电脑活用百问丛书

附送实用光盘

计算机病毒防治活用百问

主　编　吴启迪

副主编　陆金山　王岩增

上海科学技术出版社

电脑活用百问丛书

计算机病毒防治活用百问

主　编　吴启迪
副主编　陆金山　王岩增
编　委　孔闻琳　来可伟　廖志成
　　金　锴
审　稿　何支涛　张世永
策　划　郭景锋

上海科学技术出版社

本书配有光盘，需要者请到网络光盘实验室拷贝

图书在版编目(CIP)数据

计算机病毒防治活用百问/吴启迪编著.—上海：上海科学技术出版社，2002.1
（电脑活用百问丛书）
ISBN 7-5323-6332-5

Ⅰ.计… Ⅱ.吴… Ⅲ.计算机病毒－防治－问答
Ⅳ.TP309.5-44

中国版本图书馆CIP数据核字（2001）第083279号

上海科学技术出版社出版发行
（上海瑞金二路450号 邮政编码200020）
上海市印刷十一厂印刷 新华书店上海发行所经销
2002年1月第1版 2002年1月第1次印刷
开本 850×1168 1/32 印张 5 字数 160 000
印数 1—5 200 定价：18.00元
本书如有缺页、错装或坏损等严重质量问题，
请向本社出版科联系调换

前　言

我们先来看一看下面两个触目惊心的事例，也许会给你一点启示！

例 1：1999 年 4 月 26 日，一种被称为 CIH 的计算机病毒在本市全面爆发，这次病毒涉及面之广、危害性之大，是上海历史上最严重的一次。

CIH 病毒源自台湾，首次发现是 1998 年 6 月。目前已知的病毒变种主要有三种，一种是每月 26 日爆发，一种是 6 月 26 日爆发，而最厉害的一种是 4 月 26 日爆发。

这种计算机病毒的传染力强、破坏性大，对付该病毒的唯一有效方法就是在病毒发作前将其查杀。病毒一旦发作，其造成的损失是相当严重的：它会改写计算机硬件主板 BIOS，破坏硬盘分区表，全面毁坏硬盘上的所有数据。政府机关、科研机构、各类院校、新闻媒体、金融机构、工厂企业、家庭、网吧都不同程度地受到冲击。某大学的机房里，学生实习上机，数十台计算机连续被该病毒破坏。一些科研机构、设计单位也发生几台到数十台计算机遭受病毒袭击的情况，重要科研数据、设计图纸遭到破坏，损失惨重。这次受到侵袭比例最高的是个人用户。全市一天内受到 CIH 病毒影响的计算机数量估计不低于一万台。

CIH 计算机病毒在上世纪末的 1999 年 4 月 26 日凶猛地扑向全球未设防的计算机和网络系统，根据初步统计，全世界至少有 6000 万台计算机遭受到它的侵害，国内（不包括台湾、

香港及澳门地区）受损的计算机总量达到了 36 万台，其中主板受损占了 15%，所造成的经济损失达数十亿元。而且，通过因特网传播的计算机病毒来势迅猛，爆发事件接连不断。

例 2：据上海电视台 2000 年 5 月 8 日晚间新闻报道，“5 月 6 日中国远洋集装箱运输有限公司遭到爱虫病毒的攻击，估计有 4 万 5 千条爱虫通过电子邮件进入公司数百个用户邮箱，绝大部分爱虫病毒来自西欧北美公司。”

经了解，该公司是一家国内大型企业，拥有 100 多条远洋运输船舶，公司各级领导对计算机病毒防范以及信息系统的安全历来非常重视，要求“五一”期间值班的系统管理员进行严密监视。5 月 6 日公司发现带有爱虫病毒的邮件后，按照公司领导的布置，系统管理员随即采取了有效措施：一边到因特网上下载最新的杀毒软件及时对服务器进行了清除病毒工作；一边通过电子邮件发出紧急通知，要求用户对爱虫计算机病毒提高警惕。由于公司分布在世界各国的用户邮箱有数百个之多，加上每个邮箱收到的计算机病毒邮件又非常多，累计杀除 4 万 5 千多条爱虫病毒，并赶在用户 8 日上班之前将计算机病毒清除干净，避免了一场整个公司计算机信息系统遭受重创的灾害性事故。

严峻的事实已经摆在我们面前：随着国民经济和社会信息化的发展，因特网的日益普及，计算机已经在政治、经济、军事和文化等各个领域发挥越来越重要的作用，并在许多领域占有举足轻重的地位。这给我们在带来新机遇的同时也带来了风险。新的计算机病毒层出不穷，势头不减，直接威胁到各行各业的经济活动。

CIH 和爱虫病毒造成全世界计算机瘫痪和经济损失的情况如下表所示：

CIH 和爱虫病毒造成全世界计算机瘫痪和经济损失情况表

计算机病毒名称	发作日期	全球危及计算机	全球经济损失
CIH	1999.04.26	6000 万台	数十亿美元
I LOVE YOU	2000.05.04	4500 万台	100 亿美元
CodeRed	2001.08	1000 万台	26 亿美元

近来，“Funlove”、“马吉斯”（Magistr）、“红色代码 II”、“尼姆达”（NIMDA）等各类病毒在全世界频繁发作并迅速传播，给我们提出了新的问题和更深层次的思考。可以预料，今后计算机病毒发展的一个趋势将会是传播方式越来越先进、发作规模越来越大，其后果必定是经济损失越来越严重。

读了上面短短的叙述，也许会引起你的深思：

那么，

什么是计算机病毒？

计算机病毒的危害是怎样的？

计算机病毒是怎样传播的？

计算机病毒应该怎样防治？

……

这一连串的问题，都将在本书中一一给予介绍。

序

近年来，随着计算机的普及特别是因特网的蓬勃发展，计算机病毒在世界范围内泛滥成灾。数以千万计的计算机遭到破坏，用户的数据被吞噬，直接和间接的经济损失无法估量，这使人们对计算机病毒的恐惧心理骤然增加。

计算机病毒防范和信息系统安全是关系国计民生的重大问题。社会是一个整体，局部的问题很容易蔓延造成对整体的影响。只有全社会都重视计算机病毒防范，扎紧篱笆，防微杜渐，才能给我们的社会发展和进步创造良好的运行环境，才能使信息技术充分发挥国民经济发展的助推器的作用。

关于计算机病毒的书籍现在开始多了起来，这说明社会对于计算机病毒的重视程度正在提高。但是，计算机病毒的发展和计算机技术的发展几乎是同步的，因此更需要能及时反映计算机病毒防范技术最新动向和解决方法的实用技术书籍。本书的出版，正是顺应了计算机技术这一发展需要。

本书有几个特点，首先是内容新，许多新近出现的计算机病毒在书中都有比较详细的介绍；其次是实用性强，对计算机病毒防治中的许多常见问题都提供了具体的解决方案，凡具有初级计算机知识的读者都能按书中介绍自行解决有关问题；第三是提供了包括主要网站在内的比较广泛的信息来源，为读者今后及时了解计算机病毒的发展动向以及防治措施提供了方便。

希望本书的出版能有助于读者了解计算机病毒的发展动

态，提高防范计算机病毒的认识，加强计算机病毒防范的力度，提高抵御计算机病毒危害的能力。这也是作者的一个心愿。

上海市计算机病毒防范工作专家组组长
同济大学校长

吴启迪

2001．9．

内 容 提 要

计算机已越来越成为人们工作和生活中不可缺少的重要部分，毫无疑问，它为人类的发展作出了重要的贡献，但计算机病毒却给我们带来了很多烦恼。目前，计算机病毒正以每月数百种的惊人速度增长，每年总有一些新的计算机病毒在全球范围内大面积发作，造成的直接损失往往高达数千亿美元。本书以问答的形式，列举了大量病毒防范的经验体会和方法，以及针对各种常见病毒的具体防范和杀毒方案，解决了防治病毒的实际问题，使读者可以方便地直接加以引用，显著地提高病毒防治工作的效率。

本书内容丰富，通俗易懂，具有较强的针对性，适合广大电脑用户学习参考，以轻松解决病毒防治过程中的问题。

目　录

第一章 病毒基础知识

【问 1】 什么是计算机病毒？

【答】 “计算机病毒”到底是什么东西呢？是否会像其他生物病毒一样，如“感冒病毒”，对人体造成伤害呢？

“计算机病毒”与生物学上的“病毒”不同，它不是天然存在的，而是某些人利用计算机软、硬件的脆弱性，编制的具有特殊功能的程序。由于它具有与生物学“病毒”类似的传染性和破坏性而得名为“计算机病毒”。

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》，其中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”。此定义具有法律权威性。

计算机病毒一般通过磁盘、光盘、计算机网络等途径传播。当它执行时，可以根据计算机病毒编制者的动机，导致不同的影响：其中包括输出一段文字音响信息、占据磁盘空间、甚至删除文档、改变存储数据内容等，导致被感染的计算机部分或完全丧失正常工作的能力，速度降低，功能失常，直至死机。

随着因特网技术的发展，计算机病毒的含义也在逐步发生着变化，从广义的角度而言，与计算机病毒的特征和危害有类似之处的“黑客程序”、“特洛伊木马”和“蠕虫”，也可归为计算机病毒。

可见，正常的计算机程序一般是不会将自身的指令代码强行连接到其他程序之中的，是否具有传染性和危害性是判别计算机病毒的最重要依据。计算机病毒具有自我复制和传染机

制，能迅速地在一台或一组计算机，甚至全球网络之间传播、扩散，给广大计算机用户带来很大的影响。

【问 2】 最早发现计算机病毒是在什么时候？

【答】最初对计算机病毒理论的构思可追溯到 20 世纪 70 年代，美国作家雷恩出版的《P1 的青春》一书中描绘了一种能够自我复制，利用通信进行传播的计算机程序。

80 年代起，IBM 公司的 PC 系列微机因为性能优良、价格便宜等优点，逐渐成为世界微型计算机市场上的主要机型。但是由于 IBM PC 系列微型计算机自身的弱点，尤其是 DOS 操作系统的开放性，给计算机病毒的制造者提供了可乘之机。因此，装有 DOS 操作系统的微型计算机成为病毒攻击的主要对象。

1983 年出现了计算机病毒的研究性报告。

1987 年，世界各地已有一些计算机遭到计算机病毒的突然袭击的报道，但是并未引起人们的重视。

1988 年 3 月 2 日，一种苹果计算机的病毒发作，这天受感染的苹果机全部停止工作，只显示“向所有苹果计算机的使用者宣布和平的信息”，以庆祝苹果机生日。

然而，1988 年 11 月 2 日发生在美国的“莫里斯蠕虫”事件，给计算机技术的发展罩上了一层阴影。它是由美国康乃尔大学研究生莫里斯编写，其危害性完全超出以往出现的任何一种病毒。当时，“蠕虫”在 ARPANET 上迅速蔓延，使得数千台联网计算机停止运行，并造成巨额损失，众多计算机用户甚至专业人员也无从解决。

近年来，新的计算机病毒层出不穷，进入新世纪以后，计算机病毒攻击愈演愈烈，种类已达到 6 万多种。同时，各类黑客程序与蠕虫病毒结合也在因特网上广泛传播。随着我国信息