Mc Graw Hill Education

计算机病毒揭秘

VIRUSES REVEALED

〔美〕David Harley Robert Slade Urs E.Gattiker 著
朱代祥 贾建勋 史西斌 译

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

计算机病毒揭秘

[美] David Harley　Robert Slade　Urs E.Gattiker　著

朱代祥　贾建勋　史西斌　译

人 民 邮 电 出 版 社

图书在版编目(CIP)数据

计算机病毒揭秘/（美）哈利（Harley,D.）等著；朱代祥，贾建勋，史西斌译.

—北京：人民邮电出版社，2002.9
ISBN 7-115-10448-4

I. 计… II. ①哈…②朱…③贾…④史… III. 计算机病毒—基本知识 IV. TP309.5

中国版本图书馆 CIP 数据核字(2002)第 051396 号

计算机病毒揭秘

◆ 著 [美] David Harley Robert Slade Urs E.Gattiker
译 朱代祥 贾建勋 史西斌
责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www. ptpress.com.cn
读者热线 010-67132705
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：27
字数：689 千字 2002 年 9 月第 1 版
印数：1-4 000 册 2002 年 9 月北京第 1 次印刷

著作权合同登记 图字：01 - 2002 - 0390 号
ISBN 7-115-10448-4/TP・2970

定价：48.00 元

本书如有印装质量问题，请与本社联系 电话：(010)67129223

内 容 提 要

本书是计算机病毒方面的百科全书，涉及了关于计算机病毒的方方面面的知识，包括：计算机病毒实现技术、病毒的防范、病毒案例分析及计算机病毒的社会问题等等。本书的几位作者是计算机安全及病毒方面的专家，书中提出的大量忠告和建议无论对普通计算机用户还是计算机专业人员都是非常有益的。

本书实用性和可读性强，适合于广大计算机用户、系统管理人员、计算机安全专业人员。

致　谢

还有太多的人未被列举出来，而他们都是我们所要感谢的。特别地，我们必须提到我们的家人，在这项长期而苛刻的事业中，他们给予了耐心的支持。

我们感谢许多人的工作，他们是 Virus Bulletin、AVIEN、EICAR、ICSA 实验室、WildList 组织、Hamburg 大学、Tampere 大学和曼登堡大学，以及 anti-virus (AV)公司，感谢你们的专家意见、你们的帮助，感谢你们耐心地接收我们的电话。我们无法列举出所有应被提及的人们，但任何一张这样的清单，应该包括的还有那些对此书做出了间接贡献的人们，如果没有他们的艰苦工作和无私慷慨地共享的信息，我们的工作将会更为艰难。在此我们只列出一小部分，并没有特别的顺序：Alan Solomon、Paul Ducklin、Vesselin Bontchev、Jimmy Kuo、Sarah Gordon、Robert Vibert、Henri Delger、Joe Wells、Larry Bridwell、Bruce Burrell、Shane Coursen、Nick FitzGerald 以及 Graham Cluley。我们同样感谢 Rob Rosenberger 和 George Smith，感谢他们出色的保密工作；感谢那些病毒作者和前病毒作者，他们认为值得对此问题展开对话和讨论；感谢那些来自 VIRUS-L、alt.comp.virus、alt.comp.antivirus、安全中心以及别的地方的志愿者们。他们一直都在提供许多人需要的帮助和建议。虽然有时候我们也会有分歧，但他们热心公益的精神使一切变得如此的非同凡响。

一本书终究是团体努力的结果。本书也不例外——很幸运，虽然在创作阶段出现了各种困难。许多人在荣誉面前是当之无愧的：Urs，是他首先着手开始这项工作的；David，对资料按顺序进行分类；Rob，当疾病以及一场事业和职位的巨变几乎要迫使他完全脱离这项工作时，他坚持了下来；Christine，她的贡献远远超出了技术评论；Spaf，提出了应该提出的意见(就像往常一样)；还有奥斯本这个长期吃苦的工作组，他们为了我们这个由几个过度苛求，甚至有时暴躁易怒的创作人组成的集体做出了不懈的努力；还有 Gloria，她的编辑工作远远超过了妻子的责任。

关于作者

Robert Slade

Rob Slade 是一位数据通信与安全方面的专家，他来自加拿大，不列颠哥伦比亚的凡克佛北部。

当病毒程序只作为一个发生在将来的主要问题而出现的时候，他就开始了对这方面的研究。最初他只是作为刚萌芽的研究团体的非正式案卷保管人，而他开始为人所知是因为“Mr. Slade's lists”。在 VIRUS-L FAQ 的一个工作组中，他写出了一系列评论和指南性的文章，以《Rob Slade 的计算机病毒指南》的形式被发表了。他是 DECUS 加拿大安全 SIG 的建立者。但他仍认为自己是数据安全领域的局外人，所以在听到自己最近被誉为安全社区的“领袖”时，感到十分惊讶。

Rob 由于他的技术书籍的一系列评论而广为人知。如果你不想浏览 USENET 来寻找这些书籍，你可以寻找一张邮寄列表接收其中的信息，或通过 techbooks-suscribe@egroups.com 发送消息，或是访问处于 www.egroups.com/list/techbooks/的 eGroups 网站，那里也有最近的邮寄档案。书籍评论的完全档案在 http://victoria.tc.ca/techrev/mnbk.htm 上的 Victoria Telecommunity 网和北部的伊利诺州大学的计算机秘密文摘(http://sun.soci.niu.edu/~rslade/mnbk.htm)上也有些链接。这些评论源于 TeleManagement 中的一个栏目(www.angustel.ca/teleman/tm.html)。

可以通过 rslade@sprint.ca 或 rslade@vcn.bc.ca 与 Rob Slade 取得联系。

David Harley

David Harley 自 1989 年到 2001 年，他任职于伦敦皇家肿瘤研究基金会，最初是作为一名管理员和程序员，随后是网络工程师和支持分析家，最后是作为一名安全专家。他现作为支持服务部门管理员任职于英国的 NHS 信息局，在这里，他仍对安全进行专门的研究，只不过可以更为自负地表达自己。

他是 EICAR(欧洲计算机防病毒研究所)一个活跃的成员，也是 AVIEN(防病毒信息交换网络)的一个特权成员，在那里他参与了有关防病毒人员和病毒分析认证项目。更不用说，他也参加了学科委员会，其实这远不如听上去那样令人兴奋。

他还加入了其他组织，其中包括 WildList 组织和 ICSA 研究室，在那里他致力于与苹果公司的 Macintosh 相关的安全项目。他还是一个在 Mac 方面有些名气的专家，这在很大程度上是因为除了那些没有国家支持的人以外，没有多少人会对 Mac 感兴趣，他还办了一些关于安全方面的网站(在他有空闲时间的时候)，包括 Mac Virus II。

他以前的安全作品包括了一些 Internet FAQ、会议论文的一个独特分类、发表在杂志上的文章，《Maximum Security》第三版上有关病毒和特洛伊木马的章节，还有《计算机安全手册》第四版上有关安全防护的章节(和 Paul Brusil 合写)。

可以通过 macvirus@dircon.co.uk 和 David Harley 取得联系。

Urs E.Gattiker

Urs Gattiker 是 Aalborg 大学创新与科技管理的 Obel 家庭基金会教授。他曾经任职的机构包括 Stanford 机构研究中心、墨尔本商业学校、莱斯桥大学、Hamburg 的德国联邦军事大学，以及阿赫斯商业学校。他是 KonNet GmbH(德国)监督董事会的一个成员，也是 BI 科技 A/S' IT 创业基金会的银行投资咨询协会(http://www.BankInvest.dk)成员。同时他还是其他许多组织的成员，如 B2B Agro 斯堪的纳维亚 A/S、Naventi A/S、Vigilante 有限公司(美国)以及 Vupti A/S。

他的著作包括《科技管理与组织》(Sage 出版社 1990 年出版)和《多样社区的因特网：文化、组织、政治问题》(Lawrence Erlbaum 出版社 2001 年出版)；目前他正与 Inger Marie Giversen 和 Christine Orshesky 合著《电子病历、因特网和数据安全》(Lawrence Erlbaum)。不久前他与 Laurie Larwood 合编了一本书，《Impact Analysis: How Research Can Enter Application and Make a Difference》。目前他正在写一本有关企业的建立及运行的书。

Gattiker 担任美国管理研究院(美国主要的学术与咨询管理委员会)的科技改革和研究方法部门的主席一职。他是加拿大科技管理协会(CANMOT)——这个协会即现在的加拿大改革管理协会(IMAC)和加拿大行政科学协会的技术管理部门(ASAC)的创始人之一，也是行政官员之一。Gattiker 还是欧洲计算机防病毒研究所(EICAR)的信任和电子商务专门小组的主席，以及 EICAR 的科学顾问委员会和 EICAR 委员会的成员。

目前，他正领导着的病毒研究组织致力于电子商务、新媒体和技术策略的研究。研究报告和白皮书可在 http://Papers.WebUrb.net 上查寻到。

可通过 WebUrs@WebUrb.net 与 Urs Gattiker 取得联系。

关于技术编辑

Christine M.Orshesky 已有 10 年以上的信息安全经验，她一直在为支持信息安全做出努力，其中包括对恶意软件的防护和对各种政府、社团组织的事件响应。她最值得注意的职责包括为五角大楼国防部控制恶意软件。在这次经历之后，Orshesky 建立了电子安全公司，为中立的供应商提供恶意软件保护策略和教育。她参与了众多的信息安全和其他行业的会议，并且获得了信息安全和质量保证的职业认证。

序

David 和 Robert 让我给这本新书写一个序言。多年以来，我一直与他们二位保持着联系，而他们在病毒方面的功劳对我们之中的许多人而言有巨大的价值。在浏览了凝聚他们共同努力的初稿之后，我感到很高兴：他们以如此通俗易懂的方式提供了如此多的有用信息。事实上，本书的综合性之强，使我简直找不出他们没有涉及到的内容。然而，当我对此思考得更为深入时，我认识到，他们没有完全指出即将到来的东西。为了了解未来，联系过去来考虑是有帮助的。因此，我将对过去的一些问题以及它们与现在的联系作一些反思。在此之后，我会向你提出挑战：阅读此书，同时思考，现在会对未来产生一些什么样的预示，还有你的了解和行动会产生怎样一个效应。正如 George Santayana 所写的，“忘记过去的人是会遭到报应的。”(是的，这才是正确的引文，有许多人错误地引用了它)。

12 年前，我和别人合著了第一本关于计算机病毒的通用英文技术参考书(《计算机病毒：与电子破坏和程序威胁的较量》，由 E. H. Spafford、K. A. Heaphy 以及 D. J. Ferbarche 合著，由 ADAPSO(现在是 ITAA)1989 年出版)。当时，在公众领域流行的病毒不超过 100 种——其中大约有 75 种作用于 DOS/Windows，20 种作用于苹果公司的 Macintosh，还有少量作用于包括 Amiga 在内的其他平台。从外界的第一个病毒——1982 年的苹果二代电脑病毒 Elk Cloner——的成长开始，到 1986 年至 1988 年这一段时期，作用于 Intel 平台的病毒增加了 6 种，后来又出现了 IBM 圣诞树 EXEC 蠕虫/病毒，以及其后的 Morris Internet 和 WANK 蠕虫。

直到 2001 年中期，电脑病毒的种类多达成千上万种——也许有 7.5 万种以上。一些供应商声称每周收到多达 20 种的病毒报告。事实上，随着制造热门电子邮件和文字处理软件宏病毒变得日益简单，关于新病毒的报告也日益增多。如果将各种蠕虫、特洛伊木马、后门程序以及其他恶意信息也算作病毒，这个数字会增长得更为庞大。

如果你对历史数据稍稍做一番分析，用一些统计工具就可以反映出前 20 年的趋势。在几年之内，我们将看到，一种蠕虫或病毒的出现速度会超过曾有的每小时一种的记录。谁能赶上这种攻击的速度？我们要采取什么样的防御措施？还有，我们要有多大的处理力量才能得到足够的保护？

实在不必如此。

在 20 世纪 80 年代，Fred Cohen 对电脑病毒作了广义的描述，但似乎只有少数人给予了关注。后来 Harold Highland 在社论《计算机与安全》和其他的关于病毒的文章里，都注意到了这个问题。当时在我与别人合著的书及其参考中，对计算机病毒和未来潜在的问题提出了警告。在许多会议和专题讨论会上，我们讨论电脑病毒和恶意信息的未来。在 1990 年和 1991 年，Harold 和我都出席了 NYC DPMA 病毒会议(当时病毒研究的首要会议)，这个会议主要是讨论宏病毒以及它们的潜在问题——这些都是发生在病毒这个概念出现之前。

尽管如此，几个主要的软件供应商都没能到会，更没有阅读任何关于安全的出版物。供应商告诉研究人员们，他们不关心病毒，因为当时他们只有少数顾客在这方面存在问题。

特别地，有一个大公司对此尤为不在乎，而它今天招致的痛苦结果是明显的。例如，这个公司不顾反对，将使病毒更容易传播的特征设计进程序。正是这一个公司，把首个专业宏病毒标为一个“玩笑”，而且从未找出编写这个程序的雇员或是对其做出惩戒。你能猜到这是哪个公司吗？这里有个提示：所有已知的计算机病毒和蠕虫中99%只在他们的产品中运行，超过了他们在市场上实际份额的比例。这里还有另一个提示：梅丽莎(Melissa)和爱虫 LoveBug 事件影响了此公司，并造成了几十亿美元的损失，与影响巨大的 1987 年圣诞树 EXEC 事件在本质上几乎是相同的。今天的问题只会使那些忘记历史的人——或从不愿麻烦自己去吸取教训的人感到惊讶。

不幸的是，运行在我们的国防、基础公用事业和政府机构中，支持我们的银行、医药机构和教育组织的主导软件系统也是出自同一个公司。这使我们的整个计算基础设施面对恶意软件显得非常脆弱，再加上那些产品对计算机病毒的易感染性，它们似乎没完没了地需要弥补关键的安全问题的补丁。这些问题中，有许多是由几十年来已知的有安全问题的编码造成的(例如缓冲区溢出)。在这个领域中，只要有一个网页浏览器和一个文本编辑器，一个 12 岁的小孩就能运行自我复制的软件执行网络攻击脚本——可破坏一个政府机构或跨国公司的软件。如果本星期 Web 站点没有一些攻击软件，那么一个攻击者所有要做的只是花上几个星期等待或发现更多的可利用的漏洞及可以对其做出的攻击。

还记得中美洲的阿兹特克人吗？他们当时统治着一个强大的帝国，但是几百个西班牙人带来的天花和麻疹使他们 90%的人口丧失了行动能力或死亡，其国家也弱小得无法抵御异族的征服。没有了免疫力，他们很容易就被极其小(而且弱小)的力量所吞并。你认为我们从过去能吸取些什么教训？

当然，这并不只是软件供应商的错。消费者们没有要求更过硬的质量，没有作出明智的选择，没有认为供应商应该为次品负责，这样，供应商为消费者提供了他们想要的东西，他们在购买时毫无怨言，所以很难为此(完全)去指责前者。今天，许多计算机用户已经习惯性地接受了每天都出现的电脑病毒，系统崩溃和安全漏洞。他们不知道可以有其他的替换方案，要不就是觉得改换为其他方式的代价太高。尽管如此，不久之后，防病毒软件、安全软件、恢复工作、事件响应和桌面帮助上的花费将会超过它们连接的系统所用的花费。但这又怎样呢？

还存在的一个问题是，我们没有惩罚恶意软件的作者做有效的措施。自 1980 年起，据我所知，在单独的恶意软件犯罪案中，被控告和定罪的人不超过 10 个。我只知道两桩关于破坏的民事案例。从病毒作者给出的态度(见第 15 章)来看，我们有什么能威慑他们的力量呢？如果没有一些权威去揭露和惩罚他们，我们是无法减少病毒作者的数量的。事实上，随着更多计算机连接入网络，获得工具变得更容易，加上一部分人仍然认为病毒只是“正常现象”，也许病毒作者的数量还会保持增长，甚至其速度会快得超过现在。

所以，我们拥有一个对病毒非常易感染的环境，这无论对于认为安全只是个历史性的、次要的问题的供应商(要是它曾经被关心过就好了)，习惯于这种可悲境遇的消费者，还是对于并不真正害怕报复的行凶者都是一样的。防病毒软件供应商正在获利是一个奇迹吗？或者必须获利吗？

不管发生了什么，我不相信未来就该像过去一样。我们每个人都可以创造不一样的未来，我们可以从改正自身的行为开始。

- 如果 10%的人停止接收携带恶意软件的电子邮件附件(与宏相关的或其他的)，或许那些人就会停止这种邮件的发送。这可以截断或至少减少一种普遍的传输方式。
- 如果每一个新的威胁出现时，我们都确切地定义它，而非一律地称之为“电脑病毒”，或许用户会给予更多的注意。

- 如果我们停用三四个广为使用的应用软件，那么当下一次的漏洞被发现或病毒发作时，也许将不再看见能够威胁大多数使用者的恶意软件了。
- 如果有 1/5 的使用者会因为安全因素而不选开销去评估选择平台，也许我们会考虑更多的以安全为设计目的的选择。

军队离不开骑兵是因为他们在缰绳、马厩方面做出了投资，而在 20 世纪上半叶，当坦克和火枪被广泛使用时，军事训练的观念彻底地改变了。一个对一般的安全威胁有免疫能力的平台，即使它需要更多的花费并且要经过一些附加训练才能掌握，仍然具有在任何市场上竞争的优势。

所以，当你从头到尾阅读本书中由这些资深研究人员介绍的所有的历史和他们提出的忠告时，请注意关于如何设计你自己的防护的建议，规划好未来。做一个记住历史且确实从他人的教训中吸取经验的人，下定决心去开创一个全新的未来吧。

为了所有计算机的安全。

——Spaf

2001 年 7 月

Eugene H. Spafford 是 Purdue 大学的计算机科学教授、哲学教授，也是普渡大学的教育研究信息保障与安全中心(CERIAS)的主任。CERIAS 是一个校园多学科中心，它受到广泛关注的任务是探索有关信息保护、信息资源的问题。对于信息安全、软件工程和职业道德，Spaf 已讲述得十分全面。

Spafford 是美国计算机协会(ACM)的成员、美国科学进步协会(AAAS)的成员、电器电子工程师协会(IEEE)的成员，还是计算机协会 Golden Core 奖得主。在 2000 年，他被授予 CISSP 的称号。在他参加的许多活动中，他担任了 ACM 的美国公共政策协会副主席、计算研究协会的主任董事会成员，以及美国空军科学顾问董事会成员。他是国家标准和技术研究所/国家标准和认证中心(NIST/NCSC)的 2000 年国家计算机系统安全奖的得主，通常此奖被认为是此领域内在信息安全研究方面的最高荣誉。在 2001 年，他又成为 Charles B. Murphy 奖——Purdue 大学为杰出的大学生教学所设的最高奖——的得主之一。由于他的名望，他被推选进入信息系统安全协会(ISSA)，并且由于他在信息研究和教育方面所做出的贡献，他被授予 William Hugh Murray 奖，这块奖牌是国家学术讨论会为信息系统安全教育而设的。

前　言

我们为何写本书

我们想要提供高质量的可广泛使用的信息，有关一般的恶意软件、独特的病毒以及防病毒/防恶意软件技术及其在现实世界和一般安全相联系的应用。我们还想做出保证，我们涵盖了当今绝大多数病毒和恶意软件的发展趋向，这些病毒和恶意软件在最近的几年中，已经引人注目地从传统形式之中脱离出来了。最后，虽然本书主要面向系统管理员和 IT 经理，但我们也想使这本书同样适用于那些在这个领域没有做过专门研究的计算机用户。

也许，更为紧迫的是，我们想要反对那些极其卑鄙的信息，它们烦扰着整个安全领域和特殊病毒领域。到此为止，我们所做的不仅涉及到威胁和对策的分析，还有对那些源自更深信息的信息，评估其可靠性。

为什么本书与众不同

本书不同于大多数的安全著作。许多关于安全的册子对于安全的其他领域的信息介绍准确，但在病毒细微问题上并非如此。

一般的安全书籍也常常倾向于全揭露的模式，而对于一本病毒书籍来说这样做并不是十分恰当。我们并非一定要鼓吹家长主义，表现一些防病毒工业某些部门特色的“上帝和蚂蚁”思考模式，他们总是倾向于不揭露连续统一体的最终关系。我们希望你尽可能地对我们所说的进行检验，并下定决心去做。但是病毒文献中最重点揭露的问题显然是涉及到病毒的实际代码。

在我们看来，早期的病毒书籍或是其他书籍中对病毒代码(存在的或新的)不加选择地加以评述，以致于它对那些积极的病毒作者的帮助超过了对压力重重的系统主管们的帮助。正如 Gene Spafford 的一句名言：向人们显示如何把糖倒入玻璃容器并不能教会他们多少技巧性的东西。为了对病毒进行防护，你必须懂得一点病毒的运作，但这与病毒编码的更多的细节是完全无关的，所以我们不会公布病毒代码(那些病毒源代码也不会被涉及)。

除了在一些十分小心控制的环境中，自定义病毒一般是有害的。我们不能说不存在好意的研究者曾修改或制造过一种病毒，借此来测试一个概念(虽然一些技艺高超的人在任何环境下都不会这么做，而一些公司也无力去阻止)。不过，公布可行的病毒代码并不是我们想使用的方法。

对单个的病毒的分析并不会教给你防卫所有病毒的方法。你所要知道的必须不仅限于病毒的破坏，否则你就无法最有效地实施你的对策。然而，我们希望即使你确信这些防病毒措施已足够也不要放下这本书，但多数的读者仍会严重依赖于商业解决方案。我们觉得，关注解决方案的评估和实施细节，要比关注成千上万个病毒及其变体的一小部分细节有用得多。如果我们的注意力确实集中在特定的病毒上，那么我们就会更关心它们在已成为事实的社会影响和防御措施方面所

体现的重要性，而非它们代码的细节问题。

尽管如此，为了让你理解这是什么样的威胁，我们会告诉你足够的病毒机制，以及更重要的，商业防病毒软件是如何抵抗它的。此外，不像大多数供应商手册和 Web 网站，我们会告诉你防病毒软件无法弥补的一些问题。病毒作者已经直接或间接地利用了这一点，而如果要使你得到最大限度的安全，你也必须对此有所了解。

防病毒软件是一个有相当大的局限性的选择：系统主管和家庭用户也许能够阻挡某种程度的威胁，但在检测和杀灭成千上万个截然不同的已知病毒时，就无法和专业人员相比了。我们知道一些兜售书籍的伎俩，他们说："假如你读了本书，你就能写自己的防病毒软件，而且安全供应商也将为了要雇佣你而排起长队。"这个说法是荒谬的。你可以填补一些商业防病毒软件留下的空缺；你可以避免使用脆弱的操作系统、应用程序和实用程序或是配置，以此来绕过对商业产品的需求；你可以(以某个价格)使用普通防御，例如改变检测软件，但你不能在发现新病毒时就对其进行定义。你无法在检测已知病毒方面与工业界做竞争，因为这是他们的专项，而你没有时间或办法来应付每种新病毒。

难道病毒管理不是个安全问题吗？当然，它是，而且在某些人手中，它在整体安全战略范围之内得到了最好的执行，这些人对病毒的了解可与他们对其他安全领域的了解相匹敌，甚至有过之而无不及。但很不幸的是，有些人在某些安全领域能够胜任，但有时在其他领域却高估了自己的能力，而有些病毒似乎造成了一种特殊的 ultracrepidarianism(对自己的能力或知识范围以外的事物作出评论或行动)的极有害现象(这对于 Rob Rosenberger 来说正是轻车熟路，他在"假权威征候群"上的文章中首先详细介绍了我们中至少一位；你可以在 www.vmyths.com/fas/fas1.cfm 上找到此文)。当然，这个原理同样适用于其他方面。例如，不管一个防病毒供应商说他的产品有多好，只有最大胆、最神经质或最没经验的系统主管有可能会让供应商来编写他或她的防火墙策略。

Ultracrepidarianism

这个术语源于拉丁语 ultra crepidem(不属于鞋底)。故事是这样的，有个皮匠对 Apelles —— 古希腊的一个画家 —— 在一幅画中对人像的刻画提出批评。Apelles 在人物的拖鞋方面接受了批评，但考虑到对腿的表现手法已超出了鞋匠的专项，所以没有接受这方面的建议。这故事为什么出现在拉丁语而非希腊语中，尚不是很清楚。

本书与其他病毒书籍也有一些差别。毕竟，不是已经有了足够的病毒书籍了吗？是的，已有许多好的病毒书籍，还有最新出的，而且在这个项目一开始，它们就已经是分散的体系了。但很不幸，最正确的书籍往往不是最新的，因此，他们遗漏了从一开始就与我们有关的一些问题。同时，大多数的流行书籍都不准确，但有一两本例外，本书中都对其有记录。不将这个记录放在这里是因为我们想让你购买这一本书……

我们也没有认为这里已包括了你所想知道的一切，但我们已尽可能地使它及时、准确而且易懂，而它本身也使之有其独到之处。只是为了确保我们没有食言，在第 19 章末尾，我们收录了有关热门问题的信息，它们是在我们正在完成最后几章时出现的。届时敬请留意。

谁适合使用本书

在所针对的读者方面，本书也有所不同。针对需要知道病毒管理的信息技术(IT)专业人员的书籍明显不足。这个群体也许包括了系统和网络管理员、安全分析家和专业的防病毒工程师，以

及其他支持工程师、动力用户、管理阶层、计算机出版界，甚至计算机学科的学生。尽管如此，本书对技术知识水平几乎不做假设（虽然已假设你使用计算机）。家庭计算机用户或社团组织内的非专家们也能理解本书，并能根据他们的需求而受益。在与病毒横行的战斗中，教育是一个举足轻重的组成部分。我们希望技术管理者能够将本书（已对适当的章节做了标记）交给普通的办事处人员或执行人员，并让他们对一些特殊的主题提出见解。

本书并不打算面对专业内部的防病毒专家：全职、能力高超的研究人员和病毒分析专家，这些人并不需要我们在他们自己职业的技术细节上进行灌输。另一方面，与防病毒销售工作人员和 marketroid 的交谈使我们确信，关于某种产品的知识并不能代替病毒和防病毒技术产品的知识。通常，这些人甚至不知道他们只是在销售他们的产品不是你需要的东西，而且他们的销售进度建立在吹嘘上的成分与建立在事实上的成分同样多。（问：一个电脑推销员和一个旧车推销员有什么区别？答：一个汽车推销员会驾驶，并知道他或她在何处对你撒了谎。）此外，我们可以想想一些高度权威的防病毒研究人员，他们所学的技术知识只是病毒管理的一部分。如果我们不能从供应商信息提供者处得到正确答案，我们至少可以希望，一旦你阅读了本书，你可以更好地武装起来，去评估他们的专业技术。

声明四下响起："相信我：我是供应商"或是"信任我：我是顾问"，甚至"相信我：我是即时专家"，这和"相信我：我是一个病毒作者"同样地无意义。我们不想让你相信任何人(包括我们)所声称的，或那些声称他们所知道的东西。有太多的人想要为你减轻你在病毒问题上的所有责任。我们想要使你强大起来，至少在病毒管理方面能做出一个自己的决定。如果这个决定是雇用他人来解决此问题，那么，至少是根据你的知识基础做出这个决定，而不是(你自己的或他们的)无根据的妄想。

很清楚，本书也不是写给病毒作者的。我们已经解释过，我们不愿引用某些类型的代码，所以，本书对于一些想对已存在的代码做一些小小的改动并以此制造变体病毒的作者无多大用处。是的，我们知道有许多合法而有益的代码，它们建立在别的代码的基础上。尽管如此，根据我们的经验：

- 病毒代码通常不合法且无益处。
- 许多病毒变体只是对原病毒做了很小的改动(例如对文本行的一个不重要的修改)，它们除了可以让作者表明其著作权，再也没有别的作用了。

也许一个病毒作者会从这里提到的一些东西中抓住一个一闪而过的念头，并使其发展为令人吃惊的输出编辑语言，而且这可能也是恶意的。这也是安全领域内所有作者所要冒的风险。我们可以做出尝试，不发表只对那些坏家伙有用的东西，可是大多数技术信息的价值都是双方面的，它对你有用，也可能对你的敌人同样有用。我们所举的例子都只是根据其价值来选择的。

有时，反病毒研究人员会在下班后玩一些游戏(通常在安全会议上)，例如检测彼此的帮助路径或者交流噩梦情节。通常，我们只打算把我们的噩梦留给我们自己，除非现在你就能对它们做点什么。

本书构架

本书分为五大部分，如下所示。

第一部分：问题

恶意软件有许多形式，而我们要对付的几乎是其全部的形式。然而，单个的恶意软件实例并

不一定或是不经常被单独地处理。尽管我们有时说特殊问题要特殊解决，但一般我们只研究较普通的恶意软件，之后(在第二部分中)防范此类恶意软件的技术可被用来对付它们。

我们想让本书对大部分的电脑用户有用，其中包括(事实上，特别地)高级电脑学者。然而，经验指出，在计算机使用的一个领域中——包括安全(或系统管理和安全)——认为这就是专家的意见是不安全的，这是在防病毒问题上必须指出的专业知识。我们以一些基本定义作为开端，只是为了确保我们讨论一些关键概念如特洛伊木马、病毒、蠕虫、破坏和感染时，都能对相同的东西有个大概的理解。如果你熟悉关于这个主题的一些老书和其他资料，那么这些材料对你来说不会都是新的。尽管如此，在第一部分中，我们的确以考虑旧有威胁的方式反映了最近的趋势，此趋势也许在它自己的权限中比较感兴趣。当然，我们会将注意力集中在当前的威胁和威胁级别中。既然它们在第一批经典文本中已经存在，而且在最新的书籍中通常都示范其对技术及其含义的粗浅理解，因此这里不再包含，它们可能会有某种特殊的重要性。在随后的章节里会有对恶意软件集合及其子集的具体分析，而在第三部分会有关于恶意软件是否对个人有益的详细调查。

第二部分：系统解决方案

第二部分详细地介绍了防病毒和防恶意软件技术，随后继续讨论它们在公司中的实际应用。

第三部分：案例研究

在第三部分中，我们提供了对一些特殊病毒或恶意软件事件的仔细研究，这些研究由于病毒带来的后果而很值得引起我们的注意，并且能使我们从中吸取教训。

第四部分：社会方面

第四部分面向社会问题。我们相信，病毒是一个社会问题，而依靠纯技术手段是无法解决社会问题的。悲哀的是，解决社会问题所需要的知识已经超出了本书的范围，在这个范围中，计算机破坏行为只是一个小小的组成部分而已。当然，病毒管理专业人员也不能忽视人性的空间的问题，无论它是否涉及到破坏者本身或他们的受害者。第四部分也包括了摘要的概述以及“最新消息”部分。

第五部分：附录及术语表

最后的一部分包括一个详细的术语表和一些由作者和其他人给出的附加材料。

更多的信息

本书有相当大的阅读量，包含一些在系统保护中执行的工作建议。本书不会使你成为一个顶级的防病毒专家，但如果那是你的理想，读通这本书肯定会给你一个适当的基础，并涉及到足够深入的信息，使你能在数年之内保持前进。你也许会习惯那些带一张充满了免费软件和文件的 CD 的书籍，但这对反病毒软件来说不会很有用，因为等到那本书被拿来出售时，许多程序就已经过时了。我们的经验指出，制造一种可评估的防病毒软件，事实上由于它超过了软件的期限，变得越来越难。此外，既然我们毫不犹豫地推荐了一些免费软件和共享软件，也许给你一些对于流行版本和信息的提示会更好。如果有一个动态信息源，我们可以做得更好——即网站——好过一张可能会在新闻的日期和书籍的出版中过期的 CD。我们特别提到免费软件，在第 8 章中和以下站点的网页上都可以找到：

http://victoria.tc.ca/techrev/vrfresft.htm

http://sun.soci.niu.edu/~rslade/vrfresft.htm

你也可以在以下站点查找更新的网页链接：

http://www.osborne.com/errata/errata.shtml

http://www.viruses-revealed.org.uk/

我们希望这些网站将使你足够安全，那么你就还会读完本书的余下部分。

目　录

第一部分　问　题