●病毒的历史回顾
●谁制造的病毒

任何事物的产生都有其根源，病毒也不例外。计算机病毒产生的根源就是计算机技术的发展。确切地说，计算机硬件的普及和小型化为病毒的产生提供了舒适的环境，而计算机软件的发展则为病毒的产生提供了必要的手段。这并不是说，我们就不应该发展计算机技术，就像核技术一样，关键在于谁使用它以及如何使用它。在这一章中，我们来回顾一下病毒的发展史，看看它是如何从无到有，并逐渐发展、为害人间的。同时，我们也可以看到，人们是如何发现、认识，以及正确对待病毒的。

2.1 病毒的历史回顾

一、实验室病毒

计算机界首次引入病毒这一概念，是在 1983 年 11 月 3 日的一个关于计算机安全的学术讨论会上，由 Lew Adlemen（卢·安得理曼）提出，并由 Fled Cohen（弗莱德·科恩）博士首次介绍了原理。

当时，在一台使用 UNIX 操作系统的 Vax 11/750 机上，实验演示了第一个病毒。由于当时的系统管理人员对于病毒的危害和可能造成的破坏一无所知，或者说是知之甚少，他们同意了关于计算机病毒的有关实验。于是，计算机专家们整整准备了八个小时，完成了病毒演示的前奏曲。

为了避免病毒的传播失控，病毒体的植入是由手工完成的，同时还采取了诸多措施，使得病毒在监测范围之中，系统被病毒侵入的时间都不超过 60 分钟。系统的最快一次受感染只经过了短短的五分钟，平均受染时间在半个小时以内。

这一结果在讨论会上被宣布之后，引起了与会者的极大兴趣。人们首次看到了计算机病毒的危害性和威胁性。在实验过程中，没有被告知有病毒入侵的系统遭到了感染，这是不足为奇的；然而，预先知道了有病毒攻击的系统同样也难逃厄运。这一事实不能不令人们瞠目结舌。监视和检测数据指出，在不到半秒钟的时间内，病毒就可以感染系统。

系统管理人员对这一结果惊诧万分，尤其是机构中负责安全工作的行政人员，坚决反对再进行类似的试验。一直到 1984 年 3 月，计算机专家们在一台 Univac 1108 的计算机上进行了另外的实验。这次实验仅仅被允许在 26 小时之内，而且专家们此前从未在 1108 机型上操作过，还得不到熟悉 1108 系统的程序员的协助。尽管如此，1108 机还是在 18 个小时之后被病毒所感染，感染过程不到 20 秒。在 26 小时的实验结束之后，病毒不仅感染了普通用户，超级用户也未能幸免。这次实验再一次表明了病毒对没有缺陷的操作系统入侵的可能性。

专家们编制的这一计算机病毒，使用的是 FORTRAN 语言，一种专门用于科学计算的计算机语言，其源程序也就在 200 行左右。另外由于 FORTRAN 又支持系统的调用，源码中还有 5 行 12 编代码和约 50 行的命令文件。在现在来看，一个老练的程序员在一两个星期之内，就可以完成这一工作。

据知情人士透露，这还够不上病毒史的第一。

1977 年仲夏，美国科普界一本名为《Adolescence of P-1》的科幻小说极为走俏。在这部小说中，作者描述了一种能够在不同的计算机中间相互感染和传播的病毒。最后病毒控制了数以

千计的计算机，而且还企图来控制人类。

人们猜测这部小说的作者，是从贝尔(Bell)实验室年轻研究人员的游戏中受到了启发。早在60年代的初期，美国的电报电话公司有一个著名的贝尔实验室，那儿的年轻人在完成工作之余，热衷于玩一种他们自己发明的计算机游戏。这种游戏的玩法就是，每位参入者独自编写一段程序，然后输入计算机里运行，并且不能再进行任何的人工控制。由这些程序相互之间进行进攻，以吃掉别人的程序作为胜利的标志。这些程序，应是计算机病毒的最早雏形。那时候工作在贝尔实验室的年轻研究人员，绝对想不到他们发明的游戏，被后人玩得更火。

二、真刀真枪的病毒

上一节中我们介绍的只是计算机界提出的供研究使用的病毒，为了掌握病毒的行为，科学家们对它做了许多修改，它的攻击性并没有达到高峰。也许在实验室中证实了病毒的存在之前，已经有了一些有关发现病毒的报告。但它们都没有引起人们足够的关注，直到1987年秋，计算机病毒才开始在世界范围内受到新闻媒介的普遍重视。

1987年末的三个月中，计算机病毒攻击了三所大学，两所美国大学，一所以色列大学：

- 1987年10月，智囊(Brain)或称巴基斯坦(Pakistan)病毒攻击了美国的特拉华大学。
- 1987年11月，在宾西法尼亚州的利哈伊大学发现了利哈伊或称COMMAND.COM病毒。
- 1987年12月，位于以色列耶路撒冷的希伯莱大学发现他们受到了计算机病毒的攻击，经过严格检查，他们发现了黑色星期五病毒，而且在进一步的检查中，又发现了两个名为四月一日病毒或称四月愚人节病毒的病毒变种。

巴基斯坦病毒以第一个攻击美国测试实验室之外的计算机而出名。自从在特拉华大学被发现后，它已经攻击了世界各地的大学，甚至还攻击了一些商业部门，如美国罗德岛的期刊公告牌系统(Journal Bulletin)。之所以将它命名为Brain病毒是因为该病毒将Brain这个词作为卷标(Label of Volume)写到被感染的任意磁盘上，通过对一张被感染的磁盘的分析，人们知道了病毒编写者的名字：Basit和Amjad，地址是巴基斯坦的拉合尔(Lahore)，所以，该病毒又被称为巴基斯坦病毒。

巴基斯坦病毒是一种引导扇区感染型病毒，它将自己的主体部分置于被感染盘的坏扇区中，而不是完全置于引导扇区内。它只感染360KB双面双密度的5.25英寸软磁盘，并通过在FAT表的第四、五字节填入"34 12"表明此磁盘已被感染，如果下次再遇到这张盘就不会传染了。

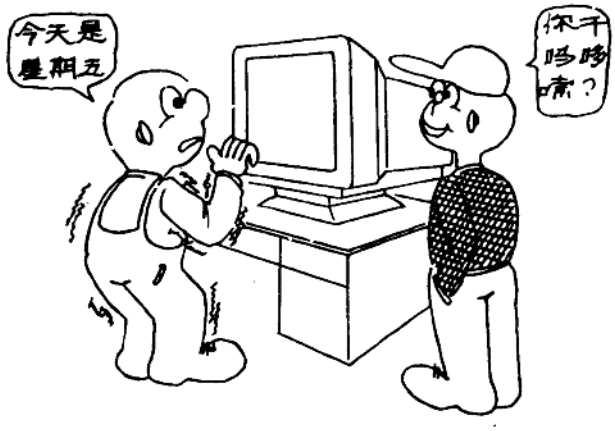
如果你用感染了巴基斯坦病毒的软磁盘启动系统的话，它就会通过取代中断向量INT 13H而取得系统的控制权。在你对系统进行操作的过程中，它始终注意系统对A或B磁盘驱动器的读操作，如果被感染标志没有出现，那么它就把三个坏簇标志写入磁盘的FAT表中，然后把原来的引导记录写入第一个坏扇区，而把病毒的其余部分写入剩下的扇区。病毒的引导扇区保留在内存中，被病毒修改过的引导扇区写入被感染磁盘的引导扇区中。最后，软盘的卷标被改为"(c)Brain"。

同巴基斯坦病毒相似，利哈伊病毒也试图通过磁盘的引导来传播，但它感染的不是磁盘的引导扇区，而是DOS的命令解释程序COMMAND.COM。COMMAND.COM在系统被引导

后驻留在内存中，负责解释用户敲入的DOS命令。当微机被一张被感染的盘引导时，已改变的COMMAND.COM程序就驻留在内存中。病毒截取DOS中断INT 21H功能的请求，如果用户敲入DIR、TYPE等引起"执行可执行程序"或"找到第一个文件"功能请求的常用DOS命令时，病毒代码就被激活。它首先检查被使用的磁盘是否为可引导磁盘，即是否含有COMMAND.COM程序。如果有，病毒就将自己拷贝到磁盘上，然后把事先设置的计数值加1，表示又有一张磁盘被感染了。当计数值大于或等于4时，病毒的第二部分就开始它的破坏性工作。病毒的第二部分在有硬盘的系统上使用DOS中断INT 26H(绝对写磁盘操作)将硬盘的头32个扇区全部写上0。这一操作将磁盘的引导扇区和目录表清除一空，被清除的磁盘就无法使用了，尽管有经验的程序员可能恢复部分盘上的数据，但效果极不理想，花费的时间和精力也很多。建议你将时间花在重新格式化磁盘和拷贝备份文件上。

1987年12月耶路撒冷的希伯莱大学的工作人员发现一些他们过去经常执行的程序突然变大而使内存容量不够，从而使程序不能运行。学校计算中心的计算机专家Yisrael Radai先生进行封闭式检查后发现，每次执行一个.EXE程序，该程序的长度就增加1808个字节，.COM程序也增加同样大小的字节，与.EXE程序不同的是它只增加一次。工作人员通过研究发现是一种病毒捣的乱，这种病毒被命名为"耶路撒冷病毒"。

进一步的研究发现，这种病毒不仅增加了可执行程序文件的长度，而且在微机的内存被感染30分钟后，计算机的处理速度明显地减慢了。病毒的发作还在于：当病毒驻留内存时，如果当前的系统日期是从1988年开始的任何一个13日又是星期五的话，则每一个被执行的程序都将被病毒从磁盘上删除，多么恶劣的行为！有鉴于病毒发作的特殊时日，这种病毒又被称为"黑色星期五病毒"。



黑色星期五病毒与前面介绍过的两种病毒都不太一样，它是通过感染以COM和EXE为后缀的可执行程序文件来传播自己的，而巴基斯坦病毒和利哈伊病毒都是通过感染磁盘的引导系统而传播的。通常，我们把感染可执行文件的病毒称为文件型病毒，而把只感染磁盘的引导系统的病毒称为引导型病毒。当你在一个干净的计算机系统中执行了带毒的程序后，病毒就将自己放入程序段前缀(PSP)之后的内存起始处，并替换掉DOS的中断INT 21H，然后检测系统当前日期：

- 如果年号为 1987，则病毒不发作。
- 如果年号不是 1987，且日期是 13 号星期五的话，病毒就设置破坏标志，而不感染可执行程序。
- 如果年号不是 1987，且日期不是 13 号星期五的话，病毒便替代时钟中断 INT 8H，给程序制造一些“无伤大雅”的障碍（减慢程序运行速度），然后调入要执行的程序。

病毒驻留内存后，提供下列功能：

- 提供已有病毒驻留、防止病毒再次驻留的信号；
- 为病毒的正常工作提供功能调用；
- 感染其它可执行程序；
- 时机适当时造成危害。

以上我们介绍了三个引起新闻界重视的病毒，它们是早期病毒的代表，随着人们对病毒的认识不断加深，再加上新闻媒体的大肆宣传，制造病毒与查解病毒开始成为一个热门的话题，并且，二者之间的斗争也进入了一个持久阶段。

三、论持久战

不知是病毒的不断产生激发了新闻界的报道热情，还是新闻界的报道热情激发了病毒制造者的热情。反正自从巴基斯坦病毒、利哈伊病毒和耶路撒冷病毒出名后，又有许多新兴的病毒以其特殊的表现出尽了风头。如我们前面提到的乒乓病毒，还有大麻病毒。

病毒是一种很奇怪的东西，它可以代表一种高技术的殊荣，于是有许多人为了获得这份殊荣不惜制造这种损人不利己的东西。也许他在报纸上看到关于自己编制的病毒发作的报道心里会窃笑，但当自己的计算机也被自己制造的病毒感染的时候，不知道他会是什么心情？

其实，编制反病毒程序也可以表示一个人的编程水平之高超。有许多人因为致力于编制反病毒程序而堂堂正正地出了名，如美国的 McAfee。它甚至为此创办了一个公司，专门出品 SCAN 系列查毒软件。

一场持久战就在反病毒程序的编制者和病毒程序的编制者之间展开了。