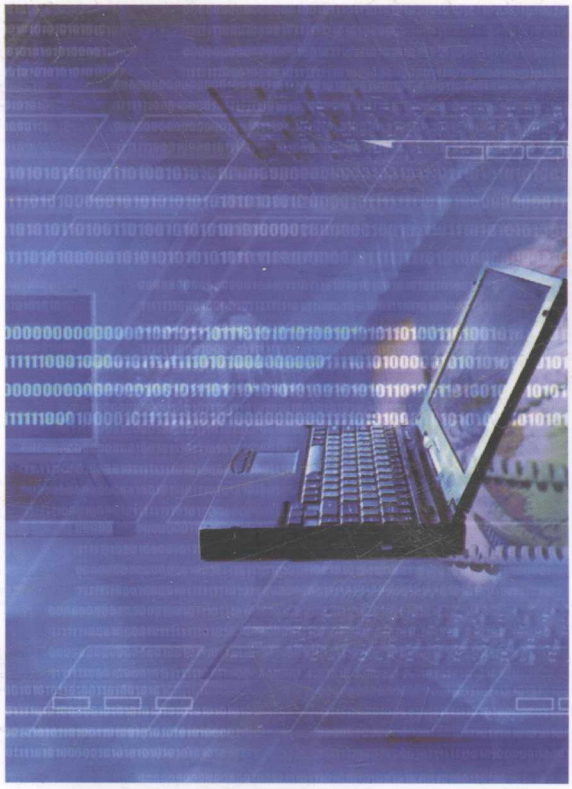
高等学校计算机应用规划教材

计算机病毒及其防范技术(第2版)

- 计算机病毒概述
- 计算机病毒及其防范模型
- 计算机病毒结构及技术分析
- 传统计算机病毒
- 特洛伊木马、宏病毒
- Linux病毒技术
- 移动终端恶意代码
- 新型计算机病毒
- 计算机病毒防范技术
- 常用杀毒软件及解决方案
- 计算机病毒防治策略



刘功申　编著

清华大学出版社

高等学校计算机应用规划教材

计算机病毒及其防范技术

(第2版)

刘功申　编著

清华大学出版社
北　京

内 容 简 介

本书详细介绍了计算机病毒的基本原理和主要防治技术，深入分析和探讨了计算机病毒的产生机理、寄生特点、传播方式、危害表现以及防范和对抗等方面的技术。主要内容包括计算机病毒概述、计算机病毒及其防范模型、计算机病毒的结构及技术分析、传统计算机病毒、特洛伊木马、宏病毒、Linux 病毒技术、移动终端恶意代码、新型计算机病毒、计算机病毒的防范技术、常用杀毒软件及其解决方案和计算机病毒防治策略等。

本书通俗易懂，注重理论与实践相结合。所设计的教学实验覆盖了所有类型的计算机病毒，使读者能够举一反三。为了便于教学，教材附带教学课件、实验用代码以及辅助应用程序版本说明等内容，下载地址为 www.tupwk.com.cn/downpage。下载并解压缩后，就可按照教材设计的实验步骤使用。

本书可作为高等院校信息安全专业和计算机相关专业的教材，也可供广大系统管理员、计算机安全技术人员参考。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

计算机病毒及其防范技术(第 2 版) / 刘功申　编著.
—北京：清华大学出版社，2011.5
(高等学校计算机应用规划教材)
ISBN 978-7-302-25452-2

Ⅰ. ①计…　Ⅱ. ①刘…　Ⅲ. ①计算机病毒—防治—高等学校—教材　Ⅳ. ①TP309.5

责任编辑：刘金喜
装帧设计：孔祥丰
责任校对：胡花蕾
责任印制：何　芊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：三河市君旺印装厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：20.5　**字　数**：473 千字
版　　次：2011 年 5 月第 2 版　　**印　　次**：2011 年 5 月第1 次印刷
印　　数：1～4000
定　　价：33.80 元

产品编号：040135-01

前　言

在全球经济一体化的背景下，信息安全技术不仅成为对抗霸权主义、强权政治以及抗击信息侵略的重要屏障，而且也是国家政治、军事、经济、文化以及社会繁荣安定与和谐发展的有力保证。计算机病毒作为信息安全领域的重要一环，近年来在军事战争、社会稳定方面就像双刃剑一样，引起了社会各界的广泛重视。计算机病毒不仅仅是信息技术高速发展的必然结果，还可在政府行为的指导下作为一种“以毒攻毒”的信息对抗手段服务于国家安全。

作者在从事大学本科计算机病毒教学 6 年，研发工作 4 年的基础上，编写了本教材。书中重点分析计算机病毒的运行机制，并通过实验的方式讲解常见病毒。在分析病毒技术的基础上，探讨了计算机病毒防范的多个层次的工作，它们包括检测、清除、数据备份及恢复、主动及被动预防、防治策略和防治方案等。

本书共分 12 章，具体内容如下。

第 1 章：计算机病毒概述。主要介绍计算机病毒的基本概念，并在此基础上讲述计算机病毒的关键历史转折点、技术分类、传播途径、感染症状、命名规则及未来发展趋势等相关问题。

第 2 章：计算机病毒及其防范模型。主要介绍计算机病毒的理论模型，例如，基于图灵机、递归函数和传染病数学模型的计算机病毒模型。在本章最后一小节介绍了计算机病毒预防理论模型。

第 3 章：计算机病毒结构及技术分析。主要介绍传统计算机病毒的功能模块和工作机制，以及实战型病毒所必需的技术特征。

第 4 章：传统计算机病毒。感染引导区、可执行文件的病毒为传统计算机病毒。本章主要讲解了 DOS 下感染引导区的病毒、感染 COM 文件的病毒，以及 Windows 下感染 PE 文件的病毒。

第 5 章：特洛伊木马。本章详细分析了特洛伊木马的技术特征、木马隐藏的一些常用技术、木马植入技术以及防范技术等。

第 6 章：宏病毒。以 Microsoft Word 宏病毒为主线介绍宏病毒的基本概念、制作机理、宏病毒实验和防范方法等内容。

第 7 章：Linux 病毒技术。在了解 Linux 安全问题的基础上，探讨了 Linux 病毒的概念。本章还精心设计了两个实验，以直观的方式分别讲解了 Linux 操作系统的脚本病毒和感染 ELF 格式文件的病毒原理。

第 8 章：移动终端恶意代码。以手机恶意代码为主线，介绍移动终端恶意代码的概念、技术进展和防范工具，使读者了解未来移动终端设备上的威胁。

第9章：新型计算机病毒。感染可执行文件、数据文件和引导区的病毒已经是过去时，蠕虫、僵尸和RootKit才是计算机病毒的进行时。鉴于此，本章重点探讨了一些采用特殊技术编制的新型计算机病毒，以使读者了解最流行的计算机病毒。

第10章：计算机病毒的防治技术。计算机病毒防治技术涉及的范围非常广，包括技术和管理等多个方面。本章给出了病毒防范的检测、清除、数据备份及恢复、主动及被动预防、防治策略等宏观思路。

第11章：常用杀毒软件及其解决方案。通过介绍企业网络的典型结构、典型应用和网络时代的病毒特征，得出企业网络防病毒体系对反病毒技术和工具的需求，从而给出一些典型病毒防治体系解决方案。

第12章：计算机病毒防治策略。通过讨论防御性策略得到的不同建议，来避免计算机受到病毒的影响。本章侧重于全局策略和规章，并且针对企业用户所讲述的内容比针对单机用户的要多一些。本章还就如何制订一个防御计划，如何挑选一个快速反应小组，如何控制住病毒的发作，以及反病毒工具的选择等问题提出了一些建议。

本书主要由刘功申编写。其中，唐祝寿重点参与了第3章的编写，来火尧重点参与了第6章和第11章的编写，任伟和石磊重点参与了第7章的编写，胡长春重点参与了第8章的编写，邓攀重点参与了第2章和第12章的编写。

在本书完稿之际，作者首先感谢第一版的读者，他们给了我非常好的建议；感谢教学6年来听过作者计算机病毒课的所有学生，他们为作者的讲义提出了很多宝贵意见；感谢各类参考资料的提供者，这些资料既充实了作者的教材也丰富了作者的知识；感谢我的太太和孩子，该书稿的完成离不开家人的支持。

为便于教学，本教材提供教学课件和实验用源代码，可通过http://www.tupwk.com.cn/downpage下载。

由于水平有限，书中难免有疏漏之处，恳请读者批评指正，以使本书得以进一步改进和完善。作者的联系方式：lgshen@sjtu.edu.cn。服务邮箱：wkservice@163.com。

作　者

2010年12月

于思源湖畔

目　录

第 1 章　计算机病毒概述 …… 1
1.1　计算机病毒的概念 …… 1
1.2　计算机病毒的发展历史及其危害程度 …… 3
1.3　计算机病毒的分类 …… 7
1.4　计算机病毒的传播途径 …… 8
1.5　染毒计算机的症状 …… 11
1.5.1　计算机病毒的表现现象 …… 11
1.5.2　与计算机病毒现象类似的硬件故障 …… 15
1.5.3　与计算机病毒现象类似的软件故障 …… 16
1.6　计算机病毒的命名规则 …… 16
1.7　计算机病毒的发展趋势和最新动向 …… 18
1.8　习题 …… 20

第 2 章　计算机病毒及其防范模型 …… 21
2.1　基本定义 …… 21
2.2　基于图灵机的计算机病毒模型 …… 23
2.2.1　随机访问计算机模型 …… 23
2.2.2　随机访问存储程序模型 …… 25
2.2.3　图灵机模型 …… 26
2.2.4　带后台存储的 RASPM 模型 …… 27
2.2.5　操作系统模型 …… 32
2.2.6　基于 RASPM_ABS 的病毒 …… 34
2.3　基于递归函数的计算机病毒的数学模型 …… 38
2.3.1　Adlemen 病毒模型 …… 38
2.3.2　Adlemen 病毒模型的分析 …… 39
2.4　Internet 蠕虫传播模型 …… 40
2.4.1　SIS 模型和 SI 模型 …… 41
2.4.2　SIR 模型 …… 42
2.4.3　网络模型中蠕虫传播的方式 …… 43
2.5　计算机病毒预防理论模型 …… 44
2.6　习题 …… 46

第 3 章　计算机病毒结构及技术分析 …… 47
3.1　计算机病毒的结构和工作机制 …… 47
3.1.1　引导模块 …… 47
3.1.2　感染模块 …… 49
3.1.3　破坏模块 …… 50
3.1.4　触发模块 …… 50
3.2　计算机病毒的技术特征 …… 51
3.2.1　驻留内存 …… 51
3.2.2　病毒变种 …… 54
3.2.3　EPO 技术 …… 55
3.2.4　抗分析技术 …… 56
3.2.5　隐蔽性病毒技术 …… 58
3.2.6　多态性病毒技术 …… 60
3.2.7　插入型病毒技术 …… 63
3.2.8　自动生产技术 …… 63
3.2.9　网络病毒技术 …… 64
3.3　习题 …… 64

第 4 章　传统计算机病毒 …… 66
4.1　引导型病毒编制技术 …… 66
4.1.1　引导型病毒编制原理 …… 67
4.1.2　引导型病毒实验(实验一) …… 68
4.2　16 位可执行文件病毒编制技术 …… 71

4.2.1 16位可执行文件结构及运行原理……71
4.2.2 COM文件病毒原理……75
4.2.3 COM文件病毒实验(实验二)……76
4.3 32位可执行文件病毒编制技术……76
4.3.1 PE文件结构及其运行原理……77
4.3.2 PE文件型病毒关键技术……77
4.3.3 从ring3到ring0的简述……84
4.3.4 PE文件格式实验(实验三)……84
4.3.5 32位文件型病毒实验(实验四)……85
4.4 习题……86
第5章 特洛伊木马……87
5.1 木马概述……87
5.1.1 木马的定义、组成与特征……87
5.1.2 木马的分类……89
5.1.3 远程控制、木马与病毒……90
5.1.4 木马的工作流程……90
5.1.5 木马的技术发展……91
5.2 简单木马程序实验(实验五)……93
5.2.1 自动隐藏……95
5.2.2 自动加载……96
5.2.3 实现Server端功能……97
5.2.4 实现Client端功能……102
5.2.5 实施阶段……103
5.3 木马程序的关键技术……104
5.3.1 植入技术及实验(实验六)……104
5.3.2 自启动技术……110
5.3.3 隐藏技术……113
5.3.4 其他技术……122
5.4 木马防范技术及经验……128
5.4.1 全面防治特洛伊木马……128
5.4.2 几种常见木马病毒的杀除方法……130
5.4.3 已知木马病毒的端口列表……132
5.4.4 木马病毒清除实验(实验七)……134
5.5 习题……134
第6章 宏病毒……136
6.1 宏病毒概述……136
6.1.1 宏病毒的运行环境……136
6.1.2 宏病毒的特点……137
6.1.3 经典宏病毒……138
6.1.4 宏病毒的共性……140
6.2 宏病毒的作用机制……140
6.2.1 Word中的宏……141
6.2.2 Word宏语言……142
6.2.3 宏病毒关键技术……143
6.3 Word宏病毒查杀……145
6.3.1 人工发现宏病毒的方法……145
6.3.2 手工清除宏病毒的方法……146
6.3.3 宏病毒查杀方法……146
6.3.4 宏病毒清除工具……147
6.4 预防宏病毒……148
6.5 Word宏病毒实验……149
6.5.1 宏复制实验(实验八)……149
6.5.2 类台湾1号病毒实验(实验九)……150
6.6 习题……151
第7章 Linux病毒技术……152
7.1 一些公共的误区……152
7.2 Linux系统病毒的分类……153
7.3 Linux系统下的脚本病毒……154
7.3.1 Linux脚本病毒编制技术……155
7.3.2 Linux脚本病毒实验(实验十)……158
7.4 ELF文件格式……159

7.5 ELF 格式文件感染原理 …… 159
7.5.1 无关 ELF 格式的感染方法 …… 159
7.5.2 利用 ELF 格式的感染方法 …… 163
7.5.3 高级感染技术 …… 171
7.6 Linux ELF 病毒实例 …… 173
7.6.1 病毒技术汇总 …… 173
7.6.2 原型病毒实现 …… 181
7.6.3 Linux ELF 病毒实验(实验十一) …… 190
7.7 习题 …… 190

第 8 章 移动终端恶意代码 …… 192
8.1 移动终端恶意代码概述 …… 192
8.2 移动终端操作系统 …… 193
8.2.1 智能手机操作系统 …… 194
8.2.2 PDA 操作系统 …… 197
8.2.3 移动终端操作系统的弱点 …… 200
8.3 移动终端恶意代码关键技术 …… 200
8.3.1 移动终端恶意代码传播途径 …… 201
8.3.2 移动终端恶意代码攻击方式 …… 201
8.3.3 移动终端恶意代码生存环境 …… 201
8.3.4 移动终端设备的漏洞 …… 203
8.4 移动终端恶意代码实例 …… 203
8.5 移动终端恶意代码的防范 …… 205
8.6 移动终端杀毒工具 …… 206
8.7 习题 …… 208

第 9 章 新型计算机病毒 …… 209
9.1 蠕虫病毒 …… 209
9.1.1 蠕虫的基本概念 …… 209
9.1.2 蠕虫和传统病毒的关系 …… 210
9.1.3 蠕虫病毒的危害 …… 210
9.1.4 蠕虫病毒的特性 …… 211
9.1.5 蠕虫病毒的机理 …… 212
9.1.6 基于 U 盘传播的蠕虫病毒实验(实验十二) …… 213
9.2 利用 Outlook 漏洞编写病毒 …… 215
9.2.1 邮件型病毒的传播方式 …… 215
9.2.2 邮件型病毒的传播原理 …… 215
9.2.3 邮件型病毒预防 …… 218
9.2.4 邮件型病毒实验(实验十三) …… 219
9.3 WebPage 中的恶意代码 …… 220
9.3.1 脚本病毒基本类型 …… 221
9.3.2 Web 恶意代码工作机理 …… 221
9.3.3 Web 恶意代码实验(实验十四) …… 224
9.4 流氓软件 …… 225
9.4.1 流氓软件的定义 …… 225
9.4.2 应对流氓软件的政策 …… 225
9.4.3 流氓软件的主要特征 …… 226
9.4.4 流氓软件的发展过程 …… 226
9.4.5 流氓软件的分类 …… 228
9.5 僵尸网络 …… 229
9.6 Rootkit 病毒 …… 233
9.7 习题 …… 237

第 10 章 计算机病毒的防范技术 …… 239
10.1 计算机病毒防范技术现状 …… 239
10.2 计算机病毒防范思路 …… 241
10.3 计算机病毒的检测 …… 242
10.3.1 计算机病毒的检测原理 …… 242
10.3.2 计算机病毒的检测方法 …… 248
10.3.3 自动检测的源码分析 …… 248
10.3.4 计算机病毒查找实验(实验十五) …… 250

10.4 计算机病毒的清除 …… 251
10.4.1 计算机病毒清除的原理 …… 251
10.4.2 计算机病毒的清除方法 …… 254
10.5 计算机病毒的预防 …… 254
10.5.1 系统监控技术 …… 254
10.5.2 源监控技术 …… 255
10.5.3 个人防火墙技术 …… 255
10.5.4 系统加固技术 …… 256
10.6 计算机病毒的免疫 …… 256
10.6.1 计算机病毒免疫的原理 …… 257
10.6.2 免疫的方法及其特点 …… 257
10.6.3 数字免疫系统 …… 258
10.7 数据备份和数据恢复 …… 259
10.7.1 数据备份 …… 260
10.7.2 数据恢复 …… 264
10.7.3 数据恢复工具箱 …… 267
10.8 习题 …… 268

第 11 章 常用杀毒软件及其解决方案 …… 269
11.1 国内外著名杀毒软件比较 …… 269
11.1.1 杀毒软件必备功能 …… 269
11.1.2 杀毒产品使用和配置 …… 271
11.1.3 流行杀毒产品比较 …… 272
11.1.4 反病毒产品的地缘性 …… 277
11.2 企业级病毒防治方案 …… 280
11.2.1 企业防病毒的需求 …… 280
11.2.2 企业网络的典型结构 …… 282
11.2.3 企业网络的典型应用 …… 283
11.2.4 病毒在网络上传播的过程 …… 284
11.2.5 企业网络防病毒方案 …… 285
11.3 习题 …… 287

第 12 章 计算机病毒防治策略 …… 288
12.1 计算机病毒防治策略的基本准则 …… 288
12.2 国家层面上的病毒防治策略 …… 289
12.3 单机用户病毒防治策略 …… 291
12.3.1 一般技术措施 …… 291
12.3.2 上网基本策略 …… 292
12.4 企业病毒防治策略 …… 293
12.4.1 如何建立防御计划 …… 293
12.4.2 执行计划 …… 296
12.4.3 反病毒扫描引擎相关问题 …… 301
12.4.4 额外的防御工具 …… 302
12.5 未来的防范措施 …… 306
12.6 防病毒相关法律法规 …… 310
12.7 习题 …… 316

附录 计算机病毒相关网上资源 …… 317

参考文献 …… 319

第1章　计算机病毒概述

对于计算机病毒，曾经有几个毋庸置疑的“真理”：计算机不可能因为仅仅读了一封电子邮件而感染病毒；计算机病毒不可能损害硬件；计算机病毒不可能感染一张有写保护的软盘；计算机不可能因为浏览一个图形文件而感染病毒。但是，在计算机病毒技术迅速发展的今天，这些说法都已经过时，我们必须更新关于计算机病毒及其防范工作的陈旧知识。

本章主要介绍计算机病毒的基本概念，并在此基础上讲述计算机病毒的历史、分类、传播途径、感染症状、命名规则及发展趋势等相关问题。

本章学习目标：

- 明确计算机病毒的基本概念
- 了解计算机病毒发展的历史转折点
- 熟悉计算机病毒的分类
- 熟悉商业计算机病毒命名规则
- 掌握计算机病毒的发展趋势

1.1　计算机病毒的概念

计算机病毒(Computer Virus)在《中华人民共和国计算机信息系统安全保护条例》中被明确定义为：“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”。

计算机病毒是一个程序，一段可执行代码。就像生物病毒一样，计算机病毒有独特的复制能力。计算机病毒可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上。当染毒文件被复制或从一个用户传送到另一个用户时，它们就随同该文件一起蔓延开来。除复制能力外，某些计算机病毒还有其他一些共同特性：一个被感染的程序是能够传播病毒的载体。当你看到病毒似乎仅表现在文字和图像上时，它们可能也已毁坏了文件、格式化了你的硬盘或引发了其他类型的灾害。若病毒并不寄生于一个感染程序，它仍然能通过占据存储空间给你带来麻烦，并降低计算机的性能。计算机病毒具有以下几个明显的特征。

1. 传染性

这是病毒的基本特征，是判断一个程序是否为计算机病毒的最重要的特征，一旦病毒

被复制或产生变种，其传染速度之快令人难以想象。

2. 破坏性

任何计算机病毒感染了系统后，都会对系统产生不同程度的影响。发作时轻则占用系统资源，影响计算机运行速度，降低计算机工作效率，使用户不能正常使用计算机；重则破坏用户计算机的数据，甚至破坏计算机硬件，给用户带来巨大的损失。

3. 寄生性

一般情况下，计算机病毒都不是独立存在的，而是寄生于其他的程序中，当执行这个程序时，病毒代码就会被执行。在正常程序未启动之前，用户是不易发觉病毒的存在的。

4. 隐蔽性

计算机病毒具有很强的隐蔽性，它通常附在正常的程序之中或藏在磁盘隐秘的地方，有些病毒采用了极其高明的手段来隐藏自己，如使用透明图标、注册表内的相似字符等，而且有的病毒在感染了系统之后，计算机系统仍能正常工作，用户不会感到有任何异常，在这种情况下，普通用户无法在正常的情况下发现病毒。

5. 潜伏性(触发性)

大部分的病毒感染系统之后一般不会马上发作，而是隐藏在系统中，就像定时炸弹一样，只有在满足特定条件时才被触发。例如，黑色星期五病毒，不到预定时间，用户就不会觉察出异常。一旦遇到13日并且是星期五，病毒就会被激活并且对系统进行破坏。当然大家都应该还记得噩梦般的CIH病毒，它是在每月的26日发作。

有计算机的地方就有计算机病毒，也可以说，计算机病毒无处不在。尽管病毒带来的损失或大或小，甚至有些没有任何损失，但是大部分计算机用户都有被病毒侵扰的经历。据中国计算机病毒应急处理中心统计，中国计算机用户受病毒感染的比例(感染率)一直处于高位(如图1-1所示)。美国权威调查机构证实，进入新世纪以来，每年因计算机病毒造成的损失都在100亿美元以上。

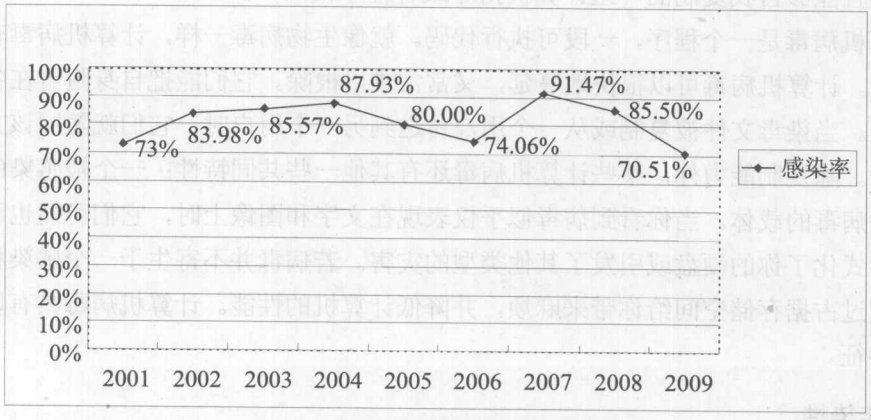


图1-1　计算机病毒感染率变化趋势

1.2　计算机病毒的发展历史及其危害程度

2008 年 12 月 5 日，在卡巴斯基实验室举办的病毒分析师峰会上，卡巴斯基实验室的高级区域研究师 David Emm 发表了关于恶意代码市场分析的主题演讲。David 在主题演讲中指出，恶意代码的数量每秒钟都在增长，到 2008 年底为止，全球大约存在恶意代码 1 400 000 种(如图 1-2 所示)。

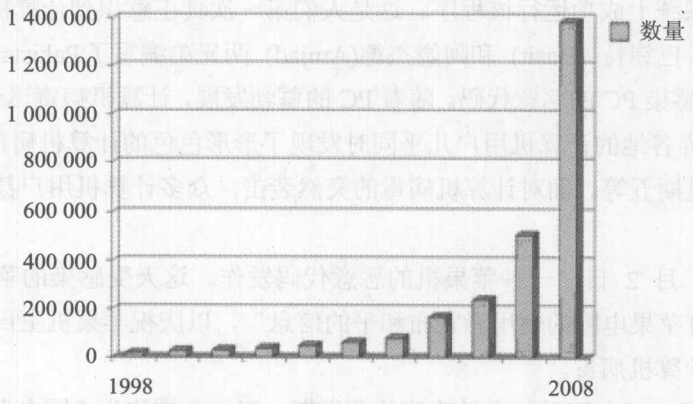


图 1-2　全球恶意代码数量增长图示(卡巴斯基实验室)

接下来，本书将以恶意代码发展过程中的关键环节为主线，回顾恶意代码从出现到蓬勃发展的历史过程中的一些关键环节。

自从 1946 年第一台电子计算机 ENIAC 问世以来，计算机与人们的生活已经越来越息息相关了，人们甚至已经无法在没有计算机的世界里生活了。但是人们发现就如同人会生病一样，计算机的世界里也存在病毒，计算机也会染病。那么，计算机病毒是如何一步一步地从无到有、从小到大发展到今天的呢？接下来的介绍可以解答读者的这一疑问。

在第一台商用计算机出现之前，伟大的计算机技术先驱——冯·诺依曼(John Von Neumann)在他的一篇论文《复杂自动装置的理论及组识的进行》里，就已经勾勒出了计算机病毒的蓝图。

计算机病毒这个短语最早是出现在科幻小说里的。1977 年夏天，托马斯·瑞安(Thomas.J. Ryan)的科幻小说《P-1 的春天》(The Adolescence of P-1)成为美国的畅销书。作者在这本书中描写了一种可以在计算机中互相传染的病毒，病毒最后控制了 7 000 台计算机，造成了一场灾难。不过，这在当时并没有引起人们的注意。

磁心大战(core war)是在冯·诺依曼病毒程序蓝图的基础上提出的概念。起初绝大部分的计算机专家都无法想象会存在这种能自我繁殖的程序，可是少数几个科学家默默地研究着这个问题。直到十年之后，在美国电话电报公司(AT&T)的贝尔(Bell)实验室中，这些概念在一种很奇怪的电子游戏中成形了，这种电子游戏称为磁心大战。

磁心大战玩法如下：双方各写一套程序并输入同一部计算机中，这两套程序在计算机系统内互相追杀，有时它们会放置一些关卡甚至有时会停下来修复被对方破坏的几行指令。

当被困时，它们可以把自己复制一次从而逃离险境，因为它们都在计算机的记忆磁心中游走，因此得名磁心大战。这个游戏的特点在于双方的程序进入计算机之后，玩游戏的人只能看着屏幕上显示的战况，而不能做任何更改，直到某一方的程序被另一方的程序完全“吃掉”为止。

1983年11月3日，弗雷德·科恩(Fred Cohen)博士研制出一种在运行过程中可以复制自身的破坏性程序。伦·艾德勒曼(Len Adleman)将这种破坏性程序命名为计算机病毒(Computer Viruses)，并在每周一次的计算机安全讨论会上正式提出，8小时后专家们在VAX 11/750计算机系统上成功运行该程序。这是人们第一次真正意识到计算机病毒的存在。

1986年初，巴锡特(Basit)和阿姆杰德(Amjad)两兄弟编写了Pakistan病毒，即Brain。Brain是第一个感染PC的恶意代码。随着PC的蓬勃发展，计算机病毒迅速发展壮大起来。

1987年世界各地的计算机用户几乎同时发现了形形色色的计算机病毒，如大麻、IBM圣诞树、黑色星期五等。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。

1988年3月2日，一种苹果机的恶意代码发作。这天受感染的苹果机停止工作，只显示“向所有苹果电脑的使用者宣布和平的信息”，以庆祝苹果机生日。这是第一个感染窗口系统的计算机病毒。

1988年冬天，正在康乃尔大学攻读的莫里斯，把一个被称为“蠕虫”的计算机病毒送进了美国最大的计算机网络——互联网。1988年11月2日下午5点，互联网的管理人员首次发现网络有不明入侵者。当晚，从美国东海岸到西海岸，互联网用户陷入一片恐慌。由于当时的网络非常有限，其破坏力没有得到充分发挥。其实，蠕虫的概念起源更早，在1982年，Shock和Hupp根据《The Shockwave Rider》一书中的概念提出了一种“蠕虫(Worm)”程序的思想。蠕虫的真正爆发却在10多年后，21世纪初，蠕虫在互联网中大爆发，其原理正是来自于莫里斯的蠕虫。

1989年全世界的计算机病毒攻击十分猖獗，我国也未幸免。其中“米开朗基罗”病毒给许多计算机用户造成了极大的损失。这个病毒比较著名的原因，除了它拥有一代艺术大师米开朗基罗的名字之外，更重要的是它的杀伤力非常强大。

1991年在“海湾战争”中，美军第一次将计算机病毒用于实战，在空袭巴格达的战斗前，成功地破坏了对方的指挥系统，使之瘫痪，保证了战斗的顺利进行，直至最后胜利。

1992年出现了针对杀毒软件的“幽灵”病毒，例如One-half。该病毒直接挑战简单的特征码扫描技术，随后，各个安全厂商推出了启发式扫描、含有通配符的特征码等技术来应对幽灵型病毒。

1996年首次出现针对微软公司Office的“宏病毒”。宏病毒的出现使病毒编制工作不再局限于晦涩难懂的汇编语言，由于书写简单，越来越多的病毒出现了。1997年被公认为信息安全界的“宏病毒年”。宏病毒主要感染Word、Excel等文件。如Word宏病毒，早期是用一种专门的Basic语言即Word Basic所编写的程序，后来使用Visual Basic。与其他计算机病毒一样，它能对用户系统中的可执行文件和数据文本类文件造成破坏。常见的宏病毒有Taiwan NO.1(台湾一号)、Setmd、Consept、Mdma等。

1998 年出现针对 Windows 95/98 系统的 CIH 病毒 (1999 年被公认为计算机反病毒界的 CIH 病毒年)。CIH 病毒是继 DOS 病毒、Windows 病毒、宏病毒后的第四类新型病毒。这种病毒与 DOS 下的传统病毒有很大区别，它是使用面向 Windows 的 VXD 技术来编制的。1998 年 8 月从台湾传入大陆的 CIH 病毒，共有 3 个版本——1.2 版、1.3 版、1.4 版。它们的发作时间分别是 4 月 26 日、6 月 26 日、每月 26 日。该病毒是第一个直接攻击、破坏硬件的计算机病毒，是破坏最为严重的病毒之一。它主要感染 Windows 95/98 的可执行程序，发作时破坏计算机 Flash BIOS 芯片中的系统程序，导致主板损坏，同时破坏硬盘中的数据。病毒发作时，硬盘驱动器不停旋转，硬盘上所有数据(包括分区表)被破坏，必须对硬盘重新分区才有可能挽救硬盘。同时，对于部分厂牌的主板(如技嘉和微星等)，会将 Flash BIOS 中的系统程序破坏，造成开机后系统无反应。1999 年 4 月 26 日，CIH 病毒在全球范围大规模爆发，造成近 6 000 万台计算机瘫痪，经济损失在 100 亿美元左右。

1999 年 Happy99 等完全通过 Internet 传播的蠕虫的出现标志着网络恶意代码将成为新的挑战。其特点就是利用 Internet 的优势，快速进行大规模的传播，从而使蠕虫在极短的时间内遍布全球。

2001 年 7 月中旬，一种名为“红色代码”的恶意代码在美国大面积蔓延，这个专门攻击服务器的恶意代码攻击了白宫网站，造成了全世界恐慌。8 月初，其变种“红色代码 2”针对中文系统作了修改，增强了对中文网站的攻击能力，开始在中国蔓延。“红色代码”通过黑客攻击手段利用服务器软件的漏洞来传播，它造成了全球 100 万个以上的系统被攻陷而导致瘫痪。这是计算机病毒与网络黑客首次结合，并对后来的计算机病毒产生了很大的影响。

2003 年，“2003 蠕虫王”在亚洲、美洲、澳大利亚等地迅速传播，造成了全球性的网络灾害。其中受害最严重的无疑是美国和韩国这两个 Internet 发达的国家。其中韩国 70% 的网络服务器处于瘫痪状态，网络连接的成功率低于 10%，整个网络速度极慢。美国不仅公众网络受到了破坏性攻击，甚至连银行网络系统也遭到了破坏，全国 1.3 万台自动取款机处于瘫痪状态。

2004 年是蠕虫泛滥的一年。中国计算机病毒应急中心的调查显示，2004 年 10 大流行病毒都是蠕虫，它们包括：

- 网络天空(Worm.Netsky)
- 高波(Worm.Agobot)
- 爱情后门(Worm.Lovgate)
- 震荡波(Worm.Sasser)
- SCO 炸弹(Worm.Novarg)
- 冲击波(Worm.Blaster)
- 恶鹰(Worm.Bbeagle)
- 小邮差(Worm.Mimail)
- 求职信(Worm.Klez)
- 大无极(Worm.SoBig)

2005年是特洛伊木马流行的一年。在经历了操作系统漏洞升级、杀毒软件技术改进后，蠕虫的防范效果已经大大提高，真正有破坏作用的蠕虫已经销声匿迹。然而，病毒制作者(Vxer)永远不甘寂寞，他们又开辟了新的高地——特洛伊木马。2005年的木马既包括安全领域耳熟能详的经典木马(例如，BO2K、冰河、灰鸽子等)，也包括很多新鲜的木马。简单举例如下。

① 闪盘窃密者(Trojan.UdiskThief)：该木马会判断计算机上移动设备的类型，自动把U盘里所有的资料都复制到计算机C盘的test文件夹下，这样可能造成某些公用计算机用户的资料丢失。

② 证券大盗(Trojan/PSW.Soufan)：该木马可盗取包括南方证券、国泰君安在内多家证券交易系统的交易账户和密码，被盗号的股民账户存在被人恶意操纵的可能。

③ 外挂陷阱(Trojan.Lineage.hp)：此木马可以盗取多个网络游戏的用户信息，用户通过登录某个网站，下载安装所需外挂程序后，便会发现外挂程序实际上是经过伪装的恶意代码，这个时候恶意代码便会自动安装到用户计算机中。

④ 我的照片 (Trojan.PSW.MyPhoto)：该木马试图窃取热血江湖、传奇、天堂2、中国工商银行、中国农业银行等数十种网络游戏及网络银行的账号和密码。该木马发作时，会显示一张照片使用户对其放松警惕。

2006年木马仍然是主流，其变种层出不穷。2006年上半年，江民反病毒中心共截获新恶意代码33 358种。据江民病毒预警中心监测的数据显示，1至6月全国共有7 322 453台计算机感染了病毒，其中感染木马的计算机2 384 868台，占病毒感染计算机总数的32.56%；感染广告软件计算机1 253 918台，占病毒感染计算机总数的17.12%；感染后门程序计算机664 589台，占病毒感染计算机总数的9.08%；感染蠕虫病毒计算机216 228台，占病毒感染计算机总数的2.95%；监测发现漏洞攻击代码计算机181 769台，占病毒感染计算机总数的2.48%；感染恶意脚本计算机15 152台，占病毒感染计算机总数的0.2%。由此可见，木马将是未来几年恶意代码的主流。

随着Internet的进一步发展，依赖互联网作为传播途径的计算机病毒成了当前最具威胁的破坏者。像冲击波、震荡波、灰鸽子等网络型恶意代码带来的损失都是不可估量的。表1-1显示了近年来几个经典计算机病毒带来的巨大危害。

表1-1　重大计算机病毒危害列表[1]

年　份	攻击行为发起者	受害PC数目(万台)	损失金额(亿美元)
2007	熊猫烧香	超过200	—
2006	木马和恶意软件	—	—
2005	木马	—	—
2004	Worm_Sasser	—	—

1 部分没有准确来源的数据没有列出。由于木马的特点在于窃取，因此，其破坏程度不可估计。

(续表)

年　份	攻击行为发起者	受害 PC 数目(万台)	损失金额(亿美元)
2003	Worm_MSBLAST	超过 140	—
2003	SQL Slammer	超过 20	9.5～12
2002	Klez	超过 600	90
2001	RedCode	超过 100	26
2001	Nimda	超过 800	60
2000	Love Letter	—	88
1999	CIH	超过 6 000	近 100

1.3　计算机病毒的分类

计算机病毒技术的发展，病毒特征的不断变化，给计算机病毒的分类带来了一定的困难。根据多年来对计算机病毒的研究，按照不同的体系可对计算机病毒进行如下分类。

1. 按病毒存在的媒体分类

根据病毒存在的媒体，病毒可以划分为网络病毒、文件病毒、引导型病毒和混合型病毒。

网络病毒：通过计算机网络传播感染网络中的可执行文件。

文件病毒：感染计算机中的文件(如 COM、EXE、DOC 等)。

引导型病毒：感染启动扇区(Boot)和硬盘的系统引导扇区(MBR)。

混合型病毒：是上述三种情况的混合。例如，多型病毒(文件和引导型)感染文件和引导扇区两种目标，这样的病毒通常都具有复杂的算法，它们使用非常规的办法侵入系统，同时使用了加密和变形算法。

2. 按病毒传染的方法分类

根据病毒的传染方法，可将计算机病毒分为引导扇区传染病毒、执行文件传染病毒和网络传染病毒。

引导扇区传染病毒：主要使用病毒的全部或部分代码取代正常的引导记录，而将正常的引导记录隐藏在其他地方。

执行文件传染病毒：寄生在可执行程序中，一旦程序执行，病毒就被激活，进行预定活动。

网络传染病毒：这类病毒是当前病毒的主流，特点是通过因特网进行传播。例如，蠕虫病毒就是通过主机的漏洞在网上传播的。

3. 按病毒破坏的能力分类

根据病毒破坏的能力，计算机病毒可划分为无害型病毒、无危险型病毒、危险型病毒和非常危险型病毒。

无害型病毒：除了传染时减少磁盘的可用空间外，对系统没有其他影响。

无危险型病毒：仅仅是减少内存、显示图像、发出声音及同类音响。

危险型病毒：在计算机系统操作中造成严重的错误。

非常危险型病毒：删除程序、破坏数据、清除系统内存和操作系统中重要的信息。

有些病毒对系统造成的危害，并不是本身的算法中存在危险的调用，而是当它们传染时会引起无法预料的灾难性的破坏。由病毒引起其他的程序产生的错误也会破坏文件和扇区，这些病毒也按照它们引起的破坏能力进行划分。目前的一些无害型病毒也可能会对新版的DOS、Windows和其他操作系统造成破坏。例如，在早期的病毒中，有一个名为Denzuk的病毒在360KB磁盘上不会造成任何破坏，但是在后来的高密度软盘上却能导致大量的数据丢失。

4. 按病毒的攻击目标分类

根据病毒的攻击目标，计算机病毒可以分为DOS病毒、Windows病毒和其他系统病毒。

DOS病毒：指针对DOS操作系统开发的病毒。目前几乎没有新制作的DOS病毒，由于Windows 9x病毒的出现，DOS病毒几乎绝迹。但DOS病毒在Windows 9x环境中仍可以进行感染活动，因此若执行染毒文件，Windows 9x用户的系统也会被感染。我们使用的杀毒软件能够查杀的病毒中一半以上都是DOS病毒，可见DOS时代DOS病毒的泛滥程度。但这些众多的病毒中除了少数几个让用户胆战心惊的病毒之外，大部分病毒都只是制作者出于好奇或对公开代码进行一定变形而制作的病毒。

Windows病毒：主要指针对Windows 9x操作系统的病毒。现在的电脑用户一般都安装Windows系统。Windows病毒一般感染Windows 9x系统，其中最典型的病毒有CIH病毒。但这并不意味着可以忽略系统是Windows NT系列(包括Windows 2000)的计算机。一些Windows病毒不仅在Windows 9x上正常感染，还可以感染Windows NT上的其他文件。

其他系统病毒：主要攻击Linux、UNIX和OS2及嵌入式系统的病毒。由于系统本身的复杂性，这类病毒数量不是很多。

1.4　计算机病毒的传播途径

传染性是计算机病毒最基本的特性，也是病毒赖以生存繁殖的条件，如果计算机病毒没有传播渠道，则其破坏性小，扩散面窄，难以大面积流行。因此计算机病毒必须要“搭载”到计算机上才能感染系统，通常它们是附加在某个文件上。

处于潜伏期的病毒在激发之前，不会对计算机内的信息进行破坏，即绝大部分磁盘信息没有遭到破坏。因此，只要消除没有发作的计算机病毒，就可保护计算机的信息。病毒的复制与传染过程只能发生在病毒程序代码被执行过后。也就是说，虽然有一个带有病毒程序的文件存储在你的计算机硬盘上，但是只要永远不去执行它，这个计算机病毒也就永