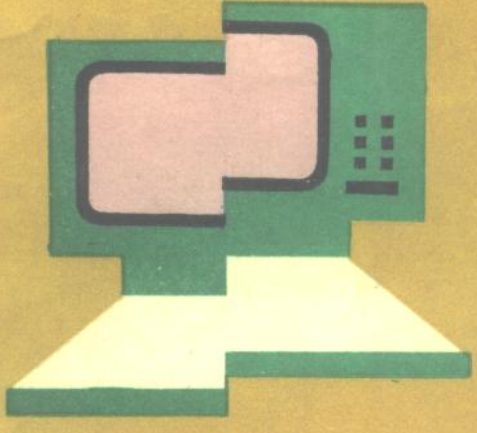
智慧的挑战

——计算机安全与病毒防治

方顺水 熊 璋 张勤勇 谢小全 编著



化学工业出版社

智慧的挑战
——计算机安全与病毒防治

中国运载火箭技术研究院
计算机病毒防治中心
方顺水　熊　璋
张勤勇　谢小全　编著

化学工业出版社

智慧的挑战

——计算机安全与病毒防治

中国运载火箭技术研究院
计算机病毒防治中心
方顺水　熊　璋
张勤勇　谢小全　编著

责任编辑：张文虎
封面设计：季玉芳
*
化学工业出版社出版发行
（北京和平里七区十六号楼）
李史山印刷厂印刷
李史山厂装订
新华书店北京发行所经销
*
开本 787×1092 1/32　印张 7 1/4　字数 164 千字
1991 年 4 月第 1 版　1991 年 4 月北京第 1 次印刷
印　数　1—6,500
ISBN 7-5025-0917-3/TP・27
定价：4.40 元

序

随着计算机技术，特别是微电子技术的飞速发展，计算机应用几乎渗透到人类社会生活的各个方面，向着集成化、网络化、智能化和标准化的方向前进。人类正进入信息化社会。

科学技术都是在自身的矛盾运动中发展的，计算机科学和技术也不例外。伴随着计算机的诞生、计算机技术的提高和计算机应用的普及，计算机不安全性一直存在并起着阻碍作用，特别是近些年来，计算机病毒的滋生和蔓延，已经给许多计算机应用领域和部门造成了严重的危害和损失，极大地威胁着人类信息社会。

几年前，当我们听到大洋彼岸一些国家计算机病毒危害情况的新闻报道时，我们还只当作海外奇谈，思想上没有引起应有的重视。岂不想嗣后不到两年的时间里，计算机病毒也在我国迅速蔓延开来。据有关部门统计，全国竟有 70～80％的微机曾先后感染病毒。中国大陆并非世外桃源，只是由于我国政府及时采取了有力措施，才有效地抑制了计算机病毒的继续蔓延，最大限度地减少了直接经济损失。

本书的作者是几位年轻的计算机科学硕士、博士，工作在计算机安全和病毒防治第一线。他们出于使命感，在很短的时间内编写了这本书，有可能文字上粗糙一些，但一种近乎神圣的社会责任感却熠熠发辉地闪现在字里行间。书中较系统地阐述了计算机安全学的有关问题，较详细地介绍了国内外计算机病毒的现状和危害，从理论与实践的结合上阐明了预防、检测、

清除计算机病毒的技术和方法。因此，本书对从事计算机技术研究和计算机应用的部门及单位的领导、管理人员、技术人员和操作维护人员都具有实用价值和参考价值。

周正清

1991 年 1 月 11 日

编 者 的 话

近年来，全球性的计算机病毒危机给社会造成了巨大的危害。这种高科技带来的负作用，不仅仅体现在巨额的经济损失上，更重要的是使人们对科技进步的意义产生了疑虑。当计算机病毒开始横行中国大陆时，人们即焦虑又恐惧，一方面是由于计算机病毒的来势凶猛和危害严重，另一方面是由于人们缺乏足够的心理准备和计算机安全的有关知识。当前，论述计算机安全，尤其是计算机病毒防治的专题文章已陆续出现，然而，从各个方面较为全面完整地论述计算机安全及有关问题的书籍却嫌少见。基于这种现状，本书不仅提供了运用微机常用工具软件对付常见计算机病毒的办法，论述了如何从技术、立法、管理和人员等方面来保证计算机系统的安全，还介绍了计算机病毒的有关理论问题，展示了当今国内外计算机安全的现状和计算机犯罪的严峻现实。本书还从计算机发展的角度论述了科技进步对社会的影响。总之，希望读者能通过本书对当前计算机系统的安全问题有一个比较全面的了解，并借此达到抛砖引玉的目的。

幸赖中国运载火箭技术研究院的鼎力襄助，本书才得以与读者见面。国际宇航协会通讯院士、长二捆火箭（CZ-2E）总设计师王德臣研究员为本书题写了书名，中国运载火箭技术研究院技术部总工程师周正清研究员在百忙中主持审定了本书并为本书作序。中国科学院计算中心刘尊全教授、中国运载火箭技术研究院计算机应用研究所税蔚栋研究员、中国运载火箭技术

研究院技术部金毓瑞高级工程师参加了审定。

本书由六位作者执笔写成，具体分工如下：第一章，张晓丹；第二章，张继红；第三、四章，谢小全；第五、七章，张勤勇；第六章，熊璋；第八、九章，方顺水。北京航空航天大学计算机系副教授熊璋从技术角度统阅了全书，中国运载火箭技术研究院计算机病毒防治中心负责人方顺水负责全书的编写组织与定稿工作。

本书的完成，完全是出于计算机专业工作者的职业道德与社会责任感。由于在计算机病毒防治工作中遇到的种种问题，作者深深地体会到“Ignorance is the computer felon's first line of defence”（无知是计算机罪犯的第一条保护线）乃至理名言，因此，作者痛感有责任尽快地向广大读者阐明计算机安全与病毒防治中的许多问题。由于在这种急切的心情下仓促成书，难免有不尽人意之处，敬请读者提出批评与建议。

在本书的完成过程中，还有许多同事与朋友给予了慷慨帮助，正是他们的鼓励与爱心，使得作者以更大的努力完成了本书。

编者

目　　录

第一章　计算机病毒的渊源与现状

1　震撼世界的“蠕虫”

1988 年 11 月，美国新闻界竞相报道所谓“INTERNET 网络事件”，“计算机病毒”这个神秘的字眼忽然间充斥大小报刊，国际计算机领域由此拉开了研究计算机病毒的序幕。

“INTERNET 网络事件”何以能掀起这般轩然大波？

INTERNET 网络是美国最大的计算机网络，与全球数百个城市网相连，其骨干是国防数据网（DDN）以及许许多多的大学校园和私人公司网〔刘瑞挺 90〕。有资料表明，目前它拥有两万台以上的主机和上百万的用户。DDN 的主要成员有 ARPANET、MILNET 和 MINET，由国防部通信局 DCA（Defense Communication Agency）管理。MILNET 是一个具有较高保密性的远程军用网。DDN 中另外还有一些保密性更强的军用网。由此看来，对那些天才的“计算机恶作剧者”（Computer Hackers）来说，INTERNET 网络确实极富诱惑力。事实上，的确有人曾一试身手：1988 年 11 月 2 日，23 岁的 Robert T・Morris，Jr.，把一个“蠕虫”（Worm）放进了 INTERNET 网络。蠕虫是计算机病毒的一种。

Morris 在美国康奈尔（Cornell）大学他自己的计算机上，用远程命令将蠕虫程序送进网络，他原本希望这个“无害”的蠕虫程序能慢慢地渗透到政府与研究机构的网络系统中，并且悄悄地呆在那儿，不为人知，然而由于他在程序编制中犯了一个

小错误，结果这个蠕虫程序疯狂地不断复制自己，并向整个INTERNET网络迅速蔓延。待Morris发现情况不妙时，他已经无能为力了。他无法中止这个进程。据说，他曾请在哈佛大学的一个朋友发一条关于这个蠕虫程序的警报到ARPANET网上，但是由于网络已超载，几乎没有什么人注意到或接收到这条信息。于是，小小的蠕虫程序，在1988年11月2日至3日的一夜之间，袭击了庞大的INTERNET网络，其速度是惊人的，下面的这张表可以大致反映蠕虫侵袭的时间顺序〔Highland 89〕，表中时间为“东部标准时间”(Eastern Standard Time)。

1988年11月2日，星期三：

17：00 纽约康奈尔大学检测出病毒。

21：00 加利福尼亚的斯坦福大学和兰德公司发现病毒。

22：00 加州大学Berkeley分校被病毒攻击。

23：00 新泽西的普林斯顿大学数学系遭遇病毒。

23：00 麻省理工学院人工智能实验室发现病毒。

23：28 加州大学Davis分校和San Diego分校、加州的Lawrence Livermore实验室、NASA（美国航空航天署）被病毒感染。

23：45 军事弹道研究实验室发现病毒。

1988年11月3日，星期四：

01：00 15台ARPANET主机被感染。

02：00 在麻省的哈佛大学发现病毒。

03：30 麻省理工学院计算中心发现病毒。

04：00 由于网络超载，病毒传播速度减慢，但是大约有1000个场地的主机已经遭到袭击。

05：15 宾夕法尼亚的匹兹堡大学发现病毒。

08：00 Smithsonian空间物理中心被袭击。

15：00 抗病毒软件分发给受侵单位。

21：00 在麻省理工学院举行第一次记者招待会。

Morris的蠕虫一夜之间攻击了INTERNET网上约6200台

VAX 系列小型机和 Sun 工作站，300 多个大学、医院和研究中心都有关于蠕虫攻击的报告，DCA 的一位发言人宣称，不仅仅是 ARPANET，军用的 MILNET 网中也有几台主机被袭击。经济损失达 9200 多万美元！

“INTERNET 网络事件”发生后，美国新闻界对此异常热心，各种宣传媒介大肆宣扬，《纽约时报》、《华盛顿邮报》、《今天》等各大报刊，连续两周纷纷报道 INTERNET 网络事件的发生，事件造成的损失，各界人士的反映，肇事者的情况等等，一时闹得满城风雨、人心惶惶。在此之前，大多数计算机用户对计算机及网络的安全性，还是很有信心的，“INTERNET 网络事件”对广大用户的这种信心无疑是一次沉重的打击。

“INTERNET 网络事件”同样也极大地震惊了计算机安全人员与其他专业人员。在 Morris 的蠕虫大举进攻之际，许多网络管理员、安全专家和研究人员急切而又灰心，他们甚至不敢相信眼前正在发生的事情，有一份介绍蠕虫攻击情况的报告是这样开头的：“现在是 1988 年 11 月 3 日，清晨 3 点 45 分。我很累了，所以请不要相信下面描述的任何事情……”〔Highland 89〕。

“INTERNET 网络事件”的确是一场灾难，但是决不是象某些报刊所说的宣告了“计算机系统的末日”。事实上，清除病毒的工作开展得相当迅速。11 月 2 日星期三发现病毒，到第二天晚上，就有一个消毒方案公布，到周末，病毒已经被控制住了。随后，美国国防部在 Carnegie-Mellon 大学的软件工程学院建立了一个由 100 名计算机专家组成的应急行动小组，专门研究国防部门计算机系统对计算机病毒攻击的防卫问题，并及时了解、监视 INTERNET 网络的安全情况。可以说，“INTERNET 网络事件”为计算机安全专家敲响了警钟，计算机系统的安全问题一

跃而成为许多公司和研究部门最迫切的研究课题。早在事件发生后的第二天，也就是 11 月 3 日，星期四，就有人指出："……这个病毒的确是件好事，它无法扼杀我们，反而能使我们更加强壮"。无论是计算机安全专家，还是一般的计算机用户，都有这样一个一致的看法，那就是："既然未能从成功中得到经验，那就让我们从失败中汲取教训吧"〔Highland 89〕。

在谈及"INTERNET 网络事件"的影响时，我们自然会想到那巨大的经济损失和艰巨的清毒劳动，也会想到计算机专家对网络安全问题的困惑和用户对其系统可靠性的担忧，这是事件影响的一个方面。事件影响的另一个方面则更加重要，那就是，计算机病毒研究，作为一项专门课题，从此登上了计算机科学领域的舞台，不仅计算机系统的安全问题得到了前所未有的重视，计算机文化的发展也引起了社会的普遍关注。

我们不得不承认，当前计算机文化与计算机科学的发展极不平衡。举例来说，人们对利用计算机病毒手段进行计算机犯罪的看法就非常混乱。"INTERNET 网络事件"后，所有的报道都认为，肇事者 Morris 编写蠕虫程序并非出自恶意，Morris 或许直到被推上法庭也不认为自己是犯了罪。事件发生后，公众对 Morris 的态度多种多样：有人愤愤然认为他犯了弥天大罪，法庭应该绞死他；有人爱惜其才华（不能不承认，Morris 编制的蠕虫程序具有极高的技巧），认为这样的青年是国家的财富；Morris 的辩护律师则声称 Morris 帮助人们认识到计算机系统本身的脆弱性，他非但是无罪的，甚至是有功的；也有人持折衷态度，认为 Morris 犯了错误，但不至于被投进监狱。我们无意在此讨论计算机犯罪的法律问题，我们只是想说明："INTERNET 网络事件"反映出来的公众对计算机犯罪有关法律问题看法的混乱，从一个方面暴露了计算机文化与计算机科学发展的极端不平衡。

作为故事的结尾，我们有必要交代一下 Morris 的情况。

有趣的是，Morris 是美国政府高级计算机安全专家的儿子，其父是致力于计算机安全研究的美国国家计算机安全局的主要科学家。Morris 从中学起兴趣就转向了计算机，17 岁到贝尔(Bell)实验室工作，接着参加哈佛大学计算机计划，在心理学计算中心当程序员，随后进入康奈尔大学计算机系学习。不管 Morris 当初编制其蠕虫程序的用意是什么，“INTERNET 网络事件”是既成事实，Morris 于 1989 年 7 月被推上了美国地方法庭。据我国《科技日报》1990 年 2 月 6 日的报道，Morris 已于 1 月 22 日被联邦法庭宣判有罪，处以 5 年监禁和 25 万美元罚款。Morris 是自 1986 年美国公布计算机欺诈和滥用条例以来，第一个被送上法庭的人。

2 计算机病毒的渊源与展望

计算机病毒是近几年内才成为热门话题的，然而如果要追溯计算机病毒的起源与历史，我们还得先谈谈计算机系统本身。

众所周知，目前的计算机系统无一不是以冯·诺依曼结构为基础的。早在 1947 年，冯·诺依曼建立其计算机系统理论时，就已经指出了计算机系统本身的脆弱性（这种脆弱性正是计算机病毒产生的基础）。然而 30 多年来，冯·诺依曼的警告没有得到人们的重视，甚至没有得到痛快的承认。直到今天计算机病毒大肆进攻之际，才有人想起了冯·诺依曼 1947 年的警告。事实证明了冯·诺依曼关于病毒的预见，后来者不能不佩服我们的先驱冯·诺依曼的远见卓识！

1977 年夏天，Thomas J. Ryan 出版了幻想小说《The Adolescence of P-1》。在这本小说里，作者幻想出一种计算机病

毒，它能从一台计算机到另一台计算机传染流行，并能控制7000台计算机的操作系统。作为一本科幻作品，小说自然没有得到计算机安全人员的重视，也没有引起一般公众的特殊兴趣。至于它是否启发了个别“计算机恶作剧者”的灵感，就不得而知了。不妨认为这是第一例幻想病毒。那么，真实的第一例病毒究竟是在什么时候、什么地点出现的呢？

1983年，美国计算机安全专家Frederik Cohen通过实验证明了计算机病毒实现的可能性，至此，计算机病毒由幻想变成了现实。1984年，Cohen在美国国家计算机安全会议上演示了病毒的实验，所以现在一般认为，世界上第一例计算机病毒是由他创造的。Cohen1984年在“国际信息处理联合会”文集（IFIP/sec'84）中发表了关于计算机病毒的论文。1987年2月，美国的《计算机与安全》杂志刊登了这篇论文。然而直至1987年，大多数计算机安全人员还认为计算机病毒只是个深奥而神秘的莫知世界，而且也不大可能发生。

不曾料想，到了1987年，计算机安全人员忽然发现，地球的这儿那儿，许许多多的地方，几乎同时出现了各种各样的计算机病毒：Brain病毒、Lehigh病毒、IBM圣诞树病毒、黑色星期五病毒等等。面对计算机病毒的突然袭击，众多计算机用户甚至专业人员都惊慌失措。尽管计算机病毒的种类不断增多，传染范围不断扩大，危害程度不断加深，但是仍然有相当一部分人抱着一种美好的愿望，希望计算机病毒不久就会“自生自灭”。因而在1988年美国“INTERNET网络事件”发生之前，计算机病毒并没有得到真正的重视。“INTERNET网络事件”能有幸成为一“事件”而为世人所瞩目，一个很重要的原因就是，“INTERNET网络事件”是一个转折点，它使得计算机病毒问题真正得到了计算机安全人员和计算机用户的普遍重视。

不过，由于很多人对计算机病毒尚没有正确的认识，也不知道如何预防、检测和清除，因此，重视中的恐惧成分仍令人不堪重负，这就使得计算机用户在诚惶诚恐中度过了 1989 年。这一年度里，全世界各处计算机病毒的进攻十分猖狂。自 4 月份起，我国也相继发现了小球病毒、Brain 病毒、大麻病毒、黑色星期五病毒等。值得一提的是 1989 年 10 月 13 日，星期五。13 日又是星期五在西方被视为“黑色星期五”，因为吟诵《圣经》的西方人认为这一天最不吉利。1989 年 10 月的黑色星期五，对计算机界人士而言，则是灾难性的一天。人们已经知道，1987 年秋在以色列耶路撒冷 Hebrew 大学发现的黑色星期五病毒，在黑色星期五这一天将被激活，并将破坏被感染的计算机磁盘。1989 年 10 月 13 日这一天，计算机用户各显神通，或前置其系统时钟，或干脆关闭其系统。幸运的是，由于有所准备，这一天，黑色星期五病毒并没有席卷全球，不过仍有不少计算机系统遭到袭击，英国、葡萄牙、法国、荷兰、瑞士等国均有黑色星期五病毒袭击的报告。据估计，在荷兰，约有 15 万台 PC 机系统受侵。我国的天津、武汉等地也发现了黑色星期五病毒。香港的一家计算机公司居然在其计算机屏幕上得到一条通知：“今年我们将您遗漏在外，但明年（1990 年）我们还会再来。”只有日本人无忧无虑，他们 90％的计算机都是与 IBM 不兼容的 NEC 机种，不是黑色星期五病毒的袭击对象。

应该指出，人们并不是眼睁睁地看着计算机病毒横行肆虐，也并非束手无策，越来越多的计算机专家已致力于抗病毒工具的研究。一般，在某种病毒被发现后不久，就能迅速推出一种检测、解毒与免疫工具。目前，国外已有不少公司拥有自己的抗病毒工具。然而，任何一种抗病毒工具都是针对某特定环境下的某一类病毒的，而病毒新品种的出现又是不可判定的，因

此，在同病毒的斗争过程中，抗病毒工具只能处于被动的地位，我们无法抑制病毒新品种的出现。而且，新品种病毒往往隐蔽性更好，危害更大。例如，1989 年底在美国出现的新一代“秘密”病毒——“4096 病毒”，破坏性强，且能巧妙地躲避抗病毒程序的检测和清除，许多抗病毒软件对它都无效〔Highland 90a〕。

计算机系统本身的脆弱性是计算机病毒产生的客观原因，计算机系统的信息共享是计算机病毒传播的基础。在今后相当长一段时间内，我们不可能抛弃冯·诺依曼结构的计算机体系，也不可能严格限制计算机系统的信息共享，因而不管人们的主观意愿如何，计算机病毒的滋生土壤总是存在的。这样，我们就不得不遗憾地承认，计算机病毒是不可避免的，它将永远伴随着计算机的持有者和使用者。最近国外发现的一种新病毒 Eddie，其中有一段提示：“Eddie 活着……迟早会出来”，着实发人深省。

3 当今世界的病毒危机

计算机病毒纠缠我们已经有几年了（它将成为 21 世纪国际恐怖活动五种新手段之一，并且排在第二位），不少用户因此而大吃苦头，侥幸被病毒遗漏在外者也未免战战兢兢，担心在某一次开机时，会发现一些意外的东西：一声“亲切”的问候（Sunnyvale 病毒），一曲优美的“蓝色多瑙河”（音乐病毒），……当您还在惊奇和迷惑时，或许您的文件已经被搞得面目全非了。今天，所有的计算机安全专家都在大声疾呼：警惕，警惕！计算机病毒在全世界肆虐！不过，要对计算机病毒的现状做一个全面而准确的介绍，仍然是件非常困难的事。首先，就计算机病毒的种类而言，一个新种病毒的出现会非常快，而检测出一