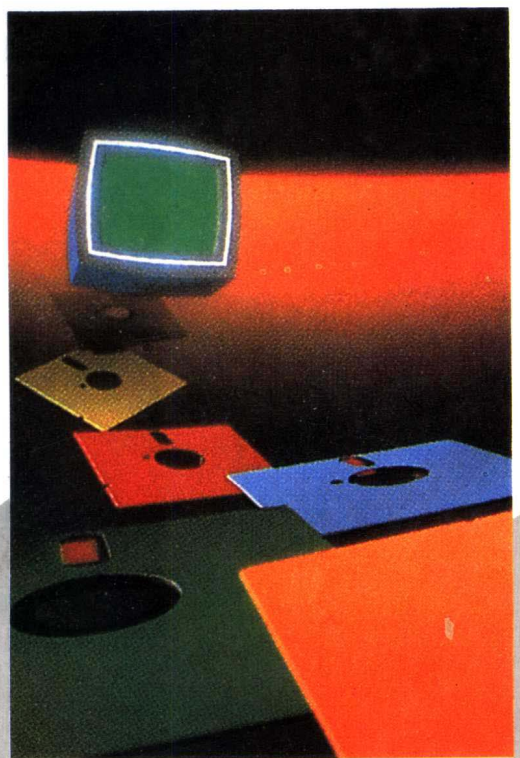
家用电脑
应用丛书

PROTECTION AGAINST COMPUTER VIRUSES

电脑病毒的防治

李大学
张义兰
编　著



复旦大学出版社

家用电脑应用丛书

电脑病毒的防治

李大学　张义兰　编著

复旦大学出版社

电脑病毒的防治

李大学　张义兰　编著

出　版　复旦大学出版社

(上海国权路 579 号　邮政编码　200433)

发　行　新华书店上海发行所

印　刷　上海第二教育学院印刷厂

开　本　787×1092

印　张　17

字　数　413 000

版　次　1996 年 4 月第 1 版　1996 年 4 月第 1 次印刷

印　数　1—5 000

书　号　ISBN 7-309-01620-3 / T · 137

定　价　19.00 元

内 容 提 要

本书共分八章。第一章为电脑病毒概述，第二章介绍电脑病毒的传染方式，第三章为DOS的基本结构分析，第四、五章介绍诊治病毒的工具软件和预防手段，第六章介绍了反病毒软件，第七章剖析了常见的电脑病毒，提出了检测与消除的办法，第八章列表介绍常见电脑病毒。

本书适合具有一定的电脑基础知识的读者阅读，同时也能作电脑培训教材。

家用电脑应用丛书编委会

序

本世纪40年代发明的电子计算机无疑是人类历史上最伟大的发明之一，从它的诞生到今天，短短不到50年间，它本身经历了从第一代到第五代的巨大变化，更重要的是，它在工业、农业、交通、通信、金融、商业、科研、教育和国防等社会生活的各个方面都已有了广泛的应用，其影响之大、之广是无与伦比的。

当前计算机正与通信、广播电视、信息服务等密切结合，从而将使计算机也要像电视、电话那样逐步进入千家万户，进入寻常百姓家，并将更广泛、更深刻地影响整个社会的政治、经济生活以及人们的工作和生活方式。

为使计算机能尽早进入寻常百姓家，一个很重要的条件是能让尽可能多的人了解计算机，学会使用计算机于自己的工作和生活之中。希望和相信这套《家用电脑应用丛书》能在这方面发挥它的作用。

本套丛书的主编李大学同志长期以来，一直从事微机应用工作，在该领域积累了不少成功的经验，并编写、出版了多部著作，在社会上有一定的影响。其他几位作者也都是对计算机有一定研究的中青年计算机工作者，在微型计算机的操作与应用方面作过大量的工作，这套丛书的出版发行，必定会给电脑应用带来一定的普及与推动。

祝丛书成功，更祝计算机能早日进入寻常百姓家。

吴立德

前　言

电脑，这个本世纪的骄子，自从诞生那天起，就受到了世人的格外宠爱。当人们还没来得及骄傲的时候。它已快速涌向科学计算、实时控制、事务处理等各个应用领域。电脑，从1946年第一台诞生到现在40多年间，体积缩小到万分之一，重量减轻到万分之一，功能与可靠性提高了10000倍，其价格却下降到原来的万分之一，经过40多年的发展与繁衍，电脑家族已是子孙满堂。

最近几年，小巧玲珑、功能齐全、安全可靠、价格便宜的微型电脑又悄悄地走进寻常百姓家，成了人人都爱不释手的宠物。它给人们的工作和学习带来了很大的帮助，也给家庭生活增添了无穷的乐趣。

电脑，它毕竟是高科技的产物，要学会操作、使用和维护它，还是要花点功夫的。目前，爱电脑、买电脑、学电脑、用电脑几乎成了人们日常议论的中心话题。不少人都觉得难以找到一套通俗、实用的教材将自己带进神秘的电脑世界。专业教科书太深奥、太理论化，而随机说明书又太粗浅。为了帮助广大电脑爱好者和用户学习电脑、使用电脑，我们组织编写了这套《家用电脑应用丛书》。

本丛书一套六本，这是其中的一本。本书从实用的角度出发，对电脑病毒的基本概念及其产生、症状、种类、特征、检测、预防和消除技术作了详尽的陈述，同时就常见的反病毒工具、其软件的功能及操作方法也作了介绍。另外，还就常见的几百种病毒以表格的形式作了简要的说明。

在编写过程中，作者集近几年对电脑病毒的研究成果、经验，参考了国内外有关书籍、报刊、杂志上刊载的有关资料，力求为读者提供一本有实用价值的参考书。

本书适合具有中等文化水平，并有一定的电脑基础知识的读者阅读，同时，也可作为电脑培训教材，还可供电脑研制、开发应用人员及中、高等学校计算机专业师生作教学参考书。

作者非常感谢复旦大学计算机科学系吴立德教授、施伯乐教授以及其他几位系领导的关怀与指导，感谢复旦大学出版社领导及为本书出版发行作过工作的同志，没有他们的辛勤工作，本书是无法与读者见面的。同时还要感谢何勇强、郝春吉、白雪峰等同志，他们为作者提供了不少的帮助。

笔者力求奉献给读者一套尽善尽美的学习指南，但限于作者的水平，书中不足之处，恳请读者批评指正。作者随时欢迎来自各方面的指教与建议，以便再版时纠正与完善。

作　者

目　录

第一章　电脑病毒概述

§1.1　引　　言

正当电脑以日新月异的发展速度广泛深入到科学计算、实时控制和事务处理等各个领域的时候，利用电脑犯罪也相继出现，特别是到了电脑飞速发展的80年代，又出现了令人生畏的电脑病毒(Computer Virus)。电脑病毒的出现给政府、法律部门及各级领导和普通电脑研究人员、电脑操作者敲响了警钟：一种利用电脑作为犯罪工具的高技术犯罪正成为日益严重的社会问题。

自电脑病毒进入我国以来，短短几年时间，它以几何级数迅速扩散，很快感染了全国各地的为数不少的电脑。许多人对此感到不理解，更有人感到惊恐不安。不少专家著书撰文介绍了一些病毒的检测、消除及预防病毒的方法，为扼制电脑病毒的泛滥起到了良好的积极的作用。随着电脑进入家庭，电脑用户队伍的日益扩大，更有必要向广大电脑用户提供一份通俗易懂、使用方便、可操作性强的介绍电脑病毒的预防和消除的系统性知识和实用技术，以便在操作电脑时，防止病毒感染；而一旦被感染，又能及时、顺利地排除故障，以最大限度地减少不必要的损失。

本书较详细地介绍了电脑病毒的产生、危害、特点和分类等基本知识，分析了电脑病毒的传染过程、工作原理、预防方法、消除方法以及常用消除工具的使用方法。

§1.2　什么是电脑病毒

电脑病毒是一种特殊的程序。这种特殊的程序本身具有再生能力，它会像生物病毒那样，在电脑系统中繁殖、生存和传播，它会自动地通过修改其他程序并把自己嵌入其他程序中或者将自身复制到存贮介质中，从而"感染"其他程序。在条件满足时，该程序就干扰电脑正常工作，搞乱或破坏电脑系统资源，甚至使整个电脑系统瘫痪，所以人们借用了微生物学中的一个名词，称这种特殊的程序为电脑病毒。

到目前为止，电脑病毒尚没有一个确切的定义。美国电脑安全专家Frederick Cohen博士认为，电脑病毒是"一个能够通过修改程序，把自身的复制品包括在内去传染其他程序的程序"。而B.W.Burnham则认为：电脑病毒是"一种能够使自身的复制品插入(通常以非破坏形式)到某一个接受复制品的程序或宿主程序中的指令序列"。在美国，还有人认为，电脑病毒是"一个能自我繁殖并向无毒的电脑系统扩散的加密性指令集"。在日本，则有人认为，电脑病毒是"一个不断滋长的且危及越来越多的电脑系统工作的程序或指令集"。

以上这些定义概括了电脑病毒的一些特性，但在某些方面仍存在着不足。生物病毒是一种能够侵入人、动物、植物，或其他微生物并给其带来危害的微生物，它没有细胞结构，但有其遗传、复制等生命特性，主要由核酸和蛋白质组成。生物病毒的一般特性有：

(1) 传染性：病毒借助介体或直接接触，进入宿主生物体，受感染的生物体可再次成为

病毒的传染源。

(2) 增殖性:病毒不是独立存在的生物体,它是利用活细胞进行增殖的。

(3) 表现性:病毒的感染能引起人类和其他动物许多疾病,能引起抗物病毒,即表现出某种症状。

(4) 流行性:流行性是传染性的必然结果,它是指在一定的时间内,一种病毒对一定地域内的某类动、植物体的广泛影响。

(5) 专一性:一定种类的病毒感染一定的动、植物体或影响动、植物体的特定组成部位。

(6) 变异性:病毒与其他生物一样,能发生变异。

(7) 抗药性:病毒可以对药物产生一定的抵抗性。

(8) 潜伏性:病毒对动、植物体的感染有一定的潜伏期,即从病毒侵入机体起,直到最初症状出现时止有一段时期。

电脑病毒与生物病毒有相似的特性:

(1) 传染性:传染性是衡量一个程序是否为病毒的首要条件。病毒程序一旦进入电脑,与电脑系统中的程序接在一起,它就会在运行这一被传染的程序之后开始传染其他程序。这样一来,病毒就会很快地传染到整个电脑系统或者扩散到硬盘上面。电脑病毒可以从一台电脑,传染到另一台电脑;从一个程序,传染到另外一个程序;从一个电脑网络,传染到另一个电脑网络上去;或在网络内各个系统上传染。同时使被传染的程序、电脑、电脑网络成为病毒的生存环境及新的传染源。

(2) 增殖性:电脑病毒在传染系统之后,可以利用系统环境进行增殖或称之为自我复制,使自身的数量增多。

(3) 表现性:电脑系统感染病毒之后,被感染的系统在病毒表现及破坏部分被触发时,都呈现出一定的症状,如某个文件被"吃"掉了、某个文件的长度增长了、系统运行速度明显减慢或屏幕显示出异常现象等。

(4) 流行性:一种电脑病毒出现之后,会通过软盘复制传染一类电脑程序、电脑系统和电脑网络,同时会通过电脑网络影响网上各个系统。

(5) 专一性:某些电脑病毒在特定的环境下,只传染某一类的电脑,有的只传染某一类的文件,如大部分电脑病毒只传染扩展名为.EXE 和.COM 文件,有的只传染 COMMAD.COM 文件,并非传染所有电脑的所有程序文件。

(6) 变异性:电脑病毒在发展、传播过程中可以产生变种。这是由于电脑病毒本身是由几部分组成的,例如一般病毒都有安装部分、传染部分和破坏部分等,有些恶作剧者或恶意攻击者对其中某一部分进行模仿或者修改,使之成为几种不同于原病毒的电脑病毒,如小球病毒已有十几个变种。

(7) 抗反病毒软件性:有些病毒程序的制造者针对反病毒软件的特性,将某些病毒修改成反病毒软件对其不起作用的病毒程序。这主要表现在原版病毒程序的变种上。

(8) 潜伏性:一般病毒软件传染电脑系统后,并不是马上发作,而是等待某种条件满足之后,才被激活,呈现出破坏作用。在满足条件之前,病毒可保存在电脑中,没有任何症状,丝毫不影响电脑系统的正常运转。如"黑色星期五"病毒只在适逢 13 号并且是星期五这一所谓"不吉利之日"才被激活;"4 月 1 日"病毒只在每年 4 月 1 日这一天才被激活。一般病

毒的触发是由电脑表现部分和破坏部分的判断条件来决定的。

由上述的特性可以看出，电脑病毒同样具有生物病毒的一些特性，于是人们便借用生物学中“病毒”这一术语，确立了“电脑病毒”一词。尽管电脑病毒和生物病毒的基本特性相似，但它们之间还是存在着根本的区别。电脑病毒是一个特殊的程序，是一组编码集合，所以不能直接引用生物病毒的定义冠于电脑病毒，电脑病毒实际上是一种隐藏在电脑系统的可存取信息资源中，利用系统信息资源进行繁殖并生存，能影响电脑系统运行，并通过系统信息共享的途径进行传染的、可执行的编码集合。

§1.3 电脑病毒的起源和流行

当电脑病毒这种特殊程序以生物病毒的特性在电脑中广泛传染、蔓延，并大量地吞噬用户的程序和数据，使电脑系统受到严重破坏时，电脑用户们产生了相当程度的恐慌。于是，一些电脑专家、电脑用户以及一些本来与电脑无关的人们都开始以不同程度或在不同立场上对电脑病毒的产生进行分析、判断和猜测。众说不一，如科学幻想起源说、恶作剧者起源说、游戏程序起源说和软件俱乐部起源说等等。本书不想参与探讨，只把文献中各种说法罗列于后，供读者参考。

1.3.1 电脑病毒的起源

1988 年 11 月 3 日，美国最大的计算机网络 Internet 受到 Morris 蠕虫程序攻击并造成重大损失以来，各种电脑病毒相继出现，人们经历了一个从不可理解到恐慌到逐步了解并认识的过程。目前，对于电脑病毒，人们已经从技术上逐步地完善了自己的认识，并已有能力对其实施控制和消除，但是，一些非专业电脑用户对电脑病毒的传染过程及造成的严重后果所产生的恐慌感和神秘感仍未消除。人们对电脑病毒的起源产生了种种推测和猜想，归纳起来有以下几种。

1. 科学幻想起源说

不少人认为电脑病毒的发源地在美国。他们认为电脑病毒起源于科学幻想小说。1975 年美国科普作家 Thomas Brunner 出版了一本名为 Shock Wave Rider(《震荡波骑士》)的幻想小说。小说以 Worn 和 Virus(电脑病毒)为主，第一次描述了信息化社会中电脑作为正义和邪恶双方斗争的重要工具的故事，使电脑之间产生了第一次“幻想”中的相互攻击。在此之后，1977 年夏天，美国 Thomas J.Ryan 也出版了一本名为 The Adolescence of P-1(《P-1 的青年》)，在该书中，作者构思出了世界第一个电脑病毒，这种病毒能从一个电脑到另外一个电脑传染流行，能控制 7000 台电脑的操作系统。1983 年，美国的科幻电影 Wan Games 上映，该影片赞美了一个孤独的少年通过一台电脑从事军事活动的故事。该影片上映之后，在一定程度上激发了电脑恶作剧者的活动。1984 年，William Gibson 出版了小说 Neuromaner，该书中第一次提出了电脑流氓(Cyberpunk)的概念，这一概念与 Fred Cohen 对电脑病毒的定义非常惊人的相似。从此，科学幻想中的电脑病毒在作家的笔下和电脑的现实世界里得到了充分的发挥和实现。有人认为，这些科幻作品是诱导和启发某些人从事电脑病毒制作的起因。

2. 恶作剧者起源说

有资料表明，电脑病毒起源于搞恶作剧的人。这些人对电脑的存取信息具有浓厚的兴

趣，他们认为自己对电脑无所不能，为了显示一下自己在电脑方面的天资，或要报复一下别人，设计并编写出具有自我复制能力的“活的”程序——电脑病毒，来达到显示自己的才华的目的，同时，从受损失一方的痛苦中取得乐趣。早在 1984 年，Steven Levy 所著的 Hackers（《恶作剧者》）一书中就已向读者详细介绍了恶作剧者的一切。正如 Levy 所说，“恶作剧者是那些对某种（如电脑）技术感兴趣的人。他们似乎对所有的有关（如电脑）知识和技术均有兴趣，并且特别热衷于那些别人认为是不可能做成的事情，因为他们认为世上没有做不成的事。”目前，尽管电脑病毒的起源问题还没有定论，但可以肯定，世界上流行的许多电脑病毒都是恶作剧者的产物。1988 年 11 月 3 日美国 Internet 网络蠕虫病毒的编写者 Morris（莫里斯）实际上是一个电脑的恶作剧者。在他编写这个旨在渗透到美国国防部的电脑网络的病毒之时，也没有考虑到这种电脑病毒会给美国带来巨大的损失，直到走上法庭，他才对他所制造的这种病毒的具体影响有所了解。

3. 游戏程序起源说

关于电脑病毒起源的另一起说法是，早在 60 年代初期，电脑刚刚在社会上得到应用和逐步普及的时候，美国电报电话公司贝尔研究所的一群年轻的研究人员常常在做完工作后，为了娱乐，在实验室里玩一种叫作“达尔文”的能“吃”掉对方程序的程序，看谁先把对方的程序“吃”光。有人认为这就是电脑病毒的雏形。

说起游戏程序，可以追溯到更远，美国人凯恩所著的《电脑防护》一书中就列举了这样一件事：早在 UNIVAC 1108 机时代，就在该系统上出现了一个称为“ANIMAL”的游戏程序。运行该程序时，向人们提出 20 个问题，请游戏者猜动物，如果游戏者猜对了，系统不做任何工作，否则该程序则把动物复制到每一个文件中去。ANIMAL 还能对复制生成的日期建立一个非法时间，并利用日期来判定文件上的 ANIMAL 程序的备份是否为当前运行的 ANIMAL 版本所建立。可以说这一程序的一些机制和当前所流行的电脑病毒的传染机制有类似之处。

4. 软件俱乐部起源说

美国电脑软件用户俱乐部是一些志同道合的电脑爱好者组成的一个团体。这些电脑爱好者通过这个组织，利用电脑网络分享对电脑开发和研究的心得。也有人在公告版上显示自己发明的程序并注明欢迎大家通过电脑网络来选用。但也有人说明，必须在规定时间内邮寄使用费用。通常这种公告版上的程序“暗藏杀机”。如果有人用了程序不付费的话，在特定的时间内，暗藏在程序中的电脑病毒就像定时炸弹一样开始爆发，藉以警告那些“占小便宜”的使用者。如果不知情的“盗用者”把这种带着“暗藏杀机”的程序分享给其他朋友使用，于是一传十，十传百，这种病毒程序就广泛传染开来。这样，他们自觉不自觉地成了电脑病毒的起源。

5. 美国中学生起源说

随着电脑的普及，尤其是在经济较发达的美国，家庭电脑较普遍，许多年轻的大中学生甚至小学生接触电脑的机会较多，他们对电脑的操作比较熟练，从有关资料中可以看出，病毒的制造者大都是一些十几岁到二十几岁的年轻人。这些被人们认为是电脑“神童”的娃娃们一开始也只是想编写一些程序和伙伴们开个玩笑，一是要显示一下自己的聪明才智，二是要从朋友的电脑资源损失中求得乐趣，然而，不幸的是这种玩笑越开越大，范围越来越广，引起了电脑病毒的广泛传染及蔓延。后来，仿效者越来越多，并且种类日增，最后成了今天电

脑安全领域中的一个大问题。

6. 软件保护起源说

由于电脑软件是一种知识密集的高科技产品，发展到一定程度，人们对于软件资源的保护不尽合理。由于软件产品不能得到适当的法律保护，软件制造商设计、开发的软件产品被大量地非法复制，其利益受到损失，为了防止自己开发的软件被非法复制，他们在自己的软件系统中加入惩罚非法复制软件者、可以传染的并具有一定破坏作用的电脑程序。这种电脑程序逐步演化成了危及社会的电脑病毒。

7. 病毒实验起源说

电脑病毒的罪魁祸首到底是谁，众说纷纭。也有人认为美国电脑专家 Fred Cohen 是第一例电脑病毒的制造者。1983 年，美国加利福尼亚的电脑研究人员 Fred Cohen 博士开始研究电脑病毒对系统攻击的可能性，并于 1984 年在美国电脑安全会议上公开演示电脑病毒。所以有人说，电脑病毒就是从那时广泛蔓延开来的。

1.3.2 电脑病毒的流行

电脑病毒的起源我们一下子很难判定，但它的出现给人类的信息化社会带来极大的灾难，给人类社会的物质财富带来了极大的损失，并严重地影响着电脑的普及应用，甚至影响着电脑技术的高速发展。这就不得不使人们关心电脑病毒传染的范围有多大、这种传染能否得到控制，电脑病毒能否被消除。

应该说人们真正认识到电脑病毒的存在是在 1988 年。1988 年 11 月 3 日，美国的 Internet 网络遭到了电脑病毒的攻击。Internet 网络是使用 Unix 为主要操作系统的网络。该网络受到电脑病毒的攻击，网中的 6200 台 VAX 系列小型机及 SUN 工作站都感染上病毒，损失约 9200 多万美元。那是一种蠕虫病毒，它利用 UNIX 系统中的电子邮件的脆弱性进入 Internet 网络，并在网络中不断自我复制，一夜之间给电脑系统造成了巨大损失。这一事件极大地震惊了 AT&T 公司，从此，整个电脑界掀起了一个谈论电脑病毒的高潮。

据有关资料介绍，制造病毒攻击 Internet 网络的 Morris 是美国政府高级电脑专家的儿子，早在读中学时，他的癖好就转向了电脑。起初，Morris 只是在家里用电脑做作业。但不久以后，他掌握了较复杂的数学计算方法及电脑编程技术，从而开始编写电脑程序。Morris17 岁时到贝尔实验室工作，后来他参加了哈佛大学电脑计划，在学校的计算中心任程序员，之后又进入康奈尔大学，开始了对电脑的系统学习和研究。

Internet 事件之后，仅三年多时间，就出现了数十种电脑病毒。这些病毒以极快的速度传遍了全世界。

微电脑的广泛普及，已经使之成为各类电脑中装机量最多的一种，因此，它也成了电脑病毒的攻击对象。据不完全统计，把 IBM PC 机及其兼容机作为主要攻击对象的病毒达五、六十种之多，常见的有

1536 / Zero Bug;
1701 / Cas Cade;
1704 / Cas Cade / Falling;
1704 / Cas Cade-B;
1704 / FORMAT;
1168 / Datacrime-B;
1280 / Datacrime;
1514 / Datacrime Ⅱ;
2708;
2930;
3551 / Syslock;
405;