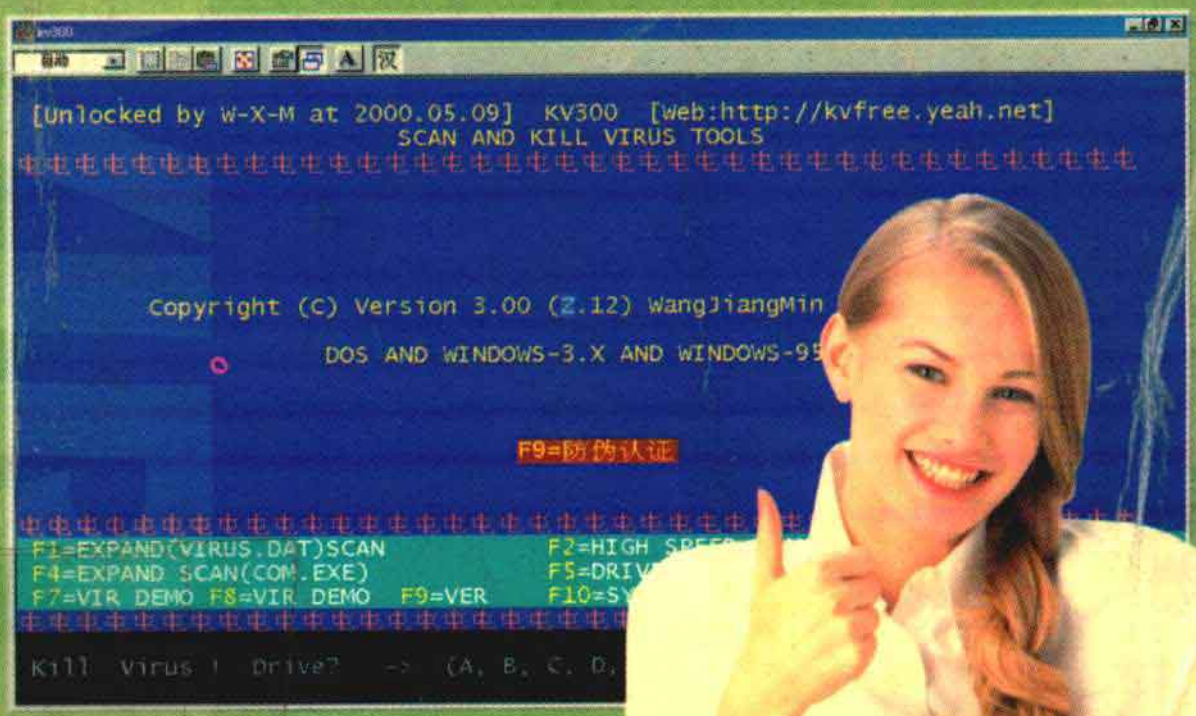
新世纪电脑快易通丛书

金桥电脑工作室

查杀病毒有绝招



科学技术文献出版社

★新世纪电脑快易

查杀病毒有绝招

金桥 袁韵锋 编著

科学技术文献出版社

图书在版编目(CIP)数据

新世纪电脑快易通丛书.3. 查杀病毒有绝招/金桥电脑工作室编.-北京:科学技术文献出版社,2001.11

ISBN 7-5023-3565-X

Ⅰ电... Ⅱ.金... Ⅲ.(1)电子计算机-基本知识 Ⅳ.TP3

中国版本图书馆 CIP 数据核字(2000)第 24747 号

新世纪电脑快易通丛书
查杀病毒有绝招

*

金桥 史武军 编著

责任编辑：敬宇

*

科学技术文献出版社出版

全国新华书店经销

重庆大学建大印刷厂印刷

*

开本 787×1092 1/64 印张 8 字数 200 千字

2001 年 11 月第 1 版 2001 年 11 月第 1 次印刷

印数：0001－5000 册

*

ISBN 7-5023-3565-X/TP.3

全套定价：60.00 元（本册定价：10.00 元）

序

以信息科技为代表的现代科学技术的不断发展和产业化，正在对各国综合国力的提高与竞争产生深刻的影响。当今计算机技术的迅猛发展，为我国通过科学技术突破实现跨越式发展提供了机遇。

放眼当今世界，计算机科学发展日新月异，各种新的硬件、软件层出不穷，令人目不暇接；各种不同档次、不同型号、不同品牌的计算机相继推出，纷纷面世。可以这么说，学习和使用计算机，已经成为人们进入现代信息社会的通行证；一个国家计算机知识的普及和推广程度已经成为衡量该国科技发展水平及综合国力的一个重要标准。本人有幸参加了中国科协第六次全国代表大会，江泽民总书记在开幕式上的讲话中指出：要在广大干部和群众中大力普及科学知识，用科学战胜迷信愚昧，在全社会形成爱科学、学科学、用科学的良好风尚。这表明了党和国家领导人对科普工作的高度重视。

我国加入“WTO”在即，一体化经济时代正在到来，而计算机知识的普及与计算机水平的提高，有利于我国跟上发达国家的科技发展步伐。金桥顺源公司以“普及科技知识、促进科技进步”为己任，充分发挥科协人才荟萃的优势，组织了一大批专家、学者，陆续编著“步步高”、“快易通”等系列电脑普及读物。这有利于国家，有利于社会。作为一名从事多年技术工作的老科技工作者，我由衷感到高兴，并欣然为之作序。

中国工程院院士

2001 年 11 月 8 日

前　言

近年来，随着计算机技术，特别是网络的高速发展，计算机应用已深入到人类的各个行业、各个领域，甚至千家万户。信息化社会、网络时代已离我们不远了。的确，这给我们带来不少的便利和效率。但是越来越多的病毒给我们带来的损失也是难以估量的。为使广大电脑用户能够更多地认识计算机、了解病毒原理、懂得计算机病毒的防范，尤其是在病毒尚未发作和破坏之前及时地发现并彻底杀除它们，谨将此书献给广大读者朋友。

本书针对近年来较为常见的病毒，阐述了病毒的危害性、剖析了病毒传染的机制、描述了一些病毒的发作现象、并且还介绍了一些常见的杀毒软件。

由于编者水平有限，书中疏漏之处，敬请读者批评。

编者

第 1 章　计算机病毒概述

众所周知，计算机病毒是对网络安全最具有威胁的因素之一。和医学上的病毒一样，计算机病毒是通过将其自身附着在健康程序(类似于医学上的健康细胞)上进行传播的，将其代码插入该程序。计算机执行该程序以前，总是首先执行病毒程序。感染上一个系统后，计算机病毒就附着在它所寄居的系统的每个可执行文件、目标文件上，并感染它们。更有甚者，有些病毒还会感染磁盘驱动器的引导区。

第 1 节　什么是计算机病毒

计算机病毒是一个程序，一段可执行码。就像生物病毒一样，计算机病毒有独特的复制能力。计算机病毒可以很快地蔓延，又常常难以根除。

它们能把自身附着在各种类型的文件上。当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。

除复制能力外，某些计算机病毒还有其它一些共同特性：一个被污染的程序能够传送病毒载体。当您看到病毒载体似乎仅仅表现在文字和图像上时，它们可能已经毁坏了文件、再格式化了您的硬盘或引发了其它类型的灾害。若是病毒并不寄生于一个污染程序，它仍然能通过占据存贮空间给您带来麻烦，并降低您的计算机的全部性能。

可以从不同角度给出计算机病毒的定义：

一种定义是通过磁盘、磁带和网络等作为媒介传播扩散，能“传染”其他程序的程序。

另一种是能够实现自身复制且借助一定的载体存在的具有潜伏性、传染性和破坏性的程序。

还有的定义是一种人为制造的程序，它通过不同的途径潜伏或寄生在存储媒体(如磁盘、内存)或程序里。当某种条件或时机成熟时，它会自身复制并传播，使计算机的资源受到不同程序的破坏等等。

而第二种说法在某种意义上借用了生物学病毒的概念。计算机病毒同生物病毒的相似之处是能够侵入计算机系统和网络里，危害正常工作的“病原体”。它能够对计算机系统进行各种破坏，同时能够自我复制，具有传染性。所以，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。

与生物病毒不同的是，几乎所有的计算机病毒都是人为地故意制造出来的。有时一旦扩散出来后连编者自己也无法控制。它已经不是一个简单的纯计算机学术问题，而是一个严重的社会问题了。

几年前，大多数类型的病毒主要是通过软盘传播。但是，因特网引入了新的病毒传送方式。随着现在电子邮件被用作一个重要的企业通信工具，病毒就比以往任何时候都要扩展得快。附着在电子邮件信息中的病毒，仅仅在几分钟内就可以侵染整个企业，让公司每年在生产损失和清除病毒开销上花费数百万美元。