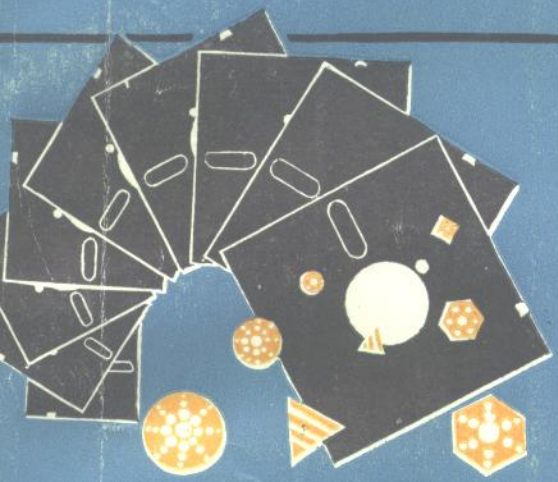
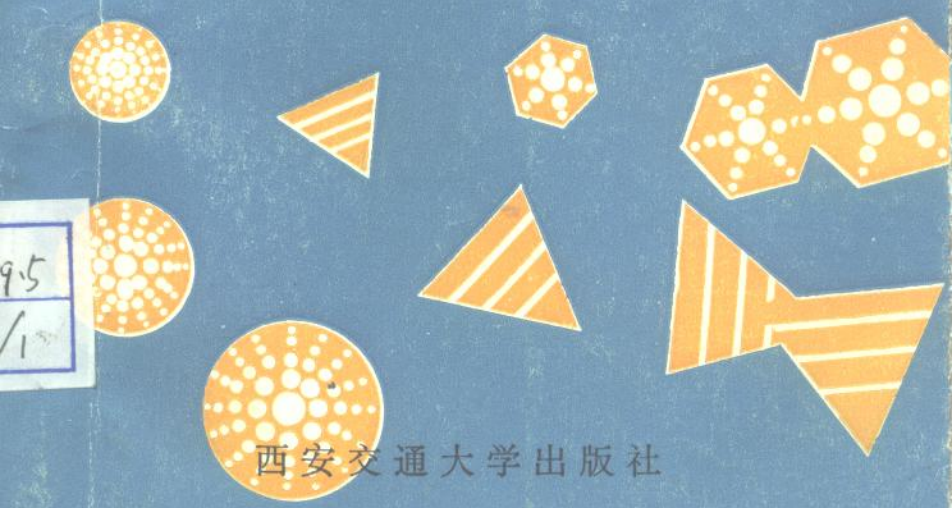
计算机病毒的原理及防治

林宣雄　叶　涛





西安交通大学出版社

计算机病毒的原理及防治

林宣雄　叶　涛

西安交通大学出版社

内 容 简 介

本书全面系统地介绍了计算机病毒的概念、计算机病毒产生的原因，以及它的危害和各种类型病毒的症状和特征，给出了预防和医治计算机病毒的方法。全书共分十章，附录部分介绍了应用软件 DEBUG、PCTOOLS 的功能、使用方法和有关参数。

本书既可作为了解计算机病毒的知识性读物，又可作为防治、研究计算机病毒的手册和工具书，供广大计算机工作者参考。

计算机病毒的原理及防治
林宣雄　叶　涛
责任编辑　赵丽平
*
西安交通大学出版社出版
（西安市咸宁路 28 号）
西安交通大学出版社印刷厂印装
陕西省新华书店发行　各地新华书店经售
*
开本 787×1092　1/32　印张 7.375 字数:159 千字
1990 年 3 月第 1 版　1990 年 6 月第 2 次印刷
印数: 10 001——30050
ISBN 7-5605-0344-6/TP·33　定价:4.20 元

前　言

1977 年夏天，一本科学幻想小说轰动了美国科普界，一时极为畅销，被认为是非常杰出的科幻作品。在这本名为《Adolescence of P-1》的书中，描写了一种可以在计算机之间互相传染的病毒，这种病毒最后控制了几千台计算机，酿成一场灾难……。也许人们因此受到启迪，今天，计算机病毒已从科学幻想变成了现实。

几年来，计算机病毒从无到有繁衍迅速，到处传播危害各国。特别是 1989 年，计算机病毒侵入我国，成为我们不得不面对的现实。计算机病毒究竟是什么东西？它是如何产生、传播和危害计算机的？对于计算机病毒应如何检测、医治和预防？这是广大计算机用户和计算机工作者迫切需要了解和极为关注的问题。为了解答这方面问题和提供这方面的知识，我们综合了一些资料加上自己对计算机病毒的研究结果编写了本书。

本书共分十章，全面系统地介绍了计算机病毒的概念、计算机病毒产生的原因，以及它的危害和各种类型病毒的症状和特征，给出了预防和医治计算机病毒的方法。本书一个特点是不但深入剖析了计算机病毒的原理，而且对典型的病毒程序作了详尽的文字注释，将其所用的手段、技巧和危害计算机的方式彻底公之于众，使之不能继续蒙骗人们。针对计算机病毒是钻了计算机的弱点、不足之处的空子这一特征，书中对计算机的细节、有关参数和各种参数的计算、换算公式作了全面介绍，这些内容一部分散见于一些书刊资料，另一部分则由作者在长期的研究工作中积累、归纳所

得．这部分内容不仅对研究计算机病毒是必不可少的知识，而且对计算机其它方面的研究也是极为难得的参考资料．书中还给出了若干检测、医治计算机病毒的实用程序，这些程序都在 IBMPC／XT，AT，286 及兼容机上通过，可供读者使用和借鉴．本书的附录介绍了在防治研究计算机病毒中最重要的工具 DEBUG、PCTOOLS 应用软件的功能、使用方法和有关参数．本书既可作为了解计算机病毒的知识性读物，又可作为防治、研究计算机病毒的手册和工具书．

本书第一章至第四章和第八章由叶涛编写，其余章节由林宣雄编写．胡正家教授在本书编写过程中曾给予指导，特此表示感谢．特别值得一提的是西安交通大学出版社赵丽平编辑，从本书一开始她就给予了热情的支持和帮助．没有她和出版社其他同志的辛勤工作，本书不可能这么快就与读者见面．特向他们表示崇高的敬意．本书在编写过程中还参考了不少专家、学者的有关论述，在此谨向他们致以谢意．

由于时间仓促，加之我们水平有限，书中难免有许多错误和遗漏之处，竭诚希望广大读者不吝指教．

作　者

1989.12

目　录

第一章　什么是计算机病毒

1-1　美国军事计算机网络遭到袭击

1988年11月2日，落日背着神秘的余晖，沉入西边的天际。夜幕降临后，美国许多大学、研究中心、国防部研究机构、军事基地依然与往常一样繁忙，计算机不断地处理着由大型计算机网络送来的各种数据，专家和科研人员还在紧张地工作和从事各种研究。突然，计算机终端屏幕上出现了一些乱七八糟的符号，随后一切正常运算全部中断，整个东西海岸上、东起麻省理工学院、哈佛大学、马里兰海军研究实验室、马里兰大学，西到加里福尼亚大学的伯克利圣地亚哥分校、以及弗吉尼亚的太空总署研究中心、斯坦福大学国家研究所、甚至兰德公司研究中心，所有计算机都同时出现了故障。正在进行国防、科学技术研究的专家和科技人员，被突如其来的故障搞得莫明其妙，顿时陷入一片混乱之中。与此同时，计算机并没有停止工作，仍在高速地运行，大量自行复制一段不明来历的程序。专家们手忙脚乱地力图排除故障，但是一切努力均为徒劳，只好无可奈何地看着这段"罪恶"的程序通过庞大、高效的计算机网络迅速扩散。这段程序所到之处都毫不客气地自行复制数百次，使得计算机系统不堪重负无法处理其他作业，从而阻塞了数以千计的计算机，使它们无法正常工作，陷入瘫痪。

这个遭到"袭击"的 INTERNET 网是美国一个重要的国防、军事计算机网络，它包括五个计算机中心和十二个地区节点，联接着政府、大学、研究所和拥有政府合同的二万五千多台计算机。在 INTERNET 网中有三个基本网：美国国防部远景规划署的 ARPANET 网(Advanced Research Projects Agency NET)、军方的 MILNET 网和美国国家科学基金会的 NSFNET 网(National Science Foundation NET)。在这个重要的网络中，历来极为重视安全问题，早在 1986 年，MILNET 网就专门组织了从外部对网络攻击的研究，并就研究结果改善了网络的安全系统。这次事件使美国国防部感到震惊，当天夜里国防部成立了一个应急中心，处理这起被称之为"计算机病毒"的袭击案，着手调查并协同全国数千名计算机专家进行网络的"消毒"工作。

到 11 月 3 日下午为止，全美国共有六千多台联网的计算机遭到"病毒"侵害，造成了整个网络瘫痪二十四小时的后果。经过日夜奋战，直到 11 月 4 日，美国国防部才宣布消除了"病毒"，受感染的计算机网络恢复正常。

据统计，这次病毒侵害造成的直接经济损失达九千六百万美元，对各大研究中心和网络用户研究工作的影响则难以用美元来估算。由于 ARPANET 网与国际上其它网相联，因此这次事件还波及了国外一些研究机构。美国计算机专家普遍认为，这是美国计算机有史以来所遭受最严重、规模最大的侵犯。

1-2 计算机病毒的概念

病毒本来是生物学领域的术语，是指能够使有生命的人

或动植物致病的微生物。病毒怎么会与计算机联系起来呢？原来，所谓的"计算机病毒"是指进入计算机数据处理系统的某些错误信息，它们能够在计算机内部反复地自我繁殖和扩散，危及计算机系统的正常工作，造成种种不良后果，最终使计算机系统发生故障以至瘫痪。这种现象与生物界病毒在生物体内部繁殖、相互传染，最终引起生物体致病的过程极为相似，所以人们把它形象地称为"计算机病毒"。

计算机病毒一般是一段程序或一组指令，它们具有下列的特点：

(1) 隐蔽性　计算机病毒都是一些可以直接运行或间接运行的具有高超技巧的程序，可以隐藏在操作系统、可执行程序或数据文件中，不易被人察觉和发现。

(2) 传染性　病毒程序一进入计算机系统就开始寻找进行感染的其它程序或信息媒介。它通过自我复制，很快地传播到整个系统或软盘、硬盘上。可以迅速地感染一个局部网络，一个大型计算机中心，或者一个多用户系统以及微型计算机系统。

(3) 潜伏性　病毒程序感染后往往并不立即发作，可以在几天、几周甚至几个月、几年内悄悄地进行传播和繁殖而不被发觉。在此期间，只要计算机系统工作，就会传染病毒，使得编制的程序和数据备份等可能染上病毒，成为病毒"携带者"。

(4) 表现性　病毒程序的最终目的是要捣乱、要破坏，因此一定要表现它的存在。病毒程序可能按照设计者的要求，在某种条件下使"攻击"部分活跃起来，对计算机实施攻击。表现（也称作"发作"）的条件与多种情况联系起来，如满足特定的时间或日期、期待特定用户识别符出现、特定文

件的出现或使用、一个文件使用的次数超过设定数等等.

计算机病毒的概念是在 1983 年 11 月 3 日的一次计算机安全学术讨论会上，由弗莱德·科恩(Fred Cohen)首次提出的. 他对计算机病毒所作的定义内容是：计算机病毒是一个能够通过修改程序，把自身复制进去进而去"传染"其它程序的程序. 弗莱德·科恩的定义强调了计算机病毒必须能够"传染"其它程序这一特点.

1-3 计算机病毒的起源

美国是计算机病毒的发源地. 早在六十年代初期，美国电报电话公司贝尔研究所里有一群年轻研究人员，常常做完工作后，就留在实验室里兴致勃勃地玩一种他们自己独创的计算机游戏. 这种叫作"达尔文"的游戏玩法很有刺激性，它是由每个人编制一段程序，然后输入计算机里运行，相互展开攻击，设法毁灭别人的程序，这种程序就是计算机病毒的雏形. 当时人们并没有意识到这一点，计算机病毒只是出现在科幻小说里作为故弄玄虚的"佐料"，没有人相信在现实生活中会出现这种东西.

真正的计算机病毒，通常认为是在十年前，首先产生于贝尔研究所，当时是因为工作失误无意中造出了计算机病毒. 也有人认为在同一时期，首先是施乐公司帕洛阿尔托研究所的研究人员在试验开发中，造出的计算机病毒. 从那之后，一些软件开发人员和恶作剧者，为了显示自己高超的技巧或存心开玩笑，陆续制造了不少计算机病毒.

计算机界真正认识到计算机病毒的存在是 1983 年. 弗莱德·科恩在 1983 年 11 月 3 日的计算机安全学术讨论会上

提出计算机病毒的概念后，随后获准进行实验演示。当天，专家们首先在运行 UNIX 操作系统的 VAX 11／750 机上实验成功第一个病毒，一周后（即 11 月 10 日）演示了另外五个实验。在五次实验中，病毒使计算机系统瘫痪所需时间平均为 30 分钟，证明病毒的攻击可以在很短的时间内出现，并得以发展和快速传播，从实验中证实了计算机病毒的存在。

1-4 计算机病毒与计算机犯罪

计算机犯罪不是说计算机去犯罪，而是指利用计算机去犯罪，犯罪的客体仍然是人。一般来说，把随意使用计算机或数据通迅设备、对受害者造成实际的或潜在的损失、或使犯罪者有实际的或潜在的收获活动，叫做计算机犯罪，通俗一些，就是"滥用计算机"。

计算机犯罪大约有五种类型：①盗窃程序和数据；②更改程序和数据；③盗用计算机时间；④用计算机进行贪污；⑤对计算机系统进行破坏。

计算机病毒是滥用计算机的典型，它用自定义程序或命令代码的方式实现对正常系统的干扰和破坏，属于计算机犯罪中的第五种形式，即对计算机系统进行破坏。由于计算机病毒与其它类型的犯罪不一样，往往在毫无知晓的情况下造成大面积"发病"，带来巨大损失。所以对制造病毒的人一定要严加惩处。

第二章　病毒造成的恐慌与危害

2-1　“黑色星期五”

1989年10月6日，荷兰警方郑重宣布，星期五（10月13日）全球将发生计算机大灾难！这一天计算机病毒将攻击计算机。灾星是三种计算机病毒，它们可以破坏计算机程序、数据或把数据全部“洗掉”。警方警告说，这些病毒已感染了荷兰10万台计算机。与此同时，台湾计算机厂商也发出警告，根据经销商回收资料估计，台湾现有70万台个人计算机中约百分之七八十已潜伏了病毒，情况严重时，星期五至少有50%可能会发病。一时间，全世界计算机用户一片恐慌。

面对警方的警告，计算机病毒防治专家迅速响应，推出了多种抗病毒软件供计算机用户使用。计算机厂商劝告人们在这几天最好不要开机，以避开病毒的袭击。对于连续工作不能停机的重要计算机网络和计算机系统，足智多谋的程序专家也施用了妙计，他们编制程序把数据存档日期从12日直接“过渡”到14日，越过13日。

由于采取了各种防范措施，事后仅有美国、荷兰、法国、英国和瑞士少数几个国家一些没有做好预防工作的计算机受到病毒侵袭，大灾难没有成为事实。

这个本来准备大肆施虐的病毒，其传染对象主要是运行

MS-DOS 的 IBM PC 机及兼容机，目前全世界共有这类计算机 2300 万台，一旦病毒流行开来，后果不堪设想。

这种病毒采取自扩散的方式传播，进行编码后向系统的各个目录、子目录扩散，通过调制解调器在网上传播，通过软盘媒介在微机上传染。当系统时钟转到 13 日星期五时，病毒就清除磁盘上 0 磁道信息、破坏磁盘目录。

这次事件虽然已经过去，但是人们并未搞清楚如何避免这次灾难的真正原因。据研究这种病毒的专家说，开发清除这种病毒的软件是极困难的。日本虽然没有计算机在这个"黑色的星期五"受到感染，但是日本政府仍被这次事件所震动，通产省立即着手考虑制定新的方针，帮助计算机拥有者防止病毒在下一个 13 日星期五，(即 1990 年 4 月 13 日) 扩散到日本来。

2-2 席卷全球的计算机病毒

计算机病毒自从 1983 年被专家们在实验中证实以后，短短几年里迅速蔓延到全世界。这里摘录部分报告：

▲ 1987 年 2 月美国东部一所医疗中心发生了一桩怪事，存储在医院计算机系统中的全部病历突然莫明其妙地消失了。专家们用了很长时间才查明，这是计算机病毒在作怪。编制这个病毒程序的恶作剧者还在计算机里留下了电话号码和这样一句话："当心病毒，请同我们联系接种疫苗。"

▲ 1987 年 10 月 21 日美国特拉华大学的一个计算机终端上发现了病毒，被感染的所有磁盘的卷标号上都变成了 Brain 这个词，并且部分磁盘中的数据文件也遭到了破坏。这就是后来风靡世界、著名的"Brain 病毒"。

▲ 1987 年 11 月 18 日美国宾夕法尼亚州勒海(Lehigh)大学受到又一种病毒的袭击，这种病毒一发作，便把磁盘上的文件撤消。仅两天时间，就有 600 多个软、硬盘被感染，造成学校图书馆含有硬盘的微型计算机系统的崩溃，使很多学生和其他读者自备的软盘也遭到了破坏。

▲ 1987 年 12 月下旬圣诞节前夕，病毒侵袭了 IBM 公司的国际电子信息网，恶作剧地先向计算机用户发出节日祝贺，然后根据该系统的用户信息来往名单记录，向每个曾使用过这个信息网的用户发出了相同的贺信，大量连锁信件使得这个著名的大型计算机网络不堪重负而瘫痪。不但美国，连以色列的赫布莱大学也遭到这种病毒的侵袭，致使多年的研究资料报废。

▲ 1988 年 3 月 2 日，这天开机工作的所有苹果牌微机 Macintosh 计算机在屏幕上自动出现了这样一条信息："《MacMag》杂志出版商 Richard Brandow 及全体人员，借此机会向全世界所有 Macintosh 用户们转达全球和平信息"，接着程序就自行毁坏了。

▲ 1988 年春，台湾大学资讯工程研究所，一台参加在台北市举行的 1988 年国际计算机围棋赛的计算机被病毒侵扰，完全瘫痪根本无法对弈。这是在台湾被发现的首例计算机病毒案件。

▲ 1988 年 8 月，苏联政府机构的计算机网络发现病毒入侵，三个月后，据专家宣称发现了三类计算机病毒，已查明其中两类。第一类是 A 型病毒，专门阻塞存储器，迫使计算机停止工作；第二类 B 型病毒，破坏程序目录，使计算机无法工作；第三类尚未说明。

▲ 1988 年 9 月 12 日，与日本电气公司联机的日本最