实用电脑丛书

电脑病毒防治

diannaobingdufangzhi

陈知生　主编

人民邮电出版社

实用电脑丛书

电脑病毒防治

陈知生　主编

人民邮电出版社

内 容 提 要

本书是“实用电脑丛书”之一，介绍了电脑病毒的特征、共性、来源、产生的背景、传染途径、发生条件、基本工作过程、检测与诊断、病毒的清除、病毒的防护和常用抗病毒软件使用方法及一些常见病毒的具体特征。

该书内容简洁，有很多独到之处，是一本有趣的读物，适合所有正在使用电脑的读者阅读。

实用电脑丛书

电脑病毒防治

陈知生　主编

责任编辑　赵桂珍

*

人民邮电出版社出版发行

北京朝内南小街南竹杆胡同 111 号

北京朝阳区展望印刷厂印刷

新华书店总店科技发行所经销

*

开本：787×1092　1/32　1995 年 6 月第 一 版

印张：5.25　1996 年 2 月北京第 2 次印刷

字数：114 千字　印数：10 101—21 100 册

ISBN7-115-05657-9/TP・191

定价：6.00 元

实 用 电 脑 丛 书

编 委 会

丛书前言

随着计算机技术的不断发展，“电脑热”已经在全国兴起。电脑这个信息时代的宠儿，已经成为现代家庭的一个“新大件”，各行各业各个层次的人们以空前的热情来学习电脑知识。为了满足广大电脑读者的各种需要，我们特编写了“实用电脑丛书”奉献给大家。

本丛书从实用的角度出发，从最基础的知识入门，以电脑初学者为读者对象，引导读者进入电脑时代的新天地，并为进一步学习电脑打下基础。本丛书各册的内容既紧密相联，又具有相对独立性，为读者买电脑、学电脑、用电脑、“玩”电脑、维护电脑提供方便。

本“丛书”共10册。想学电脑的读者，可以先学习《电脑应用入门》，此书通过丰富的实例，不同的入门方法为您打开电脑神秘的大门；准备购买电脑的读者，可以看看《电脑导购指南》，它解决了电脑配置和购机中各种疑难问题；希望或正在学习打字技术的读者，可以学习《汉字输入方法》，它为您提供了现实生活中最流行、较有发展前途的多种汉字输入方法；《电脑编程基础》则以 Quick BASIC 语言为主线，向读者介绍了一种快速学习电脑编程的方法；《FoxPro 实用入门》可以让您掌握 FoxPro 的一些基本知识和常规操作；《电脑绘画排版》和《电脑娱乐世界》主要讲解如何使用排版和绘画软件以及用电脑进行娱乐的方法和知识；《电脑实用技巧》通过大量

实例，介绍使用 DOS、汉字系统、排版软件等方面的技巧；电脑病毒是当前一个使人“谈虎色变”的问题，《电脑病毒防治》则就病毒的分类、特征、来源、产生的背景、传染途径、方式、过程、条件以及病毒的检测、清除、防护作了较广泛而深入的阐述；《电脑维修实践》介绍了有关电脑各种设备的维护和故障排除方法。

本书由陈知生主编，参加编写的人员有：王海云、李青、王尖、孔红秋、赵一单、刘步、余蓉、罗大庆、任丽珠、王唯一、李云舟、张望兰、刘壁龙、胡筑波、卞德福、许诺民、马驹等同志，由于时间仓促，其疏漏之处请批评指正。

本书在编写过程中，参考了众多的文献资料，在此向原作者表示感谢。

编著者

目　录

第一章 概 述

第一节 什么是电脑病毒

电脑病毒同生物病毒一样，能侵入电脑系统和网络，危害正常工作，同时还能自我复制，具有传染性。那么，到底什么是电脑病毒呢？目前还没有个公认的概念，使用较多的是科恩(Fred Cohen)下的定义，即计算机病毒是一个能够通过修改程序，并把自身的复制品包括在内去“传染”其它程序的程序。

不过，科恩的定义并没有完全揭示出电脑病毒的根本性质。让我们先看一个例子：某银行的职员在电脑中安置了一小段程序，检查他的名字是否还在档案中，如果不在，则破坏系统。后因某种原因，他被公司解雇了，但在他被解雇之后，银行数据立即遭到了破坏。这说明电脑病毒可在你不知不觉中侵入你的电脑系统，并在系统中潜伏起来，经过一段时间满足了一定条件后再发作，进行攻击行动。很显然这属于电脑病毒的一种，因为它具有生物病毒的某些性质，并对电脑资源进行了破坏。

那么，应如何对电脑病毒下一个较确切的定义呢？目前有关电脑病毒的定义很多。一种定义是：通过磁盘、磁带和网络等作为媒介传播扩散，能“传染其它程序的程序”；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，它会自动复制并传播，使电脑的资源受到不同程度的破坏等等。

还有一种定义是：电脑病毒是能通过某种途径潜伏在电脑各种存储媒介中，达到某种条件后即被激活，对电脑资源具有破坏作用的一组程序或指令。

电脑病毒都是人们制造出来的，有时扩散后连编者自己也无法控制。它已非纯学术问题，而成了一个严重的社会问题。

第二节　电脑病毒的分类

可以从不同的角度对电脑病毒加以分类。按表现性质可分为良性病毒和恶性病毒。良性病毒危害性小，恶性病毒可能会毁坏数据文件，或使电脑停止工作。按激活的时间可分为定时病毒和随机病毒。按其入侵方式可分为操作系统型病毒、源码病毒、外壳病毒、入侵病毒等。按其是否有传染性可分为不可传染性和传染性病毒。按传染方式分有磁盘引导区传染病毒、操作系统传染病毒和一般应用程序传染病毒。按病毒攻击的机种分类，有攻击微电脑的、攻击小型机的、攻击工作站的。其中以攻击微电脑的病毒为最多，而且几乎 90%是攻击 IBM PC 机及其兼容机。

总之，电脑病毒的分类方法很多，同一种病毒可以有许多不同的分法。但无论是何种病毒，对电脑及数据的危害都是无法预料的。即使是良性病毒，尽管它不删除数据，但由于大量

占用内存而造成死机，使电脑无法正常工作，也是极为讨厌的事。

第三节　电脑病毒的特征

一、电脑病毒的一般特点

电脑病毒一般具有以下特点：

(1) 破坏性：凡是软件手段能触及到的地方均可能受到电脑病毒的破坏。表现为：占用 CPU 时间和内存空间，造成进程堵塞；对数据或文件进行破坏，干扰屏幕的显示等。

(2) 传染性：传染是电脑病毒的一个重要特性，它通过修改别的程序，把自身的传染体插入进去，从而达到扩散的目的。

(3)潜伏性：病毒入侵后，一般不立即表现出来，需要等一段时间才发作。

(4) 隐蔽性：病毒程序大多夹在正常程序之中或者藏在"坏"的磁道中，很难被发现。

第二代电脑病毒甚至连一些基本的特征都消失了，唯一的办法是观察文件长度的变化。然而，更新的病毒也可以在这个问题上蒙蔽用户。它们利用文件中的空隙来存放自己，使文件长度没有变化。许多的新病毒则采用变形来逃避检查，成为第二代电脑病毒的基本特征。

二、电脑病毒活动的共性

电脑病毒虽然种类繁多，但不管哪种病毒，在其活动时都

具有一些共同的特征：

(1) 寄生在正常的程序中。寄生的方法一种是替代，例如圆点病毒用有毒引导扇区替代正常引导扇区的内容；一种是链接，病毒程序链接在文件首部或文件尾部以及文件的中间。

(2) 驻留内存。任何一种病毒都是通过驻留内存进行传染的。这是它传染的前提条件。

(3) 修改中断程序的入口地址(也叫系统的中断向量)。

三、不同病毒的表现形式不同

许多病毒，尤其是早先的病毒，一般都有某种特殊画面、问候语、特殊字符串。如小球病毒有个小球，火炬病毒有燃烧的火炬，星期日病毒有问候语："今天是星期日，何必这么辛苦呢?"等等。但另外一些病毒，尤其是新一代的病毒，其表现特征有了极大的变化，变得更隐蔽，令人难以捉摸。像 dir－2 病毒，它可以掩盖它修改了文件长度这一事实。因此，在对系统进行病毒检查时，必须注意这些特点，不能让表面现象所掩盖，以免让它蒙混过关。

第二章　电脑病毒的来源

第一节　电脑病毒产生的背景

一、制造电脑病毒是新的犯罪行为

制造电脑病毒是高技术犯罪，具有瞬时性、动态性和随机性，不易取证，风险小而破坏大，是某些人恶作剧和报复心态在电脑应用领域的表现。但作为政治目的、军事目的的例子也不是没有。

例如像圆点一类的良性病毒，就是电脑爱好者的恶作剧。1987 年出现在以色列耶路撒冷西伯莱大学的犹太人病毒，则是雇员在工作中受挫或被辞退时故意制造的。它针对性强，破坏性大，产生于内部，防不胜防。

二、电脑产品的脆弱性是电脑病毒产生的根本技术原因

电脑的数据在输入、存储、处理、输出时，易被错误输入、丢失和被破坏；程序易被误删除、修改；电脑软件设计者设计程序时不能事先完全确定程序有没有错误，只能在运行中发现、修改，这就造成了电脑产品的脆弱性，为病毒的侵入提供了方便。

三、电脑技术发展的意外结果

随着电脑的能力不断增强，电脑程序、电脑系统日趋复杂，这使得用于研究或某种其它目的而设计的程序，有时会由于某种原因失去控制产生了意想不到的效果，也可视为病毒的一种表现。

四、电脑的普及是电脑病毒产生的必要环境

随着我国电脑的普及，操作系统简单明了，软、硬件透明度不断提高，能够透彻了解其内部结构的人日益增多，对其存在的缺点和易攻击处也了解得越来越清楚，这都是电脑病毒产生的温床。此外，一些软件公司及用户为使自己的软件不被非法复制以保护自己的利益，采取了报复性惩罚措施。因为他们发现对软件上锁不如在其中藏有病毒，这样对非法拷贝的打击会更大。

第二节　电脑病毒的传染途径

电脑病毒容易传染，其传染途径通常有以下几种。

一、软盘

大量的软盘交换，不合法的程序拷贝，不加控制地随便在机器上使用各种软件，如不同渠道来的系统盘、游戏盘等，都容易使电脑感染病毒。其中游戏盘是交换量最大、带病毒最多的软盘。