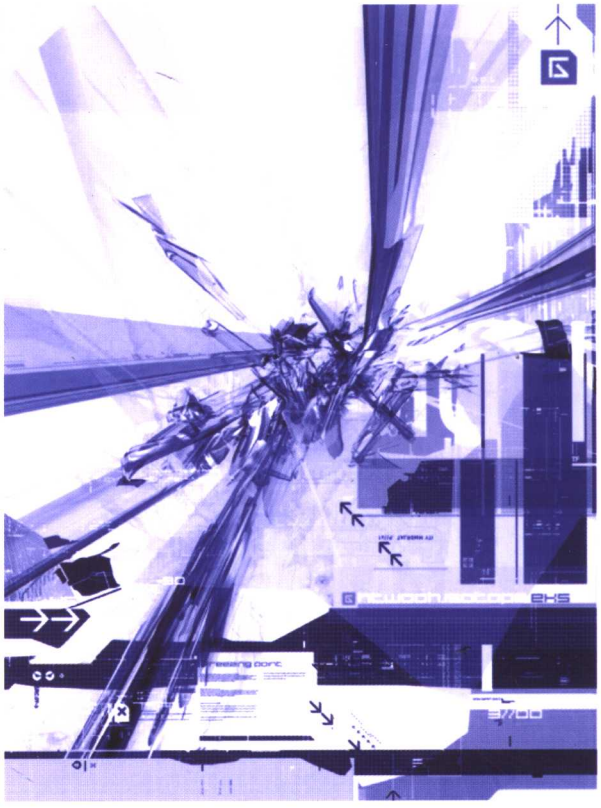
高等学校计算机应用规划教材

计算机病毒及其防范技术

- 计算机病毒概述
- 计算机病毒理论模型
- 计算机病毒结构分析
- 计算机病毒技术特征
- 特洛伊木马与宏病毒
- Linux 病毒技术
- 移动终端恶意代码
- 计算机病毒查杀方法
- 计算机病毒防治技术
- OAV 代码分析与使用
- 常用杀毒软件及其解决方案
- 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

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、计算机病毒的理论模型、计算机病毒的结构分析、计算机病毒技术特征、特洛伊木马、宏病毒、Linux 病毒技术、移动终端恶意代码、计算机病毒查杀方法、计算机病毒防治技术、OAV 代码分析与使用、常用杀毒软件及其解决方案和计算机病毒防治策略。

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、实验用源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。

图书在版编目（CIP）数据
计算机病毒及其防范技术/刘功申 编著. —北京：清华大学出版社，2008.2
(高等学校计算机应用规划教材)

ISBN 978-7-302-16923-9

I. 计… II.刘… III.计算机病毒－防治－高等学校－教材 IV.TP309.5
中国版本图书馆 CIP 数据核字（2008）第 009203 号

责任编辑：刘金喜　高晓晴
封面设计：康　博
版式设计：孔祥丰
责任校对：胡雁翎
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
c－service@tup.tsinghua.edu.cn
社 总 机：010-62770175　**邮购热线**：010-62786544
投稿咨询：010-62772015　**客户服务**：010-62776969
印 刷 者：北京市人民文学印刷厂
装 订 者：三河市兴旺装订有限公司
经　　销：全国新华书店
开　　本：185×260　**印　　张**：29.25　**字　　数**：675 千字
版　　次：2008 年 2 月第 1 版　　**印　　次**：2008 年 2 月第1 次印刷
印　　数：1～5000
定　　价：42.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103　　产品编号：025009－01

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、社会稳定方面发挥了双刃剑的作用，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 4 年，研发工作 3 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，重点分析计算机病毒的检测和清除技术。此外，还对预防计算机病毒的策略和防治方案进行了探讨。

本书共分 13 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：计算机病毒的理论模型。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：计算机病毒的结构分析。主要介绍在 DOS、Windows 9x、Windows 2000 平台下传统病毒的功能模块和工作机制。并以 3 种平台下的可执行文件结构为线索，在分析这些文件结构的基础上，引入不同平台的病毒编制技术。为了保证教材的系统性，本章还简要介绍了引导型病毒。

第 4 章：计算机病毒技术特征。本章是第三章技术的发展和提高。不仅对实战型病毒所必需的计算机病毒技术特征进行了介绍。而且还探讨了一些采用特殊技术的计算机病毒，例如蠕虫病毒、基于 Outlook 漏洞的病毒、Webpage 恶意代码和流氓软件等。

第 5 章：特洛伊木马。为了使读者充分了解特洛伊木马，本章详细分析了木马的技术特征、木马入侵的一些常用技术以及木马入侵的防范和清除方法。此外，还对几款常见木马程序的防范经验作了较为详细的说明。

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。本章在了解 Linux 安全问题的基础上，探讨了 Linux 病毒的

概念，分析了 Linux 可执行文件格式(ELF)的运行机理。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：计算机病毒查杀方法。主要内容包括计算机病毒的诊断原理和方法、计算机病毒清除的原理和方法、自动诊断计算机病毒的源码分析及关键算法及几类典型病毒的查杀经验等。

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，有些技术穿插在其他章节进行介绍。本章内容包括计算机病毒防治技术的现状、一些非常重要的计算机病毒防治技术以及数据备份和数据恢复在计算机病毒防治领域的重要性等。

第 11 章：OAV(Open Antivirus)代码分析与使用。OAV 是在 2000 年 8 月由德国开源爱好者发起的为开源社区的反病毒开发者提供交流和项目管理的资源平台。本章详细分析了 OAV 的框架和主要函数，同时详细介绍了其使用方法。

第 12 章：常用杀毒软件及其解决方案。本章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 13 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 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 和第 12 章的编写。

在本书完稿之际，作者对上海交通大学教材出版基金的资助表示衷心感谢；感谢教学 4 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；感谢我的太太和刚刚出生的孩子，该书稿的完成离不开家人的默默支持。

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。

作　　者

2007 年 7 月

于思源湖畔

目　录

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在 2001 年为 73%，2002 年为 84%，2003 年为 85%，成逐年上升的趋势。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。

1.2　计算机病毒的发展历史及其危害程度

计算机病毒的来源多种多样，有的是计算机工作人员或业余爱好者为了纯粹寻开心而制造出来的，有的则是软件公司对自己的产品被非法复制而制造的报复性惩罚，因为他们发现病毒比加密对付非法复制更有效且更有威胁，这种情况助长了病毒的传播。还有一种情况就是蓄意破坏，它分为个人行为和政府行为两种。个人行为多为雇员对雇主的报复行为，而政府行为则是有组织的战略战术手段(据说在海湾战争中，美国国防部的一个秘密机构曾对伊拉克的通信系统进行了有计划的病毒攻击，一度使伊拉克的国防通信陷于瘫痪)。

另外还有些病毒是用于研究或实验而设计的“有用”程序，由于某种原因失去控制扩散出实验室或研究所，从而成为危害四方的计算机病毒。

但是，无论病毒来源于什么地方，它们给用户带来的危害不外乎如图 1-1 所示的几种。

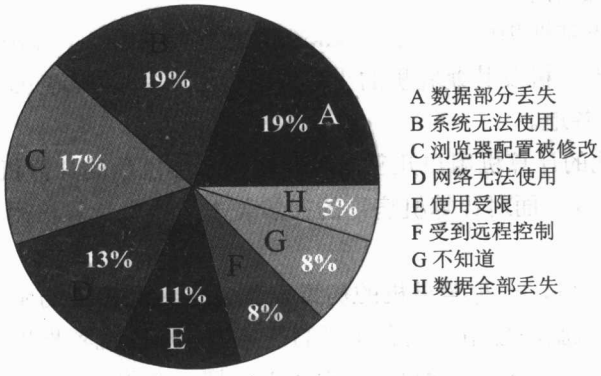


图 1-1　计算机病毒的危害情况

自 1946 年第一台“冯·诺依曼”体系的计算机 ENIAC 问世以来，计算机与人们的生活已经越来越息息相关了，人们甚至已经无法生活在没有计算机的世界里了。但是就如同人会生病一样，计算机的世界里面也存在病毒，计算机也会生病。那么，计算机病毒是如何一步步地从无到有、从小到大发展到今天的呢？下面的介绍可以解除你的这一疑问。

其实，计算机病毒概念的起源相当早。在第一部商用电脑出现之前，伟大的计算机先驱——冯·诺伊曼在他的一篇论文《复杂自动装置的理论及组织的进行》里，就已经勾勒出了病毒程序的蓝图。

计算机病毒这个词语最早是出现在科幻小说里。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 7000 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。

“磁芯大战(core war)”是在冯·诺伊曼病毒程序蓝图的基础上提出的概念。起初绝大部分的电脑专家都无法想象这种会自我繁殖的程序是可能的，只是少数几位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型了，这种电子游戏叫做“磁芯大战”。

磁芯大战玩法如下：双方各写一套程序并将程序输入到同一部电脑中，这两套程序在电脑系统内互相追杀，有时它们会放下一些关卡甚至会停下来修复(重新写)被对方破坏的几行指令。当它被困时，也可以把自己复制一次从而逃离险境，因为它们都在电脑的记忆磁芯中游走，所以得到了“磁芯大战”之名。这个游戏的特点在于双方的程序进入电脑之后，玩游戏的人只能看着屏幕上显示的战况，而不能对程序做任何更改，一直到某一方的程序被另一方的。

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 VAX11 / 750 计算机系统上成功运行该程序。这样，第一个病毒实验成功。人们第一次真正意识到计算机病毒的存在。

1986 年初，在巴基斯坦的拉合尔 (Lahore)，巴锡特 (Basit) 和阿姆杰德(Amjad) 两兄弟经营着一家 IBM-PC 机及其兼容机的小商店。他们编写的 Pakistan 病毒，即 Brain，在一年内流传到了世界各地。

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，一种苹果机的病毒发作。这天受感染的苹果机都停止了工作，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。

1988 年冬天，正在康乃尔大学攻读的莫里斯，把一个称为“蠕虫”的电脑病毒送进了美国最大的电脑网络——因特网。1988 年 11 月 2 日下午 5 时，因特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，因特网用户陷入一片恐慌。

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极大损失。这种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，更重要的是它具有非常强大的杀伤力。

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中，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，如 One-half。

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，因此，越来越多的病毒出现了。

1997 年被公认为计算机反病毒界的“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 WordBasic 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 Tw no.1(台湾一号)、Setmd、Consept、Mdma 等。

1998 年出现针对 Windows 95/98 系统的病毒，例如，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不同，它使用面向 Windows 的 VXD 技术编制。1998 年 8 月份从中国台北传入中国大陆的 CIH 病毒共有三个版本：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 日和每月 26 日。该病毒是第一个直接攻击、破坏硬件的计算机病毒，也是破坏最为严重的病毒之一。它主要感染 Windows95/98 的可执行程序，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。当病毒发作时，硬盘驱动器不停旋转，硬盘上所有数据(包括分区表)被破坏，只有对硬盘重新分区才有可能挽救硬盘。同时，病毒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 6000 万台电脑瘫痪。中国也未能在这次灾难中幸免，直接经济损失达 8000 万元，间接经济损失超过了 10 亿元。该病毒给整个世界带来的经济损失在数十亿美元以上。

1999 年 Happy99 等完全通过 Internet 传播的病毒的出现标志着 Internet 病毒将成为病毒新的增长点。其特点就是利用 Internet 的优势，快速进行大规模的传播，从而使病毒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”的病毒在美国大面积蔓延，这个专门攻击服务器的病毒攻击了白宫网站，造成了全世界的恐慌。8 月初，其变种“红色代码 II”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”病毒通过一种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从而导致瘫痪。这是计算机病毒与网络黑客首次结合，可以说对后来的病毒产生了很大的影响。

2003 年，“2003 蠕虫王”病毒在亚洲、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因特网发达的国家。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的攻击，而且连银行网络系统也遭到了破坏，全国 1.3 万台的自动取款机处于瘫痪状态。

2004 年是“蠕虫”泛滥的一年，根据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病毒，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)

随着 Internet 的进一步发展，蠕虫病毒成为当前最具威胁的病毒。像冲击波、震荡波等带来的损失都是不可估量的。

2005 年是木马流行的一年。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，Vxer(病毒编制者)们永远不甘寂寞，他们又开辟了新的高地——计算机木马。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：

“闪盘窃密者(Trojan.UdiskThief)”病毒：该木马病毒会判定电脑上移动设备的类型，自动把U盘里所有的资料都复制到电脑C盘的test文件夹下，这样可能造成某些公用电脑用户的资料丢失。

“证券大盗”(Trojan/PSW.Soufan)病毒：该木马病毒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。

“外挂陷阱(Trojan.Lineage.hp)”病毒：此病毒可以盗取多个网络游戏的用户信息，如果用户通过登录某个网站，下载安装所需外挂后，便会发现外挂实际上是经过伪装的病毒，这个时候病毒便会自动安装到用户电脑中。

“我的照片 (Trojan.PSW.MyPhoto)”病毒：该病毒试图窃取《热血江湖》、《传奇》、《天堂II》、《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。该病毒发作时，会显示一张照片使用户对其放松警惕。

2006年木马仍然是病毒主流，其变种层出不穷。2006年上半年，江民反病毒中心共截获新病毒33358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7322453台计算机感染了病毒，其中感染木马病毒的电脑有2384868台，占病毒感染电脑总数的32.56%，感染广告软件的电脑有1253918台，占病毒感染电脑总数的17.12%，感染后门程序的电脑有664589台，占病毒感染电脑总数的9.03%，感染蠕虫病毒的电脑有216228台，占病毒感染电脑总数的2.95%，监测发现漏洞攻击代码感染的电脑181769台，占病毒感染电脑总数的2.48%，脚本病毒感染的电脑15152台，占病毒感染电脑总数的2.06%。由此可见，木马将是未来几年的病毒主流。

表1-1显示了近年来几个病毒带来的巨大危害。

表1-1　重大病毒危害列表

年　份	攻击行为发起者	受害PC数目	损失金额(美元)
2006	木马和恶意软件	(破坏程度不可估计)	(破坏程度不可估计)
2005	木马	(破坏程度不可估计)	(破坏程度不可估计)
2004	Worm_Sasser (震荡波)	(破坏程度不可估计)	(破坏程度不可估计)
2003	Worm_MSBLAST (冲击波)	超过140万台	(破坏程度不可估计)
2003	SQL Slammer	超过20万台	9.5亿至12亿
2002	Klez	超过600万台	90亿
2001	RedCode	超过100万台	26亿
2001	NIMDA	超过800万台	60亿
2000	Love Letter	(破坏程度不可估计)	88亿
1999	CIH	超过6000万台	近100亿

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，特点是通过因特网络进行传播。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、无危险病毒、危险型病毒和非常危险型病毒**。

无害型：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：仅仅是减少内存、显示图像、发出声音及同类音响。

危险型：在计算机系统操作中造成严重的错误。

非常危险型：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. 按病毒算法分类

根据病毒特有的算法，病毒可以分为**伴随型病毒、蠕虫型病毒、寄生型病毒、练习型病毒、诡秘型病毒和幽灵病毒**。

伴随型病毒：这一类病毒并不改变文件本身，它们根据算法产生EXE文件的伴随体，具有同样的名字和不同的扩展名(COM)，例如：XCOPY.EXE的伴随体是XCOPY.COM。病毒把自身写入COM文件并不改变EXE文件，当DOS加载文件时，伴随体优先被执行，再由伴随体加载执行原来的EXE文件。

蠕虫型病毒：通过计算机网络传播，不改变文件和资料信息，利用网络从一台机器的内存传播到其他机器的内存，计算网络地址，将自身的病毒通过网络发送。有时它们在系统中存在，一般除了内存不占用其他资源。

寄生型病毒：依附在系统的引导扇区或文件中，通过系统的功能进行传播。

练习型病毒：病毒自身包含错误，不能进行很好的传播，例如一些在调试阶段的病毒。

诡秘型病毒：它们一般不直接修改DOS中断和扇区数据，而是通过设备技术和文件缓冲区等对DOS内部进行修改，不易看到资源，使用比较高级的技术。利用DOS空闲的数据区进行工作。

幽灵病毒：这一类病毒使用一个复杂的算法，使自己每传播一次都具有不同的内容和长度。它们一般由一段混有无关指令的解码算法和经过变化的病毒体组成。

5. 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。