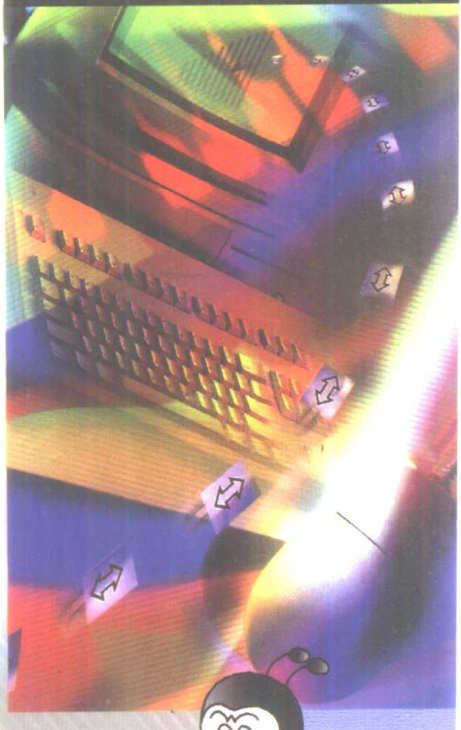
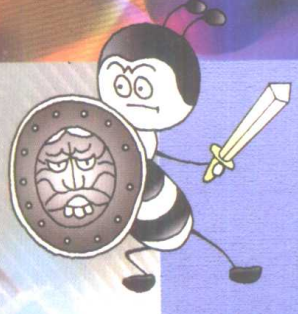
病毒与数据安全

●沈国土　编

家庭电脑工程师

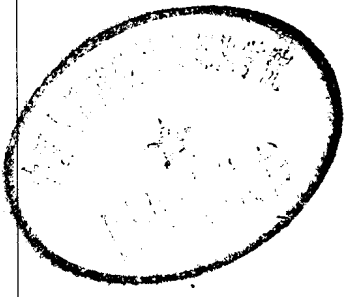




上海科学技术出版社

家庭电脑工程师

病毒与数据安全



沈国土

编

上海科学技术出版社

内容提要

本书是《家庭电脑工程师》丛书的一种。在介绍计算机工作原理的基础上，着重阐述病毒的一般原理，讲解各种主要类型病毒的工作机制、传播途径与传播方式，为读者提供现实可行的防范措施和各种技巧以提高个人电脑的“免疫力”。最后，还详细介绍了如何在病毒的攻击下挽救用户宝贵的数据。

本书摒弃了传统的单纯讲解方式，而是以大量实践操作为基础，并配上详实的图片，让读者边学边做，自己动手解决遇到的实际问题。适合具备初步计算机知识的广大爱好者。

家庭电脑工程师

病毒与数据安全

沈国土　编

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）

新华书店上海发行所经销　上海新华印刷厂印刷

开本 787×1092　1/32　印张 3.5　字数 75 000

2000年10月1版　2000年10月第1次印刷

印数 1－5 000

ISBN 7－5323－5599－3/TP·148

定价：7.00元

出版前言

随着电脑进入家庭和互联网向社会各个角落的延伸，人类社会正在步入网络时代。面对这场涉及社会生活各个领域的进步与变革，没有人能置身其外而安之若素。个人电脑作为网络时代的基本用具，如同电器是电气时代的基本用具一样，只有了解它、驾驭它，才能在社会生活中如鱼得水，充分地享受科技进步给学习、工作、生活带来的便利。

电脑这个东西，在入门之前看上去似乎很神秘，入门之后就会觉得它虽然奥妙无穷，其实并不神秘。人们在初尝入门的喜悦之后，为电脑的无穷魅力所吸引，又会产生进一步了解它、掌握它的愿望。为了满足初入门的电脑爱好者的这种需要，我们组织有实践经验的专业电脑工作者编写了这套业余级的实用小册子。

这套小册子是为喜欢自己动手的业余电脑爱好者编写的。它针对自己动手之中必然会遇到的实际问题，分成若干专题，如个人电脑硬件的组装、软件系统的安装与维护、电脑病毒的防范、网络应用，以及多媒体应用等，一个专题一册地进行介绍。每个专题的介绍均有虚有实、以实为主。我们希望它能成为初级电脑爱好者在电脑和网络世界遨游的一套必备手册。在入门的基础上，带着自己遇到的实际问题，阅读这套小册子，边学边做，不单能够解决实践中的疑难，逐步提高也是指日可待的事情。我们希望刚入门的电脑爱好者，以阅读这套手册为起点，通过家庭的电脑操作实践，增长才干，个个都能成为业余电脑工程师。正是基于这样的良好愿望，我们把这套小册子称为《家庭电脑工程师》。

目　录

病毒与数据安全

第1章 计算机病毒概述

- 计算机病毒
- 病毒的起源
- 病毒的特征
- 病毒的表现

1.1 计算机病毒

几年前，笔者去教计算机初级课，课间有位学员说其计算机不能进入WPS(word process system)系统，重新启动计算机仍然如此。当时我说这台计算机可能感染了病毒。那个学员马上从座位上跳起来，说："病毒不会传染到我身上来吧！"其他学员都笑起来了。现在大概很少有这种情形了，但是计算机病毒到底是什么呢？

在给病毒下定义之前，首先需要说明一下计算机程序的概念。大家知道，在日常生活中每做一件事情都有一定的步骤，比如说打电话，就有以下几个步骤：拎起话筒；听到拨号音开始拨号；当拨通后对方拿起话筒说一声"喂"时，开始讲话；通话结束后挂上话筒。打电话这个过程就有点类似于计算机硬件运行一个程序完成一项任务的过程。

一般情况下，程序都是预先编制好的，然后由执行者——CPU（central processing unit，中央处理单元）来执行。在打电话的例子中，人脑中已经有了打电话的流程，然后指挥手、耳朵、口去执行。在计算机硬件执行程序时，CPU根据这个程序去指挥计算机中的其他硬件完成任务。

归纳起来说，程序就是人们预先设计好的，让计算机硬

件完成一定功能的指令的组合。要注意的是，计算机硬件只是一个执行者，做什么事情、如何做，都需要人来预先设计好指令。当然这些指令计算机硬件要听得懂，否则不管你怎样“喊破嗓子”，硬件都不会理睬你。这就像你用英语指挥一个不懂英语的人一样，白费劲!

从上面的解释已经知道，硬件是由一种它能够理解的程序（或者指令）所控制，这种程序是由人预先编制好的。其实这些程序就是些计算机软件。当然，程序可以让计算机硬件为人服务，也可以让计算机硬件完成些人们不愿看到的事情，比如破坏计算机系统等。其实，计算机病毒就是这样一种某些心怀叵测的人编制的、破坏其他用户计算机系统的程序。

当然，这个程序除了破坏其他用户的计算机系统这个功能以外，还有一些其他的辅助功能，比如说它能在计算机系统内部自我复制等。这里需要说明的是，由于计算机病毒是一种特殊的计算机程序，所以只能破坏计算机系统本身，而肯定是不会传染给人的。只是由于计算机病毒具有与生物学病毒相类似的特征（潜伏性、传染性、发作期），所以人们借用了生物学上病毒的名字来称呼它。

确切地说，计算机病毒就是那些能够在计算机系统内部反复自我繁殖，危及计算机系统正常工作，浪费系统资源，破坏存储数据的一种特殊的计算机程序。

计算机病毒的定义有广义和狭义两种。前面提到的就是计算机病毒狭义上的定义。就广义而言，计算机病毒是指凡驻留于计算机系统内部（指掌握着系统的控制权），对系统原有功能进行非正确或用户未预计修改的程序。常见的广义上的计算机病毒有逻辑炸弹、特洛伊木马等。

1.2 病毒的起源

一般认为，计算机病毒的发源地是美国。早在1960年代初期，美国电报电话公司贝尔研究所里的一群年轻研究人员常常做完工作后留在实验室里饶有兴趣地玩一种他们自己创造的计算机游戏，这种被称为“达尔文”的游戏很刺激。它的玩法是，由每个人编一段小程序，输入到计算机中运行，相互展开攻击并设法毁灭他人。这种程序就是计算机病毒的雏形，然而当时人们并没有意识到这一点。

计算机界真正认识到计算机病毒的存在，是在1983年。在这一年11月3日召开的计算机安全学术讨论会上，美国计算机安全专家科恩（Frederick Cohen）博士首次提出了计算机病毒的概念，随后获准进行试验演示。当天，专家们首先在运行Unix操作系统的VAX 11/750计算机上进行实验，并成功地验证了第一个计算机病毒。一周后，又演示了另外五个病毒，由此证实了计算机病毒的存在，并证明计算机病毒可以在短时间内实现对计算机系统的破坏，且可以迅速向外传播。

计算机病毒的广泛传播始于1987年，计算机病毒的问题从1988年开始才受到人们的重视。

1.3 病毒的特征

计算机病毒与生物学中的病毒一样，具有潜伏性、传染性、破坏性和多样性等特征。

1.3.1 潜伏性

病毒感染计算机之后并不是马上就破坏计算机系统的，而是要潜伏一段时间，这就是病毒的潜伏性。从病毒感染某计算机系统开始到该病毒发作为止的这段时间，就是病毒的潜伏期。

计算机病毒发作一般是有条件的(指病毒已经获得系统控制权后还需要一定的条件)，其中最典型的就是以时间作为发作条件。比如，早期的耶路撒冷病毒，就是每逢星期五和每月13日发作，发作时破坏用户的数据，降低系统运行的速度。又如，最近一段时间闹得沸沸扬扬的CIH病毒，它就是在每月26日发作，发作时对硬盘做格式化。这两个病毒都是以满足时间条件才发作的。当然还有其他发作条件的，比如按下某一个键、组合键或者键序列等。

与生物学上的病毒潜伏在人体内，等人体的抵抗力下降时才发作和致病不同，计算机病毒并不是在计算机的抵抗力下降时才发作的，而是满足一定条件后就发作。病毒这种潜伏性，也叫做病毒的隐蔽性。

正是病毒的这个特性更增加了病毒的危害性。据媒体报道，1999年4月26日CIH病毒大爆发，国内有36万台之多的计算机遭到破坏，也许实际的数字还要大。这是因为病毒

可能在此之前早已感染了计算机，但是由于不满足发作条件，因而很多用户并未意识到，到了26日满足了病毒发作的条件，于是就有如此众多的计算机遭到了破坏。假如病毒一感染就马上发作的话，也许26日以前病毒发作的事例会引起其他用户的警觉，在26日也就可能不会遭到如此大的损失。另据国外媒体报道，美国和西欧的损失相应就小一些，因为他们在26日前做了一些预防工作，如用可以杀灭CIH病毒的杀毒软件在26日前对计算机进行全面的清理，在CIH病毒发作之前把它杀死——从计算机系统中清除了。

1.3.2 传染性

生物学上的病毒会通过各种途径进行传播，计算机病毒也一样，也能通过各种途径在计算机之间传播。

1988年11月2日晚，ARPA网(advanced research projects agency net, ARPAnet)上的所有正在运行的计算机突然停止了正常工作，屏幕显示一片混乱，这个连接全美约三百所大学、公司、研究中心、军事基地的网络系统及与之相连的全国军用、民用及其他计算机网络都同时出现了类似的故障，整个网络瘫痪近二十四小时。另据不完全统计，1988年—1990年之间，我国近40万台微型计算机中约有11%以上受到病毒不同程度的侵入和破坏。从上面两个例子可以看出，计算机病毒具有很强的传染性，可以说是无孔不入，到处渗透。对计算机用户而言，如果能够掌握病毒的传染途径，就能为预防病毒的传染提供了一定的帮助，这也正是本书的主旨之一。

1.3.3 破坏性

简言之，病毒感染计算机后，经过一定的潜伏期，在满足病毒发作的特定条件下病毒做出破坏用户计算机系统的行为，就是病毒的破坏性。

病毒的目的，就是要让他人的计算机系统不能正常工作。绝大部分病毒发作时都会对计算机系统造成破坏，比如前述的例子中破坏应用程序使用户无法正常进入WPS系统，CIH病毒对硬盘进行格式化破坏用户数据和应用程序等。当然，病毒的破坏性有大有小，所以也常根据其破坏力的大小把病毒分成破坏性不大的一般病毒和破坏性极大的恶性病毒。

在上文提到的ARPAnet被病毒破坏的例子，也充分体现了病毒具有很大的破坏性。世界上每年由于计算机病毒所造成的直接经济损失已是数以亿美元计。

另外需要说明的是，病毒的发作和传染有一定的区别，也有一定的联系。大部分病毒一旦获得控制权就会传染，而发作则要满足另外的条件。比如，CIH病毒若不在26日就获得系统控制权，则它就感染文件，当26日来临时，就开始对硬盘进行格式化等破坏性活动。当然也有一部分病毒在传染过程就对计算机系统进行了破坏。比如，大麻病毒感染计算机系统时占用磁盘中的一些重要区域，从而破坏磁盘中的数据。

除了病毒获得控制权后故意传染以外，有时候人们也会在有意无意之中促成病毒的传播，甚至成为传播病毒的“工具”或者“通道”。比如当你把一个感染了病毒的程序拷贝到一台没有感染该病毒的计算机中，一旦在这台计算机上运行这个程序就会使该计算机感染这种病毒。在病毒发展的早期，这往往是计算机之间传播病毒的一种主要途径。现在随

着计算机网络的兴起，病毒传播的途径也越来越多。

1.3.4 多样性

计算机病毒的多样性表现在两个层面上。第一层面是指病毒有很多种。据不完全统计，目前世界上已经有近万种计算机病毒，几乎每天都要产生新的病毒，威胁着计算机系统和数据的安全。

第二层面是指某些病毒有很多变种，使人防不胜防。现在至少已经发现了CIH病毒的四个变种，据说该病毒的编制者已经公开了CIH病毒的源代码，这样一来将会有更多的CIH病毒的变种出现。在DOS系统中很有特色的DIRⅡ病毒也至少有三种危害比较大的变种。这正像感冒病毒一样，具有多种变种，因此使得很多感冒药使用周期很短，迫使人类加快感冒药的研制。

1.4 病毒的表现

计算机病毒感染和发作时，会使计算机表现出许多异常的现象。一般情况下，计算机有它自己的正常运行规律，如果发现计算机运行不正常，则可能是感染了病毒。异常现象可分成显示不正常，运行速度不正常，操作不正常等，下面分别举例说明。

（1）显示不正常

小球病毒发作时，若是在西文状态，其症状是用户的显

示屏上出现一个小圆点，这个圆点不停地作无规则运动，当圆点运动到屏幕边缘或者遇到英文字母时会反弹回来；若在汉字方式下，则当圆点遇到汉字时，消除半个汉字，从而使整个屏幕显示的内容面目全非，极不正常。

大麻病毒发作时，首先判断此时是否为表现时间。如果是，就在屏幕的左上角显示一串字符“Your PC is now stoned!”。

有一种称为泡沫男孩（bubble boy）的病毒，它发作时电脑屏幕上出现黑底白字：“泡沫男孩事件，有图有声”。

如果用户在7月1日至31日期间使用Word编辑感染了“七月杀手”宏病毒，则病毒会弹出一个标题为“醒世恒言”的简体汉字对话框。病毒逼迫用户选择“确定”按钮表示与其一致的观点，否则，如果用户选择三次“取消”按钮的话，后果将十分严重：病毒主动启动计算机，并会把C盘中所有文件删除。

（2）运行速度不正常

病毒发作时往往会降低系统的运行速度，这时用户往往觉得突然之间计算机运行得很慢，比如启动一个应用程序需要很长的时间。前面提到的耶路撒冷病毒发作时就会使计算机运行速度减慢。

（3）操作不正常

有时，当用户从软盘中读取数据时，计算机却告诉用户软盘设置了写保护。本来计算机只要从用户的软盘中读取信息就可以了，所以写保护设置与否是不重要的。这种情况说明，计算机要往软盘里写入数据，这很可能就是病毒在作怪，要将自身写到软盘里去。

在Windows 95下，CIH病毒发作时产生不正常的硬盘操作（其实在破坏硬盘）情况，有非正常的程序运行出错、死机等，甚至重新开机硬盘无法启动等情况。

有一种恶性病毒称为“小贼婆”(MiniZip)。当用户给感染了该病毒的计算机发一个电子邮件，则很快就会收到“收件人”的回复邮件。其内容为：“我已收到了你的邮件，将尽快给你答复，在此之前，请先看一下附带的压缩文件。”附件是名为zipped-files.exe的文件。打开附件，您的计算机便被“小贼婆”病毒感染，其他人再向您发电子邮件时，病毒会自动替您回复来信并继续传播病毒。“小贼婆”病毒的发作不受时间的限制，每次启动Windows病毒都会发作。病毒发作时将删除硬盘上的所有Office文件（如后缀为doc、xls、ppt等的文件）和部分源程序（如后缀为c、cpp、h、asm等的文件），这种病毒破坏后数据将不可被恢复。

病毒发作时会表现出很多现象，其中不少是很不正常的现象，这里就不一一列举了。用户可以根据这些不正常的现象怀疑计算机感染了病毒，并及时采取补救措施。

病毒与数据安全

第2章 计算机工作原理

- 计算机系统组成和功能
- 软件系统的实现
- 数据组织方式
- 解读硬盘奥秘
- 内存管理简介
- CMOS数据初探
- DOS启动流程
- Windows 9x启动流程