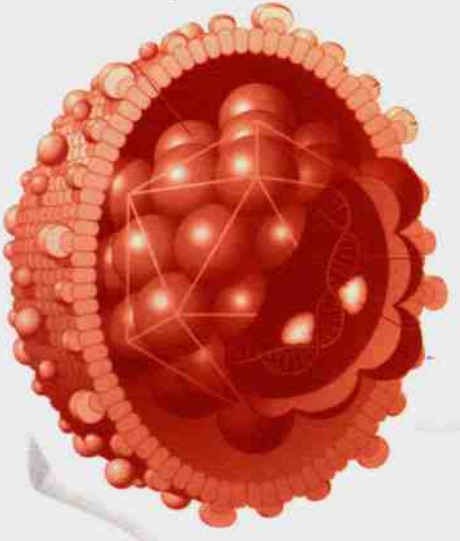
Broadview
www.broadview.com.cn

信息安全领域多年经验的总结和提炼！

安全技术大系

计算机病毒分析与防范大全

韩筱卿 王建锋 钟 玮 等编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

计算机病毒分析与防范大全

韩筱卿 王建锋 钟 玮 等编著

内 容 简 介

本书是作者在信息安全领域多年经验的总结和提炼。本书从计算机病毒的定义及特征开始，将目前发现的所有计算机病毒加以分类，总结出每一类病毒的共性和特征，提出具有针对性的防范建议，以便普通读者揭开病毒的神秘面纱，构建自己的防范体系。

本书适合计算机安全领域的从业者及爱好者阅读，对计算机普通用户更深入地了解计算机病毒也有莫大的帮助。

图书在版编目（CIP）数据

计算机病毒分析与防范大全 / 韩筱卿，王建锋，钟玮等编著．—北京：电子工业出版社，2006.3
（安全技术大系）
ISBN 7-121-02157-9

Ⅰ．计… Ⅱ．①韩… ②王… ③钟… Ⅲ．计算机病毒－防治 Ⅳ．TP309 5

中国版本图书馆 CIP 数据核字（2005）第 152779 号

责任编辑：朱沐红 zsh@phei.com cn
印　　刷：北京智力达印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×980　1/16　印张：32　字数：800 千字
印　　次：2006 年 3 月第 1 次印刷
印　　数：4000 册　　定价：59.00 元（含光盘 1 张）

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

作者简介

韩筱卿，1971 年生，现任北京瑞星公司客户服务总经理。从 1995 年开始涉足计算机反病毒技术研究领域；1997 年，参与开发的瑞星杀毒软件第一代产品获中国国家科委（现科技部）国家科技成果奖；参与了 CIH 病毒、BO 黑客、红色代码、尼姆达、Happy Time 等多种典型流行病毒的解决处理过程。2000 年组织筹备成立了瑞星数据修复中心，经过多年的发展，使之成为计算机用户数据灾难恢复的首选之地。先后在清华大学、北京大学、北京理工大学、北京航空航天大学、上海同济大学、四川科技大学等多所高校做关于计算机反病毒技术的专题报告。

王建锋，1971 年生，现任北京瑞星公司客户服务副总经理。多年来一直从事反病毒技术研究及技术支持工作。2000 年以来，主要负责重大恶性计算机病毒的应急处理工作，组织并参与创建瑞星客户服务中心呼叫中心系统及计算机病毒应急处理平台，在新型病毒预警、分析以及反病毒策略研究等领域具有丰富的经验。

钟玮，1976 年生，现任北京瑞星公司数据安全部经理，全面负责信息安全增值服务的管理与拓展工作。2002 年以来，参与国务院新闻办、港澳办、中组部、华远集团等国内 20 余家政府部门及大型企业信息安全整体解决方案及安全外包方案的制定与实施；为中粮集团、中央电视台、微软公司、国务院中直管理局、联合国驻京机构等 30 余家重点单位长期提供数据安全、数据恢复咨询及数据安全管理项目实施；多次组织并参与信息产业部电子教育中心、清华大学、中科院计算所等国内权威机构信息安全培训项目的实施，具有丰富的信息安全项目实践经验。

序

计算机病毒是一个社会性的问题，仅靠信息安全厂商研发的安全产品而没有全社会的配合，是无法有效地建立信息安全体系的。因此，面向全社会普及计算机病毒的基础知识，增强大家的病毒防范意识，“全民皆兵”并配合适当的反病毒工具，才能真正地做到防患于未然。我们很高兴地看到战斗在反病毒领域第一线的专业人士，将自己多年的反病毒经验加以总结，与大家共享，帮助普通的计算机使用者揭开计算机病毒的神秘面纱，这无疑是一件有利于促进信息化发展的好事情。

这本书实用性比较强，较为全面地介绍了计算机病毒的基本知识，分析了典型病毒的特征，很适合初中级水平的计算机使用者参考。希望这本书的发行，能够在普及计算机防病毒知识方面发挥积极的作用，并根据实际情况不断更新，将最新的技术和发展趋势带给广大的读者。

瑞星公司董事长

王苹

2005 年 11 月于北京

写在前面

提起计算机病毒，绝大多数计算机的使用者都会深恶痛绝，因为没有“中过招”的人已经是凤毛麟角了。但在谈虎色变之余，很多人对计算机病毒又充满了好奇，对病毒的制造者既痛恨又敬畏。这种复杂的感情实际上很容易理解，就像古人面对大自然的感情一样，因为无法解释风雨雷电，也就只能制造神话，崇拜图腾了。

计算机病毒当然不值得崇拜，它给社会信息化的发展制造了太多的麻烦，每年因为计算机病毒造成的直接、间接经济损失都超过百亿美元。但同时，它也催化了一个新兴的产业——信息安全产业。反病毒软件、防火墙、入侵检测系统、网络隔离、数据恢复技术……这一根根救命稻草，使很多企业和个人用户免遭侵害，在很大程度上缓解了计算机病毒造成的巨大破坏，同时，越来越多的企业加入到信息安全领域，同层出不穷的黑客和病毒制造者做着顽强的斗争。

但稻草毕竟是稻草，救得一时不一定救得一世。目前市场上主流厂商的信息安全产品经过多年的积累和精心的研发，无论从产品线还是从技术角度来讲，都已经达到了相当完善的程度。但是，再好的产品，如果不懂得如何去使用，发挥不了产品真正的优势，又与稻草有什么区别呢？很多用户在被病毒感染以后才想起购买杀毒软件，查杀以后就再也不管，没有定期的升级和维护，更没有根据自己的使用环境的特点，制定相应的防范策略，可以说把产品的使用效率降到了最低，这样的状态，怎能应付日新月异的病毒攻击呢？

那么，如何将手中的稻草变成强大的武器，当危险临近时，能够主动出击，防患于未然呢？笔者认为，关键的问题在于对“对手”的了解。正如我们上面举过的例子，我们现在之所以对

很多自然现象习以为常，是因为我们对其成因有了最基础的了解，这样才可能未雨绸缪，配合手中的工具，防患于未然。

本书的创作初衷正是将笔者在信息安全领域多年的经验加以总结、提炼，从计算机病毒的定义及特征开始讲起，将病毒的起源、发展历史、发展趋势及造成的危害系统而全面地介绍给读者，并将目前发现的所有计算机病毒加以分类，总结出每一类病毒的共性和特征，提出具有针对性的防范建议，以便于普通读者揭开病毒的神秘面纱，构建自己的防范体系。同时，本书还根据杀毒软件行业的特点，以专业的视角介绍了反病毒行业病毒分析的流程，帮助读者构建自己的病毒分析实验室，从而对计算机病毒进行彻底的剖析。此外，为了更好地将书中提到的知识和技能运用到实践中，我们还特别地为初学者设计了非常实用的小实验，并对实验过程进行了必要的演示，以帮助大家更好地理解计算机病毒的原理。

魔高一尺，道高一丈。我们相信，只要知己知彼，我们一定会在与计算机病毒进行的这场持久战中取得最终的胜利！

读者交流信箱：AntiVR@hotmail.com

作　者

2005 年 12 月 8 日

病毒防范实验演示说明

为了使广大读者更好地理解本书的内容，了解计算机病毒的感染和发作原理，作者特意准备了几个比较实用的小实验，并录制了实验内容和实验步骤，供读者参考（见光盘）。

由于实验中有部分代码具有一定的危险性，为了避免初学者操作失误，故将代码部分隐去，详细实验步骤和实验效果请见病毒防范演示中的相应内容。

读者在观看演示过程中，单击“▶”按钮播放录像，单击“⏸”按钮暂停播放，再次单击“⏸”键时继续播放，单击“■”按钮或按键盘“ESC”键停止播放，并退出演示屏幕。单击“定位”菜单可以看到录像的每一帧画面。

目　录

第一篇　认识计算机病毒

第二篇 计算机病毒分析

第三篇 反病毒技术

第四篇 反病毒产品及解决方案

第一篇
认识计算机病毒

CHAPTER 1

第 1 章　什么是计算机病毒

1.1　计算机病毒的定义

我们知道，生物界的“病毒”（Virus）是一种没有细胞结构、只有由蛋白质的外壳和被包裹着的一小段遗传物质两部分组成的比细菌还要小的病原体生物。如 H5N1、O-157 大肠杆菌、HIV（艾滋病毒）、口蹄疫病毒、狂犬病毒、天花病毒、肺结核病毒、禽流感病毒、埃博拉病毒等。绝大多数病毒只有在电子显微镜下才能看得到，而且不能独立生存，必须寄生在其他生物的活细胞里才能生存。由于病毒利用寄主细胞的营养生长和繁殖后代，因此给寄主生物造成极大的危害。在人类或动物的传染性疾病中，有许多是由病毒感染引起的，如人类所患的病毒性肝炎、流行性感冒、艾滋病、脊髓灰质炎、SARS 等疾病，动物中的猪瘟、鸡瘟、牛瘟等瘟疫。

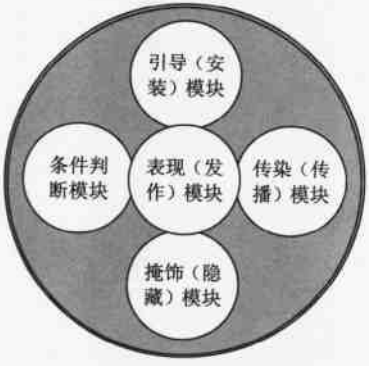


图 1-1　计算机病毒的结构

我们通常所说的“计算机病毒”（Computer Virus），实际上应该被称做“为达到特殊目的而制作和传播的计算机代码或程序”，或者被称为“恶意代码”。这些程序之所以被称做病毒，主要是由于它们与生物医学上的病毒有着很多的相同点（如图 1-1 所示）。例如，它们都具有寄生性、传染性和破坏性，有些恶意代码会像生物病毒隐藏和寄生在其他生物细胞中那样寄生在计算机用户的正常文件中，而且会伺机发作，并大量地复制病毒体，感染本机的其他文件和网络中的计算机。而且绝大多数的恶意代码都会对人类社会生活造成不利的影响，造成的经济损失数以亿计。由此可见，“计算机病毒”这一名词是由生物医学上的病毒概念引申而来的。与生物病毒不同的是，计算机病毒并不是天然存在的，它们是别有用心的人利用计算机软、硬件所固有的安全上的缺陷有目的地编制而成的。

从广义上讲，凡是人为编制的，干扰计算机正常运行并造成计算机软硬件故障，甚至破坏计算机数据的可自我复制的计算机程序或指令集合都是计算机病毒。依据此定义，诸如逻辑炸弹、蠕虫、木马程序等均可称为计算机病毒。按照目前信息安全领域的普遍观点，我们可以总结出计算机病毒

的十大特征，即非法性、隐蔽性、潜伏性、触发性、表现性、破坏性、传染性、针对性、变异性及不可预见性。为了使读者进一步了解计算机病毒，我们将在下一节对计算机病毒的十大特征进行详细论述。

需要指出的是，单独根据以上某一个特征是不能判断某个程序是否是病毒的。拿“破坏性”来讲，例如 DOS 操作系统中的“Format”程序，虽然能消除磁盘上数据，造成对数据的破坏，但它显然不是病毒，因为它除了不具备病毒的传染性这个根本特征以外，也不具有其他大部分特征。

在 1994 年中华人民共和国国务院颁布的《中华人民共和国计算机信息系统安全保护条例》中，计算机病毒被明确定义为：“指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。

1.2　计算机病毒的特征

1. 非法性

正常情况下，计算机用户调用执行一个合法程序时，把系统控制权交给这个程序，并给其分配相应的系统资源，如内存，从而使之能够运行以达到用户的目的，程序执行的过程对用户是透明和可知的，因此，这种程序是“合法”的。

而计算机病毒是非法程序，计算机用户不会明知是病毒程序而故意去执行它。但由于计算机病毒具有正常程序的一切特性，它会将自己隐藏在合法的程序或数据中，当用户运行正常合法程序时，病毒伺机窃取到系统的控制权，得以抢先运行，然而此时用户还认为在执行正常程序。由此可见，病毒的行为都是在未获得计算机用户的允许下“悄悄地”进行的，而病毒所进行的操作，绝大多数都是违背用户意愿和利益的。从这种意义上来讲，计算机病毒具有“非法性”。

例如我们将在第 6 章讲到的木马病毒，有些木马病毒会将自己加载到启动项中，用户每一次启动计算机或运行某些常用程序时都会“顺便”激活病毒，一般的计算机使用者很难察觉。

2. 隐藏性

隐藏性是计算机病毒最基本的特征，正像我们上面讲到的，计算机病毒是“非法”的程序，不可能正大光明地运行。换句话说，如果计算机病毒不具备隐藏性，也就失去了“生命力”，从而也就不能达到其传播和破坏的目的。另一方面，经过伪装的病毒还可能被用户当做正常的程序而运行，这也是病毒触发的一种手段。

从病毒程序本身来讲，计算机病毒是一种具有很高编程技巧、短小精悍的可执行程序。一般只有几百字节或几千字节，而 PC 机对 DOS 文件的存取速度可达每秒几百千字节以上，所以病毒转瞬之间便可将这短短的几百字节附着到正常程序之中，使之非常不易被察觉，从而更好地隐藏自己。

从病毒隐藏的位置来看，有些病毒将自己隐藏在磁盘上标为坏簇的扇区中，以及一些空闲概率较大的扇区中；也有个别的病毒以隐含文件的形式出现；还有一种比较常见的隐藏方式是将病毒文件放在 Windows 等系统目录下，并将文件命名为类似 Windows 系统文件的名称，使对计算机操作系统不熟悉的人不敢轻易删除它。

不同类型的病毒的隐藏方式也是多种多样的。引导型病毒通常将自己隐藏在引导扇区中，在系统启动前就发作。一些蠕虫病毒非常注重隐藏和伪装自己，它们不但伪造邮件的主题和正文，利用