计算机病毒防护

〔美〕帕梅拉·凯恩 著

毋笃强 杨福缘 译

黄宗瑛 校

内容简介

本书介绍了计算机病毒的发展史及其防护，并从广泛的社会角度说明了计算机的安全问题。本书共分三部分：第一部分介绍了计算机病毒的产生、发展和现状；第二部分介绍了保护系统的重要信息；第三部分介绍了计算机病毒防护软件的应用。书末附有完整的系统安全检查清单和病毒程序一览表。本书把知识性和趣味性融为一体，既是专业性论述，也可作为科普读物。

本书适用于从事计算机开发、使用和管理的技术人员，也适合于对计算机病毒防护知识感兴趣的读者。

计算机病毒防护

〔美〕帕梅拉·凯恩 著

毋笃强 杨福缘 译

黄宗瑛 校

兵器工业出版社 出版发行

(北京市海淀区车道沟 10 号)

各地新华书店经销

兵器工业出版社印刷厂印装

开本:787×1092 1/16 印张:17 字数:458.64 千字

1990 年 12 月第 1 版 1990 年 12 月第 1 次印刷

印数:1～5000 定价:13.40 元

ISBN 7-80038-277-X/TP·17

译 者 的 话

1989 年伊始，计算机病毒惊动了整个世界。日本《朝日新闻》评选 1988 年世界十大科技新闻时，将“计算机病毒侵入日、美、苏计算机网”排在第二条；美国科学家评述 1988 年生物和技术物理领域重要国防科技十大新闻时，也将“计算机病毒在欧美流行”选入其中。其实，12 年前，计算机病毒只是科学幻想作品中的一个灾星，不久它从科幻闯入现实世界。1983 年 11 月 3 日，美国的科恩（Cohen）博士通过实验首次确认计算机病毒的存在。尽管当时的实验使在场的专家目瞪口呆，但直到 1987 年也只有专家和少数新闻记者知道计算机病毒的危害。然而，从 1987 年开始，计算机病毒象恶魔一样在全球范围肆虐。1989 年初，国内的计算机界人士还未来得及仔细推敲“计算机病毒”的含义、还没有采取任何预防措施，计算机病毒已开始登陆中华大地并四处蔓延。据报道，80%的微机曾受到感染。

何谓计算机病毒？它是何时、何地、何种背景下产生和发展起来的？它如何传播，应该怎样预防？这些问题不仅是从事计算机管理、开发和使用的科技人员迫切需要了解的，也是一般公众需要了解的知识。此书的翻译出版希望能满足广大读者的要求。

美国是计算机病毒的发源地，也是计算机病毒侵害的重灾区。本书于 1989 年 9 月在美国出版发行。本书的第一、二部分全面介绍了与计算机病毒有关的各个方面，包括计算机病毒的起源、发展；历次重要的计算机病毒入侵事件的全过程；对计算机病毒的社会反映；有关的法律和案例介绍；公众心理学；反病毒商业的兴衰；计算机病毒的原理介绍等。第三部分介绍计算机病毒防护系统，包括 DR.PANDA 防护软件的使用方法。经过熊猫公司的可靠性试验，这套防护系统能查出微机上出现的 99.94%的破坏性代码（包括计算机病毒）。附录 I 介绍了计算机管理上的完整安全措施清单；附录 II 是根据美国计算机网及微机上出现的病毒所列的计算机“病毒程序一览表”。

黄宗瑛同志仔细审校了译稿。本书的翻译出版得到了机械电子部第二〇二研究所技术开发中心和第十一室领导的大力支持。雷加印、毛征、魏玮等同志协助完成了全书的计算机输入工作。在此谨向他们表示感谢。

由于译者水平所限，译稿中不妥之处在所难免，敬请读者批评指正。

译者　1990.9

原 书 前 言

你大概不愿看到下面的情况吧？你用了 XYZ 公司的文字处理软件后，发现你的所有文件都被那个软件所破坏，因为 XYZ 公司雇用的一个卑鄙家伙在软件里面放置了某种病毒；也许有种病毒正等待着那个家伙在软件里设置的某个信号（可能是未来某日），日期一到，它会抹掉硬盘上你保存的一切文件；也有可能 XYZ 公司的竞争对手设置了某种病毒在他们自己的程序里，这个程序什么都不做，专等 XYZ 公司的版权标识出现，一旦出现，就使 XYZ 公司的软件失去作用。

要是染上病毒，这些小程序导致计算机不能正常工作，这是完全可能的。事实上，这些小程序就藏在某个地方。病毒比一般的乱七八糟程序更可恶，搅得我们终日不得安宁。

其实，几年前病毒还是个新鲜名词的时候，《National Enquirer》刊物的一个作者找过我。她感到，现在到了联合起来讨论病毒制造者写的代码是否可能进入国防部计算机系统发起第三次世界大战的时候了。有人问起我这个问题，我想很多专家都已讨论过这个问题。但当这位作者收集了足够的题材并动手写一本黄色报刊上登载的恐怖小说时，她惊奇地发现，关于这一题材的幽默感已经过时或者消失。事实上，这个刊物的出版社时常收到一些讨论文章要求刊登，讨论那些以前没有写过片言只字，以后也许会发生的事情。这并不是要吓唬一切阅读极其恐怖的《Enquirer》故事的老太太。要是那样的话，我本来可以选择关于来自火星的外星人的题材。现在，我很庆幸我的题材没有归于这一刊物的谎诞内容一类，而是成为现实，我感到很荣耀。

但事实毕竟是事实，病毒（viruses）、寄生虫（worms）和其它的 gotcha 软件代码就在那儿等待着牺牲品。牺牲品可能就是你，也可能是金融界，还可能是整个纽约市！象其它的疾病一样，预防胜过治疗千百倍，同样胜过复制保存原盘千百倍。

了解是预防之基础。最初，病毒恐怖曾影响国家大计算机公告牌系统（BBS）正常运行，因为人们害怕用户之间拷贝来拷贝去的软件可能是大部分病毒扩散之根源。现在，几乎所有的公告牌系统在合并文件时都十分严格，确保每一个文件都没有病毒。因此，“了解”是减少病毒传播的关键。

然而，最重要的是让用户明白，不论是否需要，都要让用户经常地把文件拷贝出来，而不是“一年拷贝一次”。但是，我们要做的事情不仅仅如此。这就是《计算机病毒防护》一书要做的事情。除了书尾附加的 DR.PANDA 防护软件，本书代表了一套完整的保护系统，它让我们的用户明白，离开它不行。本书描写生动，通俗易懂。

防止病毒经常出现在个人计算机的关键问题也很简单：不要借给别人。它就象涂鸦，如果一见到涂鸦就从墙上清除掉，涂鸦大师就会离开。他们要向人们展示他们的作品，他们不能容忍“爱清洁的人”对他们的作品作大量的“清扫”。这样，他们就会去城里找块人们愿意保留涂鸦的地方去乱涂，让涂鸦招来别的涂鸦。病毒代码的构思与涂鸦一样，也许，如果用户都来齐心协力预防他们的这种恶作剧，一发现就清除掉，那么，这些家伙可能就去别处，也许会变坏事为好事，作一些有益的事情。

我在旧金山湾认识的一位前“涂鸦”大师，他现在是一家大广告公司的高级广告家。我欢迎他们走正道，发展一些商业程序。他们中大部分人都有搞恶作剧的本事，同时也有编制高级程序的诀窍，使用户受益无穷。

幸运的是，本书可能会使“涂鸦”大师们醒悟。用户根本没有时间花在毫无价值的东西上，请给病毒代码制造者们带个口信：做点实事!

加州伯克莱　1989.6

目　录

第一部分　起源、发展和现状

第二部分 保护系统的重要信息

第三部分 DR.PANDA 实用软件

引　言

按照梅丽安姆-韦伯斯特字典出版者 G・C・梅丽安姆 (G.C.Merriam) 的说法，“计算机病毒”是 1988 年出现的新名词。计算机病毒、一些破坏性程序以及要求采取保险措施是成千上万的计算机用户正面临的问题。

计算机不是新生事物，但在许多家庭里、在每一个办公桌上使用计算机的现实却是新生事物；计算机病毒想法不是什么新闻，但公开传播却是头版新闻；害怕病毒是人之常情，但不断蔓延着的病毒恐慌却是新问题；“病毒(VIRUS)”不是新词，但把它用在计算机领域却是新题目。

0-1　V.I.R.U.S.——基本定义

由于新闻媒介、美国和外国政府、《FORTUNE 500》和差不多每个人似乎都在用病毒解释所有与计算机有关的反常现象，那么就让我们顺水推舟，用词首缩写词“V.I.R.U.S.”代表“攻击性的致命信息源”(Vital Information Resources Under Siege)。尽管问题很严重，但“真正”的计算机病毒只是 PC 机面临的威胁中最小的组成部分。

0-2　计算机安全问题——产生与发展

纵观历史，计算机工业的发展过程可以用皮秒来形容。本书的大部分读者——只要上过学，有点阅历——都会记着，“想当年”个人计算机在日常生活中还算不上什么离不开的帮手。然而，对 40 岁左右的人来说，大家都知道，他们的记忆实际上可追溯到计算机产生的年代。作为当时的孩子们，现在一定有不少人还记得当时观看查尔斯・范・多雷 (Charles Van Doren) 和乔伊斯 (Joyce) 博士兄弟二人回答一个 64000 美元的问题，题目出现在从 UNIVAC 机器抛出的纸卡上。当吐出穿孔的纸卡时，我们中间的一些人都看呆了，觉得不可思议。对今天的计算机看来，它只不过是过时的游戏。

人们总想把计算机安全与安全实施看作是相对新的问题。后面的说明会告诉读者，这种问题已经几十年了，只是目前这问题比以往任何时候都显得强烈。本书及软件会满足读者愿望，提供给读者许多工具和信息，帮助加强计算机安全管理。

0-3　本书简介

与凯撒执政时的古高卢人的所有作品风格一样，《计算机病毒防护》分三部分，每一部分相互独立，也就是说读者可以以任何次序阅读。本书并不是按前后章节循序渐进的方式编写的。

计算机病毒及解决办法只是范围很大的保险问题的一小部分。本书每一部分有所侧重地对技术方面、管理方面及威胁危险方面作出论述。至于如何掌握，则在于读者自己。

第一部分　起源、发展和现状

第一部分考查从第一代计算机在实验室安装就位并开始工作以后大约三分钟到今天这一发展时期，计算机犯罪和其它强盗行为(包括病毒活动)的历史过程，展示病毒攻击事件及伴随的社会舆论。它惊醒了一颗沉睡的行星，引起全世界高度警惕。第一部分也论述新闻媒介在传播新闻方面和在一个新兴工业诞生之际所起的作用，同时从各个方面展望未来。

第二部分　保护系统所需要的重要信息

本书的第二部分介绍计算机内部在做些什么、潜在的危险在何处、为什么以及人们该如何应付，搞清在保险问题出现的新时期责任在何处，帮助人们制定反攻击计划，并详细叙述了与计算机有关的法律及与读者有何关系。

第三部分　DR.PANDA 软件的应用

你也许不买《计算机病毒防护》一书，因为没有打算使用所附的软件。但就在第三部分才包含了本书的使用价值，从中你可以找出为什么和如何使用，及有关的技巧和陷井。

附录

附录中包括了更多的重要信息，一张保险措施清单和一般的"病毒程序一览表"(Dirty Dozen)，迄今为止已收集 200 多个。

0—4　软件概述

不论从技术还是实用方面，都没有一种绝对的方法把破坏性代码拒之于系统之外。唯一使系统绝对安全的办法就是关掉 PC 机电源，永远不再使用，但这不现实。

迄今为止，也还没有一种实用的方法能自动检验每一个进入系统的程序，无论这些程序是买来的还是拷贝来的。然而 DR.PANDA 问世了，它能做到这一点。

如果你还没有 DR.PANDA 防护系统，该到商店去看一看啦!

本书后面附有 DR.PANDA 软盘:

MONITORS——遏止破坏性程序攻击。

TSRMON(ITOR)——使非认可的程序不能进入 RAM。

TSRMONEZ——简化的 TSRMON 版本。

PHYSICAL——检查是否有破坏性代码对程序文件的修改。

QUIKPHYS——简化的 PHYSICAL 版本。

PHYSED——按规格改制 PHYSICAL 的编辑程序。

PINSTALL——PHYSICAL 及 QUIKPHYS 装入程序。

NOBRAIN——屏幕上检查一个软盘是否带有(C)脑病毒。

LABTEST——运行之前检查新程序。

DRHOOK——用现役程序描绘 RAM 区的使用情况。

GOPANDA——快速缺省方式装入的程序。

0—5　安全魔法(Safe Hex)

安全魔法是十六进制记数法的双关语，聪明的计算机专家从现在开始要进行训练。大家都"尝"苹果机 (IBM、Tandy 及 Compaq 计算机)，早期的清白已成为过去。现在该进入计

算机保险时代了。

0–6 请“医生”进来——多像医生在行医

在读下文之前，若你未在计算机上用过所附软件，你可能想看第十三章，按缺省方式装入三个基本的应用程序 PHYSICAL、MONITOR 及 TSRMON。找回原 DOS 盘，使用 GOPANDA 自动装入软件。一旦置入这些基本部分，大家都会放心多了。

0–7 警 告

至此，你已完成了最重要的部分——如何做，它能使 PANDA 对它周围起防范作用。

然而要记住，这个软件只能你用，一次只能在一台机器上用，就像两个人不能同时读一本书一样。两个人不应该同时使用这个软件，因为拷贝一个软件比起偷拍几百页厚的书要来得容易。所以请不要共同使用一个软件或一本书。事实上，共同使用是非法的，这就是版权警告。

0–8 学 习

每个人，从喜欢唱“独角戏”的人到成千上万的联网计算机管理员都必须关心安全问题。装入反病毒软件，即使是 PANDA 也仅仅是个冒险计划的第一步。虽然熟悉本书，但还需向有过此实践经验的人学习，设法搞清楚别人的特别情况是什么，与自己的需要和构成设计有何关联，查看其它有用的资料，共同分享知识的硕果。

第一部分　起源、发展和现状

第一章　基本概念

1-1　第一代计算机——庞然大物

在斯坦福·利维（Steven Levy）所著的《HACKER》一书中，作者把第一代计算机称作庞然大物，它是科学技术上的一次革命。我首次与庞然大物打交道是在大学一年级拼搏CO-BOL语言时。60年代中期，即使在最出名的大学里，在编程技术方面，几乎没有多少教授和导师比精力充沛的学生了解得多。大家都在一起相互学习，经常是由有直觉的、有才能的学生，而不是由教授或导师结束对全体人员的讲座。

我们学院的庞然大物是一年前以不可思议的高价买下的，的确是现代技术发展的水平。它座落在室温可以控制的"宫殿"里(真空管易于过热)，庞然大物只能由那些穿白大褂的"僧人"及助手们侍候，使人们想到它象一座医院。它还配备了一位特殊的助手，他的工作是专门更换烧坏的管子。不穿白大褂是不允许进入庞然大物驻地的。

那个庞然大物所用的内存是64k——仅有本书应用的PC机内存的十分之一。与PC机相比体积太大，不能让那些经常忘记数学公式的人使用。然而这一技术上的奇迹，不仅能处理熟练人员的实验工作，而且还能应付三万多学生的上机课。

当时数据是穿孔输入的，即使是最简单的程序也得要求数百张卡片，要预先用好多时间穿孔。象打印错误一样，错误的卡片放在错误的位置会导致灾难。在我的学生年代，使用过庞然大物两次，先在大学田径场上的小房子登记注册，每个系都建起了自己系的小厅子，完全象"电话厅"。在我的记忆里，完全象一场教育性商业表演。学生依次向门卫出示他们注册的穿孔卡片，门卫会查看学生是否按预定的时间到来(控制两天之内要安排三万多学生上机)，然后第一张卡片就换成了标有学生姓名和学生身分证号码的卡片。

入校生可优先选择(当时，早上十点钟去甚至比七点半去还快)，拿来一张所选的报名登记表，填好后还要拿到一张穿孔卡片，从而保证排上队。学生拿上穿孔卡片要前往集中卡的出口报到，不久，这些卡统统输进庞然大物。

第一组涉及整个过程的庞然大物的输出结果是期中成绩。二十五年之后，我还记得当时在"英国哲学"通过八个星期之后，"基本伦理学"差一点没通过。尽管这门课考得不好，但总算过去了，也没损失学分，计算机给出的结果伦理学课一定不会有错。我想庞然大物一定是对的，不会出错吧！一定有人放错了卡片。按照计算机输出的信息，花了数小时的时间找伦理学教授谈话，查找放错卡片的人接受了什么贿赂。

庞然大物也用来计算每个学生的"大学费用单"。整个学期的学费、住宿费和实验室使用费都要收集起来列出清单分送给学生的家长。的确，我们处在科学的前沿。大学发布的每个

人的情况，我们以前从未见到过，今天看来实际上是信用卡。卡上标有学校名及我们这个“吉祥物”代表的图案，我们为此感到骄傲。除此之外，卡上还有学生的姓名，学生的身分证号码。但我们发现，这个塑料卡片真正有用的地方是：当我们不堪忍受学生公寓或联谊会食堂的饭菜时，凭此卡可以在学生会买顿饭吃。据我们所知，击剑运动费、年鉴费及保龄球费，都是免费的。没有钱是行不通的，但每年邮回家的年度大学费用单却把父母吓坏了。

当然，每个人花费多少依赖于个人的因素，也就是你输入数据的准确与否。计算机是很笨的，庞然大物没有办法知道损坏了实验室一只试管后征收你 2 222 222.22 美元是不正常的，这个数字在当时可能能买下不包括建筑本身的整个实验室。不过这个问题总比学课分数搞错了容易发现。

当时，计算机课只教授三种高级语言：COBOL(商用)、FORTRAN(科学计算用)和APL(未来语言)。APL 语言是为掌握前两种语言但觉得还不够的人安排学习的。正是在 APL 语言班上，我神不知鬼不觉地对庞然大物进行报复。那时，我写出了世界上第一个计算机病毒程序，尽管它不是由机器传染的，而是人为传播的。

首例计算机病毒程序?

我突然有了灵感，肯定人们能用 APL 语言创造一个自动码产生器(不管它实际做起来是否需要 20 多年)。处在二年级学生智慧充分发挥的一刻，我觉得一个很长的编程工作的工作量可以减少 90%以上。编程很快完成，这个“大学生的秘密”只有几个好友知道。

首次运行，这个梦幻似的、了不起的编程就使庞然大物嘎地一声停住。超载、过度疲劳，所有的管子都过热发光。与高级主管的讨论，几乎让人象得了外胫炎那样可笑。主管在另外的若干次机会中尽量提高他的论证技巧，让班上同学花费很大力气对这个秘码再次穿孔。结果，在紧接着的后面几周里，连续七次使庞然大物崩溃。这使得“换真空管中队”忙得不可开交。

最早的安全考虑——最初的对策

这件事对校方有不少启示，更仔细的管理结构随之产生，它要导师在学生上机前仔细过滤学生自己想出的密码和新点子。有人写了一个名为“上帝之父”程序，用来查找使庞然大物无止境高速循环的代码串。所以，只要写出的东西不用上机，就是较笨的二年级学生在学 APL 理论时也能拿“A”。

最初的使用经验显示，早期与今天一样，计算机安全问题的提出经常是受到出现的前所未有的问题的触动之故。

1-2 登陆地球，逍遥自在

早先的计算机是很昂贵的，只有象政府机构、规模较大的大学及庞大的公司才会拥有。到了 70 年代初，随着硅芯片的问世，计算机不论从价钱或体积都明显地降到了适合于中等规模商业使用的水平。越来越多的计算机要求越来越多的人去使用，“计算机科学”随之变成人们选择赚大钱的行业。要求更高的技术人员去摆弄机器；越来越多的与计算机有关的公司应运而生。

从此不再要求早期那种恒温建筑的安全措施，磁带代替了穿孔卡片，挤在计算机机房的维修人员和所有过去有点计算机知识的人员几乎倾刻都变成了专家。当出现了专用任务软件接口后，处理器的直接编程随之消失，安全措施也随之而去。

由于许多产品涌入市场来满足人们不断增长的物质要求，这一代计算机不论硬件还是软件都有“滥”的趋势。计算机公司看到了在操作系统上设计一种“活动天窗”的价值，它使任何技术人员可以在任何机器上不经过繁琐的“登陆”过程就可以方便地使用计算机。年轻的罗伯特·莫里斯(Robert Morris)恰恰就是通过这样的“后门”，在 1988 年岁末打进了 ARPA 网(远景研究规划局计算机网)。

1-3 进入 PC 机世界

目前，无处没有的 PC 机到底有些什么缺陷呢？其答案是：说它简单，它确实复杂；说它复杂，它确实简单。这个答案很象过去的“先有鸡，还是先有蛋”的理论，要么接受先有鸡，然后才生蛋；要么又陷入不合逻辑的无休无止的辩论之中。

当 IBM 公司首次推出 PC 机时，大篮公司(Big Blue)当时就认为它比玩具高明不了多少，只是比玩具贵了点，好象少了它，这间屋子就低级一点。1987 年引入 PS／2 生产线时，IBM 公司的总经理以惊奇、揭示性的口吻大胆地说：“我们过去认为，要是能售出 50 万台 PS／2，那我们就算很幸运啦！”显然，IBM 公司已占据了“真正的”家用电脑市场，而且还预测不到价钱低廉的 PC 机到底会变成 IBM 公司什么样的忠实老黄牛。

使 PC／MS—DOS 个人计算机高人一筹或低人一等都在于它的操作系统。DOS 系统操作简单，这样使许多人用它来进行“计算”。随着 Visicale、Wordstar、dBase Ⅱ的问世，一台简单的 PC 机具备了大多数人梦寐以求的功能。尽管 PC／MS-DOS 的“C”提示符令人不可思议，但用起来却比较简单。正是由于它的使用简单，才使 PC／MS-DOS 计算机如此容易受到攻击。

要是听听“大篮”公司的劝告，仔细地“想一想”——早期的 IBM 公司老前辈经常这样做——那么今天的局面也许完全不同了。要是 IBM 公司先前预测到今天成千上万台 PC 机汇成全美的主流，那么操作系统也许现在还在研制过程中；如果早先有比较复杂、比较安全的操作系统出台，PC 机会不会象今天这样容易使用，会不会有这么大的吸引力迷住了这么多人呢？

1-4 进入 OS／2 世界

要理解怎样把 OS／2 产品推出来用不着火箭专家。1987 年召开了个人计算机系统第二系列产品介绍会，在许多城市同时举行了盛大的表演会。会上再次提出的一篇论文强调：“这一新系列计算机要对我们尊敬的客户负责。”我把自己当作买方中的一个典型用户，花了 15 分钟绞尽脑汁思考才弄明白，IBM 公司的子弹击中个人用户只是附带的结果，IBM 公司瞄准的是更远大的目标。个人用户就站在瞄准线上，早就被击中。显然，如果广大尊敬的客户的愿望和要求能得到完全满足，就算是巨大的合作。

可以想象，操作一词用 PC 机的术语解释就是“个人”。凡控制红色电源开关的人(从来弄不懂为什么它不用纯蓝色开关)都拥有个人计算机，那是他的(或她的)计算机，他(她)可以在上面随心所欲地摆弄。PC 机只受到操作员知识、兴趣和爱好的限制。对贯于控制计算机世界的美国来说，PC 机已变成管理上令人头疼的问题。为此，许多新的更为安全的操作系统以及不断发展的地区网络会逐渐地交由官方控制。