



信息安全技术与教材系列丛书

011000100100110101011001110011100011
110100100100110111010100111000110110
0110011001100110 10010101010101001011
1101111010100110 10101011010110100100
01010101010010010010010010101010101

计算机病毒 分析与对抗

傅建明 彭国军 张焕国 / 编著



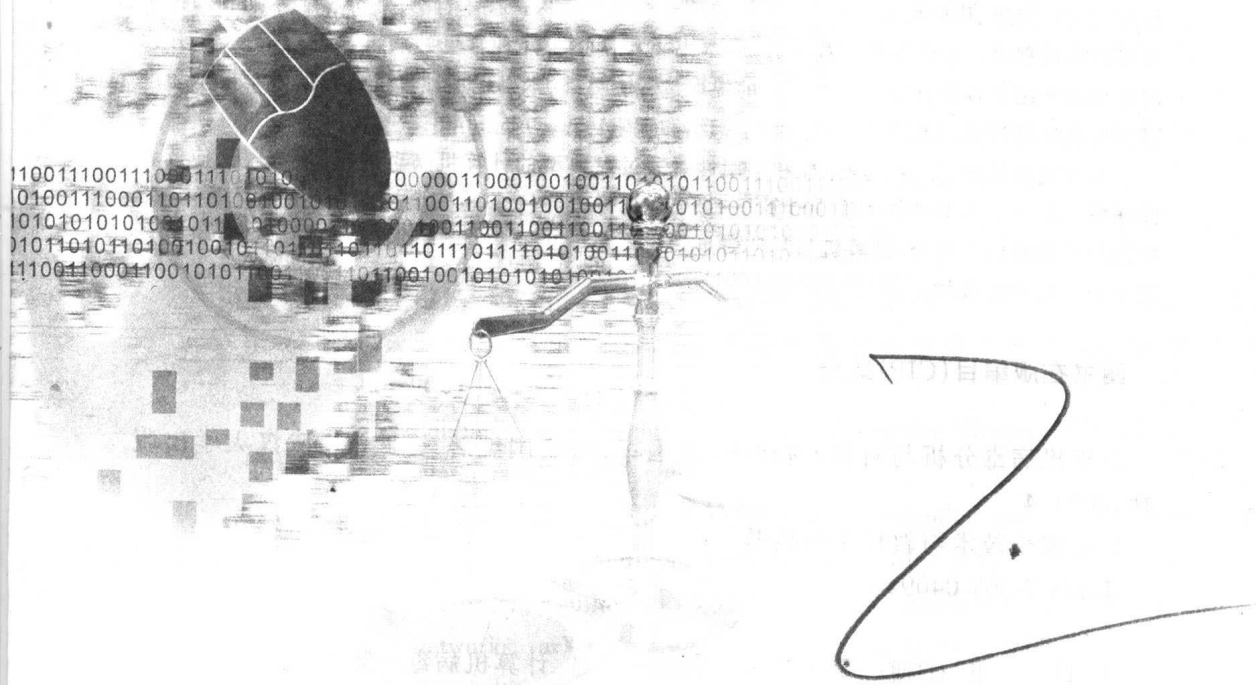
全国优秀出版社
武汉大学出版社

信 息 安 全 技 术  系 列 丛 书

国家自然科学基金项目 (90104005, 66973034)

教育部博士点基金项目 (20020486046)

国家863计划项目 (2002AA141051)



计算机病毒分析与对抗

傅建明 彭国军 张焕国 / 编著



全国优秀出版社
武汉大学出版社

内 容 简 介

本书比较全面地介绍了计算机病毒的基本理论和主要防治技术。特别对计算机病毒的产生机理、寄生特点、传播方式、危害表现以及防治和对抗等方面进行了比较深入的分析 and 探讨。

本书不仅介绍、分析了 DOS 病毒和 Windows 病毒,而且还分析了其他平台的病毒。从计算机病毒的结构、原理、源代码等方面进行了比较深入的分析,介绍了计算机病毒自我隐藏、自加密、多态、变形、代码优化、SEH 等基本的抗分析和自我保护技术,此外还分析了木马和邮件炸弹等破坏性程序。在病毒防治技术方面,本书重点阐述了几种常见的病毒检测对抗技术,并比较详细地介绍了各类计算机病毒样本的提取过程。另外,本书也从计算机病毒的数学模型角度更深层次地对计算机病毒的特征进行了归纳和探索。

本书通俗易懂,注重可操作性和实用性。通过对典型的计算机病毒进行实例分析,使读者能够举一反三。本书可作为广大计算机用户、系统管理员、计算机安全技术人员的技术参考书,特别是可用做信息安全、计算机与其他信息学科本科学生的教材。同时,也可用做计算机信息安全职业培训的教材。

图书在版编目(CIP)数据

计算机病毒分析与对抗/傅建明,彭国军,张焕国编著. —武汉:武汉大学出版社,2004.4

信息安全技术与教材系列丛书

ISBN 7-307-04094-8

I. 计… II. ①傅… ②彭… ③张… III. 计算机病毒—防治 IV. TP309.5

中国版本图书馆 CIP 数据核字(2003)第 113367 号

责任编辑:黄金文 责任校对:王 建 版式设计:支 笛

出版发行:武汉大学出版社 (430072 武昌 珞珈山)

(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.whu.edu.cn)

印刷:武汉大学出版社印刷总厂

开本:787×980 1/16 印张:35.375 字数:727 千字

版次:2004 年 4 月第 1 版 2004 年 4 月第 1 次印刷

ISBN 7-307-04094-8/TP·147 定价:52.00 元

版权所有,不得翻印;凡购我社的图书,如有缺页、倒页、脱页等质量问题,请与当地图书销售部门联系调换。

信息安全技术与教材系列丛书

编委会

主 任：沈昌祥（中国工程院院士，武汉大学兼职教授）

副 主 任：蔡吉人（中国工程院院士，武汉大学兼职教授）

刘经南（中国工程院院士，武汉大学校长）

执行主任：张焕国（中国密码学会理事，武汉大学教授）

委 员：肖国镇（中国密码学会副理事长，武汉大学兼职教授）

张孝成（江南计算所研究员）

屈延文（国家金卡工程办公室安全组组长，武汉大学兼职教授）

卿斯汉（中国科学院信息安全技术工程中心主任，武汉大学兼职教授）

冯登国（信息安全国家重点实验室主任，武汉大学兼职教授）

吴世忠（中国信息安全产品测评认证中心主任，武汉大学兼职教授）

覃中平（华中科技大学教授，武汉大学兼职教授）

何炎祥（中国计算机学会常务理事，武汉大学教授）

何克清（软件工程国家重点实验室副主任，武汉大学教授）

黄传河（武汉大学教授）

江建勤（武汉大学出版社社长，教授）

秘 书：黄金文

序 言

21 世纪是信息的时代，信息成为一种重要的战略资源。信息科学成为最活跃学科领域之一，信息技术改变着人们的生活和工作方式，信息产业成为新的经济增长点。信息的安全保障能力成为一个国家综合国力的重要组成部分。

当前，以 Internet 为代表的计算机网络的迅速发展和“电子政务”、“电子商务”等信息系统的广泛应用，正引起社会和经济的深刻变革，为网络安全和信息安全开拓了新的服务空间。

世界主要工业化国家中每年因利用计算机犯罪所造成的经济损失远远超过普通经济犯罪。内外不法分子互相勾结侵害计算机系统，已成为危害计算机信息安全的普遍性、多发性事件。计算机病毒已对计算机系统的安全构成极大的威胁。社会的信息化导致新的军事革命，信息战、网络战成为新的作战形式。

总之，随着计算机在军事、政治、金融、商业等部门的广泛应用，社会对计算机的依赖越来越大，如果计算机系统的安全受到破坏将导致社会的混乱并造成巨大损失。因此，确保计算机系统的安全已成为世人关注的社会问题和计算机科学的热点研究课题。

信息安全事关国家安全，事关经济发展，必须采取措施确保信息安全。

发展信息安全技术与产业，人才是关键。培养信息安全领域的专业人才，成为当务之急。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。到 2003 年，全国设立信息安全本科专业的高等院校增加到 20 多所。2003 年经国务院学位办批准武汉大学建立信息安全博士点。

为了增进信息安全领域的学术交流、为信息安全专业的大学生提供一套适用的教材，武汉大学组织编写了这套《信息安全技术与教材系列丛书》。这套丛书涵盖了信息安全的主要专业领域，既可用做本科生的教材，又可作为工程技术人员的技术参考书。

我觉得这套丛书的特点是内容全面、技术新颖、理论联系实际，努力反映信息安全领域的新成果和新技术。在我国信息安全专业人才培养刚刚起步的今天，这套



丛书的出版是非常及时的和十分有益的。

我代表编委会对丛书的作者和广大读者表示感谢。欢迎广大读者提出宝贵意见，以使丛书能够进一步修改完善。

中国工程院院士，武汉大学兼职教授

沈昌祥



前言



随着计算机和互联网络技术的快速发展与广泛应用,计算机网络系统的安全受到严重的挑战,来自计算机病毒和黑客攻击及其他方面的威胁越来越大。其中,计算机病毒更是计算机安全中很难根治的主要威胁之一。

在日常生活中,人们大都受到过生物病毒的侵扰。人们通过与生物病毒长时间的斗争,对生物病毒已经有了比较深入的研究,从而具备了防治与对抗生物病毒的能力。

计算机和网络的普及给计算机病毒带来了前所未有的发展机会,计算机病毒给我们带来的负面影响和损失是刻骨铭心的,譬如1999年爆发的CIH病毒以及2003年元月的蠕虫王等都给广大用户带来了巨大的损失。因此,了解计算机病毒的原理、掌握计算机病毒的防治技术、正确认识计算机病毒,可有效地对抗计算机病毒以减少计算机病毒造成的损失。

本书从生物病毒的概念入手,介绍了计算机病毒的定义、特征、分类以及与生物病毒的联系和区别,接着阐述了计算机病毒和破坏程序的发展,其中包括计算机病毒、网络蠕虫、陷门、逻辑炸弹、拒绝服务程序和特洛伊木马等。这些内容构成了本书的第一章。希望通过本章的学习,读者能较全面了解计算机病毒等破坏性程序的基本概念和基本的预防知识。

计算机病毒涉及到较多的计算机基础知识,如操作系统、编程语言、计算机网络等。第二章从一个简单的计算机病毒的原型出发,引入计算机病毒的逻辑结构,进而介绍计算机的磁盘管理、Windows的文件系统、计算机的引导过程、计算机的中断与异常、计算机的内存管理、EXE文件的格式等与计算机病毒相关的预备知识。如果读者对这些知识比较熟悉,则可跳过该章。希望该章能为读者提供计算机病毒的系统知识。

在第三章中我们将计算机病毒的逻辑结构分为三部分:病毒的传播机制、触发机制和破坏机制。第三章重点阐述了计算机病毒的这三种机制,并讨论了计算机病毒的几种生存状态及它们之间的相互转换。我们知道计算机病毒的传播、触发和破坏方式是各式各样的,但是计算机病毒的传播和破坏是有它的特定条件的,了解这



些条件有利于我们把握计算机病毒的本质。

目前用户常用的操作系统大多数为 Windows 系列,少数为 DOS, Linux 等其他操作系统。由于 DOS 病毒是计算机病毒的典型代表,第四章介绍了 DOS 下的引导区病毒和文件型病毒的概述、原理和相关病毒源码分析。接着,第五章从 Windows 病毒出发,首先分析了 Win32 PE 病毒的原理,随后阐述了宏病毒、脚本病毒、网页病毒、网络蠕虫的原理和特征以及相关病毒的源码分析。这两章从感性上认识病毒,从原理上分析病毒,从而了解病毒的本质。

反病毒技术的不断发展迫使病毒不断地提高自己的生存能力,病毒技术得到了不断的发展。第六章分析了目前病毒常采用的抗分析技术,其中包括各种隐藏技术、花指令、简单自加密技术、多态技术、变形技术、代码优化技术、异常处理技术等。这些技术的综合运用给病毒的检测带来较大困难。

第七章介绍了木马、邮件炸弹的概念、原理以及基本的预防策略,同时也简单分析了虚假的文本文件,这些文件的运行同样也会带来很大的破坏性。本章是第四、五两章的延伸。

自第一个病毒出现后,人们通过与病毒长期的斗争,积累了大量反病毒的经验,掌握了很多实用的反病毒技术,并开发出了一些优秀的抗病毒软件产品。第八章介绍目前抗病毒软件主要采用的病毒对抗技术。本章首先阐述了特征值检测技术、校验和检测技术、行为监测技术、启发式扫描技术和虚拟机技术,接着介绍了病毒的清除和预防,最后介绍了生物免疫系统、计算机病毒免疫的原理、数字免疫系统和以毒攻毒思想。本章将进一步提高我们对反病毒技术水平的认识,这将有利于我国的反病毒事业的发展。

为了深刻认识计算机病毒的本质,人们努力用形式化的方法刻画计算机病毒。第九章介绍了计算机病毒的各种理论模型,包括基于图灵机的计算模型、基于递归函数的数学模型和互联网中蠕虫传播模型。这些模型有利于进一步深入理解计算机病毒、研究计算机病毒的各种机制。

除了前面介绍的病毒外,还有许多其他操作系统的病毒,如 UNIX/Linux 下的病毒。第十章首先概述了其他平台的病毒,然后重点介绍 UNIX/Linux 下 ELF 的文件格式以及基于 ELF 的计算机病毒原理,最后简单地介绍了手机病毒。

第十一章作为本书的结束,介绍了计算机样本的获得和提取方法,并给出了一个简单的提取实例。本章是作为前面第二章、第三章、第四章、第五章、第六章、第八章内容的实践部分。读者在提取样本时需要格外小心,因为稍有不慎会造成病毒对计算机系统的感染,甚至会造成比较严重的后果和损失。



本书第一章、第三章、第七章、第八章、第十章由傅建明和彭国军编写，第二章、第四章、第五章、第六章、第十一章由彭国军和张焕国编写，第九章由李晓丽和傅建明共同编写。全书最后由傅建明和彭国军统稿，张焕国审定。

本书的研究和编写工作受到国家自然科学基金项目（编号：6697304，90104005）、国家 863 计划项目（编号：2002AA141051）和教育部博士点基金项目（编号：20020486046）的资助。

本书从各种论文、书刊、期刊以及互联网中引用了大量的资料，有的在参考文献中列出，有的无法查证。在文字的录入和整理中，得到了王丽娜、周伟、程炼、杨晓东等的帮助。在此谨向他们表示衷心感谢。

由于时间和水平有限，难免有错，恳请读者批评指正，使本书得以改进和完善。

作 者

2003 年 6 月于珞珈山

目 录

第一章 计算机病毒概述	1
1.1 生物病毒的定义和特征	1
1.1.1 生物病毒概述	1
1.1.2 生物病毒的结构	2
1.1.3 生物病毒的繁殖	2
1.1.4 生物病毒的分类	3
1.2 计算机病毒的定义和特征	4
1.2.1 计算机病毒的起源	5
1.2.2 计算机病毒的产生	7
1.2.3 计算机病毒的特征	8
1.3 计算机病毒与生物病毒的联系与区别	9
1.3.1 病毒的本质	10
1.3.2 病毒的危害性	11
1.3.3 病毒的结构方式	13
1.3.4 病毒的产生及其效果	13
1.3.5 病毒的防治	15
1.4 计算机病毒的分类	16
1.5 病毒的基本防治	18
1.6 计算机病毒的发展	20
1.6.1 病毒的发展概述	21
1.6.2 网络蠕虫	26
1.6.3 陷门	31
1.6.4 逻辑炸弹	31
1.6.5 拒绝服务程序	32
1.6.6 特洛伊木马	34
第二章 预备知识	38
2.1 计算机病毒的结构	38



2.1.1 一个简单的计算机病毒	38
2.1.2 计算机病毒的逻辑结构	39
2.2 计算机磁盘的管理	39
2.2.1 硬盘结构简介	40
2.2.2 扩展 Int 13H 的技术资料	44
2.3 Windows 文件系统	51
2.3.1 文件系统的发展	51
2.3.2 FAT16 格式说明	54
2.3.3 FAT32 文件系统	55
2.3.4 文件分配表的使用	56
2.3.5 NTFS 文件格式	57
2.4 计算机的引导过程	57
2.4.1 认识计算机启动过程	58
2.4.2 主引导记录的工作原理	60
2.5 中断与异常	65
2.5.1 中断	65
2.5.2 异常	65
2.5.3 中断优先权	66
2.5.4 中断向量表	67
2.5.5 中断处理过程	68
2.6 内存管理	68
2.6.1 DOS 内存布局	69
2.6.2 Windows 9x/NT 内存布局	69
2.6.3 操纵内存	71
2.7 EXE 文件格式	73
2.7.1 MZ 文件格式	73
2.7.2 NE 文件格式	75
2.7.3 PE 文件格式	77

第三章 计算机病毒的基本机制	92
3.1 计算机病毒状态	92
3.2 计算机病毒的三种机制	93
3.3 计算机病毒的传播机制	98
3.3.1 病毒感染目标和过程	100
3.3.2 感染长度和感染次数	103
3.3.3 引导型病毒的感染	106



3.3.4 寄生感染	108
3.3.5 插入感染和逆插入感染	110
3.3.6 链式感染	111
3.3.7 破坏性感染	112
3.3.8 滋生感染	114
3.3.9 没有入口点的感染	115
3.3.10 OBJ、LIB 和源码的感染	117
3.3.11 混合感染和交叉感染	117
3.3.12 零长度感染	118
3.4 计算机病毒的触发机制	120
3.4.1 日期和时间触发	120
3.4.2 键盘触发	126
3.4.3 感染触发	126
3.4.4 启动触发	127
3.4.5 磁盘访问触发和中断访问触发	128
3.4.6 其他触发	128
3.5 计算机病毒的破坏机制	129
3.5.1 攻击系统数据区	130
3.5.2 攻击文件和硬盘	131
3.5.3 攻击内存	134
3.5.4 干扰系统的运行	135
3.5.5 扰乱输出设备	138
3.5.6 扰乱键盘	141
第四章 DOS 病毒分析	144
4.1 引导型病毒	144
4.1.1 引导型病毒的概述	144
4.1.2 引导型病毒的原理	144
4.1.3 大麻病毒分析	148
4.2 文件型病毒	157
4.2.1 文件型病毒的概述	157
4.2.2 文件型病毒的原理	157
4.2.3 “黑色星期五”病毒分析	162
4.3 混合病毒	171
第五章 Windows 病毒分析	173



5.1 Win32 PE 病毒	173
5.1.1 Win32 PE 病毒原理	173
5.1.2 一个感染的例子分析	188
5.2 宏病毒	201
5.2.1 宏病毒的概述	201
5.2.2 宏病毒的原理	202
5.2.3 美丽莎病毒分析	212
5.3 脚本病毒	216
5.3.1 WSH 介绍	216
5.3.2 VBS 脚本病毒的特点	218
5.3.3 VBS 脚本病毒原理分析	219
5.3.4 VBS 脚本病毒的防范	226
5.3.5 爱虫病毒分析	227
5.4 网页病毒	238
5.4.1 修改注册表	240
5.4.2 操纵用户文件系统	242
5.4.3 防范措施	243
5.5 网络蠕虫	244
5.5.1 蠕虫的定义	244
5.5.2 蠕虫的行为特征	246
5.5.3 蠕虫的工作原理	247
5.5.4 蠕虫技术的发展	249
5.5.5 蠕虫的防治	249
5.5.6 SQL 蠕虫王分析	250
第六章 病毒技巧	259
6.1 病毒的隐藏技术	259
6.1.1 引导型病毒的隐藏技术	259
6.1.2 文件型病毒的隐藏技术	260
6.1.3 宏病毒的隐藏技术	261
6.1.4 Windows 病毒的隐藏技术	261
6.2 花指令	262
6.3 计算机病毒的简单加密	265
6.4 病毒的多态	268
6.5 病毒的变形技术	269
6.6 病毒代码的优化	279

6.7 异常处理	288
6.7.1 异常处理的方式	288
6.7.2 异常处理的过程	289
6.7.3 异常处理的参数	290
6.7.4 异常处理的例子	293
第七章 破坏性程序分析	298
7.1 特洛伊木马	298
7.1.1 特洛伊木马概述	298
7.1.2 木马的基本原理	301
7.1.3 木马的预防和清除	308
7.1.4 木马技术的发展	311
7.1.5 木马的示例—冰河	316
7.2 邮件炸弹	323
7.2.1 邮件炸弹的概述	323
7.2.2 邮件炸弹的原理	324
7.2.3 邮件炸弹的防御	330
7.2.4 垃圾邮件	334
7.3 虚假的文本文件	336
7.3.1 HTML 的文本文件	336
7.3.2 恶意碎片文件	337
7.3.3 eml 文本文件	339
第八章 病毒对抗技术	341
8.1 病毒的检测技术	341
8.1.1 特征值检测技术	342
8.1.2 校验和检测技术	345
8.1.3 行为监测技术	348
8.1.4 启发式扫描技术	352
8.1.5 虚拟机技术	358
8.2 病毒发现和抗病毒软件	363
8.2.1 现象观察法	363
8.2.2 抗病毒软件	365
8.2.3 感染实验分析	369
8.3 病毒的清除	370
8.3.1 引导型病毒的清除	370



8.3.2 宏病毒的清除	371
8.3.3 文件型病毒的清除	371
8.3.4 病毒的去激活	374
8.4 计算机病毒的免疫技术	375
8.4.1 生物免疫系统	375
8.4.2 计算机病毒免疫的原理	378
8.4.3 数字免疫系统	381
8.4.4 以毒攻毒	384
8.5 计算机病毒的防治	386
8.5.1 病毒入侵的途径	386
8.5.2 病毒预防的原则	387

第九章 计算机病毒的理论模型

389

9.1 基于图灵机的计算机病毒的计算模型	389
9.1.1 RAM 模型	389
9.1.2 RASPM 模型	391
9.1.3 图灵机模型	392
9.1.4 RASPM_ABS 模型	393
9.1.5 操作系统模型	399
9.1.6 基于 RASPM_ABS 的病毒	401
9.2 基于递归函数的计算机病毒的数学模型	405
9.2.1 Adleman 病毒模型	405
9.2.2 Adleman 病毒模型的分析	407
9.2.3 田畅 & 郑少仁病毒模型	408
9.2.4 李祥病毒模型的分析	410
9.3 Internet 蠕虫传播模型	412
9.3.1 SIS 模型和 SI 模型	412
9.3.2 SIR 模型	413
9.3.3 网络模型中蠕虫传播的方式	415
9.3.4 SI 模型的仿真	415
9.3.5 SIS 模型的仿真	418
9.3.6 SIR 模型的仿真	419
9.3.7 解析结果和仿真结果的对比	420

第十章 其他平台的病毒

423

10.1 其他平台病毒的概述	423
----------------------	-----



10.1.1 安全机制与病毒	423
10.1.2 Shell 脚本与病毒	424
10.1.3 蠕虫	424
10.1.4 伪造的库函数	424
10.1.5 内核级的传播	426
10.1.6 Mac OS 环境下的病毒	427
10.2 ELF 文件格式	428
10.2.1 目标文件	428
10.2.2 ELF 头	430
10.2.3 节	438
10.2.4 字符串表	446
10.2.5 符号表	447
10.2.6 重定位	452
10.2.7 程序头	456
10.2.8 程序载入	462
10.2.9 动态链接	465
10.3 基于 ELF 的计算机病毒	478
10.3.1 代码段和数据段	478
10.3.2 覆盖式感染	481
10.3.3 填充感染	482
10.3.4 数据段感染	485
10.3.5 代码段感染	485
10.3.6 PLT 感染	486
10.3.7 Linux 病毒的分析	487
10.4 移动设备(手机)病毒	487
10.4.1 手机病毒的危害	488
10.4.2 手机病毒的防治	490
10.4.3 手机病毒的发展	490
10.4.4 手机病毒的实例	493
第十一章 计算机病毒样本的提取	495
11.1 病毒样本的获取	495
11.1.1 反病毒公司的样本获取方法	495
11.1.2 个人如何获取病毒样本	496
11.2 VBS 脚本病毒样本的提取	496
11.2.1 一次性加/解密的病毒样本	496



11.2.2 解密一处执行一处的病毒样本	498
11.3 宏病毒样本的提取	499
11.3.1 利用代码进行提取	500
11.3.2 利用 Word 直接提取	500
11.4 PE 病毒样本的提取	501
11.4.1 病毒提取环境	501
11.4.2 病毒提取工具	501
11.4.3 样本提取方法	502
11.4.4 病毒样本的提取实例	505
 附录 A DOS 引导程序说明	 510
附录 B 分区类型表	516
附录 C 电脑开机轰鸣声	518
附录 D 电脑病毒的编年史	520
参 考 文 献	544