计算机病毒防治实用教程

何江安　梁新宇　著　唐龙　审

清华大学出版社

计算机病毒防治实用教程

何江安　梁新宇　著
唐　龙　审

清华大学出版社

内 容 简 介

本书是介绍计算机病毒防治技术的一本实用书籍。它介绍了计算机病毒的概念、分类以及防治方面的有关知识，提供了目前出现较多的几种病毒的防治方法，并对如何预防计算机病毒提出了一些具体的建议。贯穿本书始终的指导思想是简单、实用而又兼顾理论基础。

本书力图从一般计算机用户的角度来阐述问题，内容丰富，结构严谨，适合于从事和关心计算机工作的各类人员阅读，也可作为一般的教学和自学用书。

计算机病毒防治实用教程

何江安　梁新宇　著

唐　龙　　审

清华大学出版社出版

北京　清华园

清华大学出版社激光照排室排版

清华大学印刷厂印刷

新华书店总店科技发行所发行

开本：787×1092 1/32　印张：5.75　字数：126 千字

1990 年 11 月第 1 版　1991 年 5 月第 2 次印刷

印数：10001—25000

ISBN 7-302-00753-5/TP・253

定价：2.50 元

序

当代信息社会的计算机化，使得大到国际政治、外交、国防、财政金融，小到家庭、个人生活都越来越密切地与计算机相关联。计算机安全问题自然也就成为人们关注的问题。近两、三年在计算机安全问题上，更引人注目的是 Computer Virus，这个词可直译为计算机病毒。据估计，计算机病毒每年在全世界造成的损失超过十亿美元。

我国自去年三月报告发现第一起计算机病毒（“小球”病毒），半年内计算机病毒席卷全国，尤其各高等院校普遍受到骚扰。目前我国已发现的计算机病毒有 Ping Pong（“乒乓”或“小球”），Stone/Marijuana（“石头”或“大麻”），Pakstani Brain（“巴基斯坦”），Disk Killer（“磁盘杀手”），Jerusalem-B（“耶路撒冷-B”），Yankee Doodle（“扬基”或“扬基都德”），Vienna（“维也纳”），1701/1704（“瀑布”或“落花”）等将近十种。据清华大学校刊《新清华》89 年 12 月 31 日报道，全校上千台 PC 机受计算机病毒感染。“疫情”的确相当严重。我们曾在校内外十余个机房检查过数十台机器和数百片软盘，这些机房的机器几乎无一能幸免于难，有的一个大机房二十余台微机接待上千学生上机，却没有一台硬盘能正常工作；有的一台机器存在四、五种病毒，个别常用文件重复感染次数超过 50 次，其长度增加上百 K 字节；被抽查的师生员工手中软盘感染率平均为 70%左右。

面对这严峻的挑战，我们不得不应战。经过几个月的努力，总算基本控制住病毒蔓延。但计算机病毒不仅未完全扑灭，而且可以意料得到，今后还会有其他新的病毒继续骚扰计算机用户。目前，不少兄弟单位遭受计算机病毒的困扰，我们时常接到求援的信件或电话。编写一本有关防治计算机病毒知识的实用参考书，无疑是广大计算机用户的迫切要求。何江安、梁新宇同志编写的这本书正是他们踏实、认真而细致地工作的结晶。该书从计算机病毒基本概念、具体病毒实例剖析、预防措施、治理方法直至所使用的主要工具都做了全面的阐述，值得广大计算机用户一读。

要控制和扑灭计算机病毒，应特别强调法制教育和职业道德教育，有组织、有计划地采取切实有效的措施。与此同时，进行有关防治计算机病毒的科学知识普及宣传也是重要的一环，唯有这样，才能引起普遍重视，防治措施才能奏效。

唐　龙

1990 年 6 月 15 日

前　言

当计算机正以日新月异的发展速度广泛地深入到社会生活的各个方面的时候，计算机病毒的出现给社会——不仅仅是计算机工作者，而且包括政府、法律部门、各级领导乃至普通的工作人员敲响了警钟：一种新的利用计算机作为犯罪工具的高技术犯罪正成为日益严重的社会问题。

计算机科学的发展为计算机的迅速普及和广泛应用创造了条件。微型计算机的出现则将计算机引入家庭，大量的软硬件产品得到开发和运用。以计算机为核心的信息产业成为一个国家现代化水平的重要标志之一。在这种情况下，计算机病毒的出现和广泛传播正成为各国政府所关注的一个问题.

自去年上半年国内发现计算机病毒以来，在短短的一年时间里，病毒以几何级数扩散，迅速地感染了全国各地的大多数微机。不少人对此感到惶恐和不理解，他们非常迫切地希望了解计算机病毒方面的有关知识。虽然有不少报刊杂志不同程度地介绍了一些病毒的检测、消除方法和病毒的简单工作原理，为扼制计算机病毒的泛滥起了积极的作用。但这些文章还缺少系统性，有些甚至还有一些错误。因此，有必要向广大计算机用户介绍有关计算机病毒防治的系统性知识和实用技术，以便在遇到新情况时能排除故障，减少损失。

本书主要就微机病毒作一较系统地介绍，并简单介绍了出现在网络上的“蠕虫”(Worm)病毒。全书共九章。第一章介

绍计算机病毒的概念及其发展历史，并从几个方面对其作一些简单分类。第二章介绍计算机病毒的简单作用机制。第三章介绍微机操作系统（DOS 系统）的基本知识和磁盘分配情况，为病毒的消除和检测提供预备知识。第四章对目前流行较广的八种病毒作一解剖分析，并给出具体的处理方法。此外，本章还对目前在微机上发现的大部分病毒作一简介，并给出一般性的防治方法。第五章着重说明计算机病毒的防治技术。第六章介绍发生在网络上的“蠕虫”病毒。第七章介绍反病毒软件及其存在的问题。第八章介绍几个常用工具软件的简单使用方法。第九章简单讨论了计算机系统的安全性问题。

本书以实用性强为特点，较全面地分析了大家所关心的一些实际问题，同时也向广大读者介绍了计算机病毒防治的一些理论知识。

本书的编写得到了单位领导和其他许多同志的热情帮助，在此谨向他们表示衷心的感谢！魏淑馆、王萌、高虹等同志为本书的编写提供了大力帮助，在此也深表谢意！

作　者

1990 年 5 月　清华园

目　录

第一章　计算机病毒

随着计算科学及计算机制造技术的发展，计算机，尤其是微型计算机，已经广泛地深入到社会生活的各方面。在发达国家，计算机的使用几乎与所有家庭都有着直接联系，人们享受着人类智慧的结晶——计算机所带来的许多便利。然而，任何一门新的技术如果被应用到不正当的场合，则可能会产生许多消极的影响。计算机技术也一样。最近几年出现的利用计算机作为犯罪工具的高技术犯罪已经成为日益严重的社会问题，它不仅阻碍着计算机的应用和发展，而且构成了对整个社会的严重危胁。

计算机病毒(Computer Virus，简称 CV)是计算机犯罪现象中的一种。它的出现很快就引起了社会各界的关注。由于计算机病毒的传染性，在很短的时间里，它已经传播到全世界许多地区，甚至是偏僻的地方，并产生了许多恶性事件。许多人对此感到不理解，同时也感到惊慌，他们中的有些人对计算机的使用前景感到悲观，对计算机的可靠性丧失信心；而更多的人则是在寻找积极的方法去分析去防止、去消除计算机病毒的影响，提高自身系统的可靠性。这也是我们所必须正视的现实。

无疑，积极的方法才是我们应当采取的态度。计算机病毒的出现确实给计算机的应用带来了很多困难和损失，但是只要我们了解它，控制它，便有可能把计算机病毒限制在有限的范围，极大地减少它的危害。

1.1 计算机病毒的现状

目前对计算机病毒的现状还缺乏可靠的统计，但从已有的一些报道来看，计算机病毒已经普遍出现在许多单位，相当多的机器特别是微型计算机，感染过或多次感染过一种或多种病毒。1987 年到 1989 年可以说是计算机病毒从出现到猖狂的时期，特别是 1988 年 11 月在美国出现的 Internet 网被“Worm”病毒感染的事件，使得计算机病毒成为公众舆论的热点。有资料认为，到目前为止已经出现的病毒种类超过 100 种，其中在世界广为流行的大概有十几种。被病毒感染的机器和受到攻击的用户不断增多，图 1.1 是美国在 88 年、89 年受到病毒攻击的用户数目表。

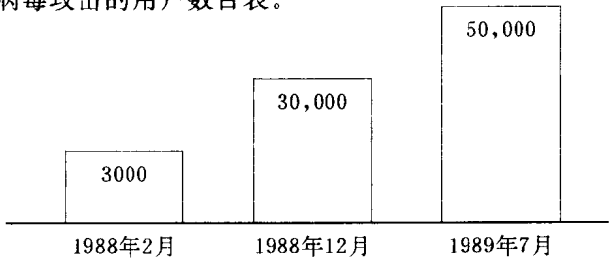

图 1.1

在我国计算机病毒的出现开始于 89 年初，但在不到一年的时间里，病毒就迅速传播，感染了相当多的机器，且病毒种类不断增多。目前发现的病毒不下于十种之多（还不包括一些变种）。从各地的反映来看，目前还只发现了微机病毒，其中绝大多数是出现在 DOS 环境下，还有一些是在 Macintosh 机器上。

在国内已发现的病毒有："小球"(Bouncing ball)，"大麻"(Marijuana)，"巴基斯坦智囊"(Brain)，"1701/1704"(Cascade1701/1704)，"扬基都德"(Yankee Doodle)，"648-A"(Vienna/648)，"磁盘杀手"(Disk killer)，"Dbase 数据库"，"耶路撒冷-B"(Jerusalem-B)和"音乐"病毒等。这些病毒具有强再生能力。有的单位受多个病毒交叉感染，系统受影响较严重。

虽然尚缺少有关病毒传播和破坏的详细材料，但从一些报道和我们接触到的情况来看，感染过病毒的单位和机器绝不是一个小数字。在国内应用微机较多的一些部门和地区，如银行系统、计算中心、高校等，发现的病毒和受感染的机器较多。

计算机病毒的出现曾一度引起了大家的恐慌，但经过一段时间的学习了解后，其传播得到了一定的控制，其消除方法也被许多人所掌握。但是否可以说人们就找到了对付计算机病毒的方法呢？其实，目前出现的计算机病毒还只是一个信号，它预示着更大的潜在危险。已经有人在探讨将计算机病毒的技术应用到军事领域，使其成为攻击敌方计算机系统的一种高级手段。新出现的计算机病毒对抗(Computer Virus Countermeasures，简称 CVCM)就是一种不同于传统的电子对抗(Electronic Countermeasures，简称 ECM)的新技术，它通过无线电技术将病毒程序植入受攻击的目标，让其潜伏下来，以在某种条件下执行预定的任务。对这种技术的思想，我们不作评论。但令人忧虑的是，计算机病毒程序的滥用有可能带来非常严重的后果，尤其是在敌对的军事系统中，甚至会给人类带来毁灭性的打击。因此，从全人类的利益出发，应该停止计算机病毒的制造和滥用。

1.2 计算机病毒的危害

我们认为，由于目前的病毒更多出现在一般的系统中，因而其危害性还是有限的。但是，随着计算机网络的发展和计算机在控制系统中的广泛运用，计算机病毒可能产生的潜在危害是不可估量的。

在一般的系统中，人们所从事的工作结果往往以数据或程序的形式存储在一定的介质上，因此，计算机病毒的危害性主要体现在对这些数据的破坏和对系统本身的攻击上。从宏观上来看，这种破坏的结果还是可挽回的，只是要花费一定的人力和物力。

但在控制系统中，由于计算机扮演着重要的“指挥官”角色，它的每一个命令，每一个数据的失误都可能会产生不可估量的后果。尤其是在实时控制系统中，计算机的任何一点故障（包括硬件的和软件的故障）都可能引起严重的危害，更不用说当计算机病毒作用时可能引起的系统瘫痪了。在工业系统、实验系统和国防系统等方面的实时控制中，病毒的危害可能产生的严重后果是难以设想的。

1.3 计算机病毒的起源

对计算机系统的攻击具有多种形式。最早期的一种是特洛伊木马(Trojan horse)程序，它借用古代特洛伊战争中把士兵隐藏在木马中进入敌方城堡，出其不意攻占城堡的故事，来表示某些有意骗人犯错误的程序。程序开发者开发一个表面上很有魅力而且显得可靠的程序，可是使用者使用一定时间

或运行一定次数后，便会发生故障，出现各种问题。1982 年，Shoke 和 Hupp 提出了一种“蠕虫”(WORM)程序的思想。这种蠕虫程序常驻于一台或多台机器中，并有自动重定位的能力。如果它检测到网络中的某台机器未被占用，便把自身的一个拷贝发送到那台机器，如此递归下去，便可检测到网络上一些机器的情况。蠕虫程序不一定有害，Shock 和 Hupp 论证了蠕虫程序可用作为网络设备的一种诊断工具。它也可用作“通告板”、报警钟或用在机器动画中。1984 年 5 月，Dewdney 提出了一种叫做“磁心战”(Core war)的游戏，其大意为，编写一个程序，用来分配计算机存储器内某个限定容量的空间，该空间由连续的单元构成。按模运算使得该存储器循环。然后再编写两个或更多个汇编程序，这些程序的唯一用途是试图破坏其它程序。它们被装填到任意的一些非覆盖区中并被执行，通过使用自动重定位，每个程序按存储器循环周期每次一条指令地逐渐接近其它程序。结果有二：若已执行 N 条指令仍未接触到对手，则为和局；否则，被对手修改而不能执行某条指令的一方为败者。

1984 年，Fred Cohen 博士获准首先在运行 UNIX 操作系统的 VAX 11/750 机上进行病毒试验。在五次试验中，使计算机系统工作瘫痪所需的平均时间为 30 分钟，最短为 5 分钟。他认为在对某特定系统有个基本了解的条件下，可以构成一种病毒代码，该病毒代码容许攻击者在平均 30 分钟内使大量程序受到感染，从而控制整个系统。Cohen 的实验证明了计算机病毒的存在可能性。此后，一些公司为了保护他们的软件不被非法复制，在发行软件中加入病毒，以期打击非法复制者。这在一定程度上助长了各种病毒的传播。虽然在这类病毒中尚未发现恶性病毒，但他们的变种却可能成为严重的灾难。计

算机病毒的另一个来源是一些恶作剧者、计算机狂以及在工作中心怀不满、蓄意报复的人，他们对计算机系统往往比较熟悉，也容易编写计算机病毒。

但到底计算机病毒的起源如何，目前还只有各种猜测。我们认为，计算机病毒是随着计算机软件的发展而逐渐产生的，其思想来源于早期的特洛伊木马程序。编制这种程序的人一般有两种，一是恶作剧者，他们具有较丰富的系统知识和编程经验，试图通过这种程序来显示自己的才能；其次是心怀不满的报复者，他们因生活或工作上的不顺心而产生对单位或社会的报复心理，从而在自己开发的软件中加入特洛伊木马，以达到报复目的。后来，随着软件的发展，了解系统的人越来越多，他们中少数人从一些生物界的现象中受到启发，便不断地改进自己的特洛伊木马程序，从而衍生出现在的计算机病毒。

微型机的出现使计算机的应用发生了革命性的变化，许多家庭都购置了计算机。而随着微机出现的DOS操作系统则同微机一道为大家所了解和掌握。大量的应用软件不断涌现。由于软件拷贝的方便性，软件版权侵权现象非常严重。一些人或单位为了追踪非法复制软件的现象，在软件中加入计算机病毒，从而导致病毒的大范围流行。这从另一方面也说明了软件侵权行为的普遍性。

总之，无论计算机病毒的起源如何，它已确确实实出现在人们的面前，解决这些现实的问题才是我们的紧迫任务。

1.4 计算机病毒的定义

前面谈了计算机病毒的现状、危害及起源，但究竟什么是计算机病毒呢？实际上，目前还没有一个定义为大家所普遍接

受。而确定什么是计算机病毒却是判断、控制病毒的关键，也是法律判定的科学依据。

Fred Cohen 博士是较早研究计算机病毒的专家之一，他认为计算机病毒是“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 则认为计算机病毒是“一种能够使自身的拷贝插入(通常以非破坏形式)到某一个接受拷贝的程序或宿主程序中的指令序列”。这些定义虽然概括了计算机病毒的一些特性，但不难看出它们在有些方面仍有欠缺。我们知道，在生物界，“病毒”是指那些能够侵入动物体内并给动物体带来疾病的微生物，其最大特点为传染性和危害性，那么计算机病毒既然采用了“病毒”这一术语，它也就同样有这两大特点，在其定义中应得到体现。因此我们认为，计算机病毒是“能够侵入计算机系统的并给计算机系统带来故障的一种具有自我繁殖能力的指令序列”。也可以认为它是“特洛伊木马＋传染性”。

计算机病毒一般具有如下重要特点：

(1)是一个指令序列：也即计算机病毒是程序(但它不是一个完整的程序，而是寄生在其它可执行的目标上)。因此它享有一切程序所能得到的权利；此外，它与生物病毒是在不同系统中出现的两个相似概念，两者各自在本系统中发挥作用。

(2)传染性：一个计算机病毒能够主动地将自身的复制品或变种传染到其它对象上，这些对象可以是一个程序，也可以是系统中的某些部位，如 DOS 的引导记录等。

(3)欺骗性：计算机病毒寄生在其它对象上，当加载被感染的对象时，病毒侵入系统，它是在非授权的情况下因具有一定的欺骗性而被加载的。这也正是特洛伊木马程序的特点。

(4)危害性：计算机病毒的危害性是广义的，它不仅仅是

指破坏系统，删除或修改数据，而且包括占用系统资源，干扰机器运行等。

此外，为服从于传染性和危害性的需要，病毒一般还有以下特点：

(5)隐蔽性：计算机病毒的隐蔽性使得其难以被发现，因而可以有更长的时间去实现其传染和破坏的目的。

(6)潜伏性：计算机病毒侵入系统后一般不立即发作，而需经过一段时间满足一定条件后才发生作用，这样可为其传染和破坏争取时间。计算机病毒的潜伏期长短不一，长的可达数年以上。

(7)精巧性：计算机病毒的代码一般都很短，很精巧，这样可使其不引人注目。

(8)顽固性：计算机病毒即使在被发现的情况下，它所破坏的数据、程序和操作系统等也往往难于恢复。

另外，还有一些与"病毒"易混淆的现象，这在最后附录一的术语中将作说明。

1.5 计算机病毒的分类

计算机病毒的分类取决于所采用的分类标准。如以产生的后果来看，病毒有"良性"病毒和"恶性"病毒之分。所谓"良性"是指那些不破坏数据或程序并导致系统瘫痪的病毒，这种病毒多是一些恶作剧者所造。但正如计算机病毒的定义所说，危害性是所有病毒的一大特点，"良性"病毒并非没有危害性，只是它们的危害性相对而言要小得多。但在用户缺乏对病毒和系统的了解的情况下，这种病毒也可能会产生较大的破坏作用。因此，"良性"只是一个相对的概念。从本质上讲，所有