普通高等教育“十一五”国家级规划教材

教育部“高等学校教学质量与教学改革工程”立项项目

教育部第二批特色专业建设——信息安全配套教材

赖英旭 钟 玮 编著

李 健 主审

计算机病毒与防范技术

计算机科学与技术专业实践系列教材

清华大学出版社

计算机病毒与防范技术

普通高等教育“十一五”国家级规划教材

计算机科学与技术专业实践系列教材

教育部“高等学校教学质量与教学改革工程”立项项目

计算机病毒与防范技术

赖英旭 钟 玮 编著

李 健 主审

清华大学出版社

北京

内 容 简 介

本书全面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、防治和对抗等进行了深入的分析和探讨。

本书从计算机病毒的结构、原理、源代码等方面进行了深入的分析，介绍了计算机病毒的自我隐藏、自加密、多态、变形等基本的对抗分析和自我保护技术。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技术，并详细地介绍了几款杀毒软件的工作原理和特点。

本书通俗易懂，注重可操作性和实用性。对典型的计算机病毒代码进行剖析，使读者能够举一反三。

本书适合用作信息安全、计算机与其他信息学科本科生的教材，也可作为广大计算机用户、计算机安全技术人员的技术参考书，同时，也可用作计算机信息安全职业培训的教材。

图书在版编目（CIP）数据

计算机病毒与防范技术/赖荣旭，钟玮编著. —北京：清华大学出版社，2011.6
（计算机科学与技术专业实践系列教材）
ISBN 978-7-302-24401-1

Ⅰ. ①计… Ⅱ. ①赖… ②钟… Ⅲ. ①计算机病毒－防治－高等学校－教材 Ⅳ. ①TP309.5

中国版本图书馆 CIP 数据核字(2010)第 260402 号

责任编辑：汪汉友　顾　冰
责任校对：白　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：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185×260　　**印　　张**：15　　**字　　数**：365　千字
版　　次：2011 年 6 月第 1 版　　**印　　次**：2011 年 6 月第 1 次印刷
印　　数：1～4000
定　　价：26.00 元

产品编号：035508-01

普通高等教育“十一五”国家级规划教材
计算机科学与技术专业实践系列教材

编 委 会

前　言

随着计算机技术的不断发展和网络应用的普及，计算机系统广泛地应用于生活、管理和办公中，成为人类社会不可或缺的一部分。但是，计算机技术和网络的高速发展在给人们带来巨大便利的同时，也带来了各种各样的威胁。其中，计算机病毒是最不安全的因素之一。随着网络的飞速发展，计算机病毒的传播速度也越来越快，如果不能运用有效手段预测并查杀计算机病毒，将对社会造成极大的经济损失。如何防治计算机病毒已成为计算机安全领域研究的重要课题。

本书由北京工业大学教师和北京瑞星信息技术有限公司的工程师共同编写。其中，北京工业大学教师从事大学本科计算机病毒教学 4 年，研发工作 3 年；瑞星公司工程师有多年从事计算机病毒防范技术研发工作的经验。

书中重点分析了计算机病毒的运行机制，并采用大量代码剖析的方式讲解常见计算机病毒。在分析病毒技术的基础上，本书重点介绍了计算机病毒的检测和清除技术。

本书分为 8 章，具体内容如下所示。

第 1 章：计算机病毒概述。本章从生物病毒入手，介绍了计算机病毒的定义、特征和分类，接着阐述了计算机病毒和破坏程序的发展。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。

第 2 章：Windows 文件型病毒。本章主要介绍文件型病毒特点与危害、PE 文件格式和文件型病毒感染机制，还给出了典型文件型病毒的代码片段，剖析文件型病毒编制技术。

第 3 章：木马病毒分析。本章着重介绍木马病毒的特点及危害、木马病毒的结构和工作原理等。为了让读者更充分地了解木马病毒的技术特征，还对典型木马病毒进行了解析。

第 4 章：蠕虫病毒分析。为了使读者充分了解蠕虫，本章详细分析了蠕虫的技术特征、蠕虫入侵的一些常用技术以及蠕虫入侵的防范和清除方法。此外，还对几款常见蠕虫程序的防范经验做了较为详细的说明。

第 5 章：其他恶意代码分析。本章探讨了一些采用特殊技术的计算机病毒，如脚本病毒、即时通信病毒、网络钓鱼、流氓软件等。通过对典型病毒的代码剖析，对上述计算机病毒所采用的技术特征进行了介绍。

第 6 章：计算机病毒常用技术。本章介绍计算机病毒的加密、多态技术，以及计算机病毒的反跟踪、反调试、反分析技术，使读者了解对计算机病毒进行检测是件很复杂的事情。

第 7 章：计算机病毒对抗技术。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等。

第 8 章：反病毒产品及解决方案。本章通过介绍企业反病毒技术和工具，从而为一些典型病毒防治体系提供解决方案。

本书由北京工业大学的赖英旭、杨震、刘静和北京瑞星信息技术有限公司的钟玮、杨威、叶超、孔静超、白子潘、徐传宇、毛钧和刘锋共同编写，全书最后由赖英旭和杨震统稿，李健

审定。

与本书相关的研究工作和编写工作受到了教育部和北京市“信息安全特色专业建设项目”资助。本书从各种论文、书籍、期刊以及 Internet 中引用了大量的资料，在文字的录入和整理中，得到了李健老师的帮助，在此谨向他们表示衷心感谢。

由于时间和水平有限，难免有误，恳请读者批评指正，使得本书能得以改进和完善。

作　者

2011 年 1 月于北京

目　录

第 1 章　计算机病毒概述

1.1　计算机病毒简介

生物界的“病毒”(virus)是一种没有细胞结构、只是由蛋白质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 病毒、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被看到,而且不能独立生存,必须寄生在其他生物的活细胞里,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。

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具有相似的特点。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。计算机病毒结构如图 1-1 所示,一般由引导模块、条件判断模块、表现模块、传染模块、掩饰模块等组成。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普遍所接受的观点,可以总结出计算机病毒的十大特征,即非法性、隐藏性、潜伏性、可触发性、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,1.2 节将对计算机病毒的十大特征进行详细论述。

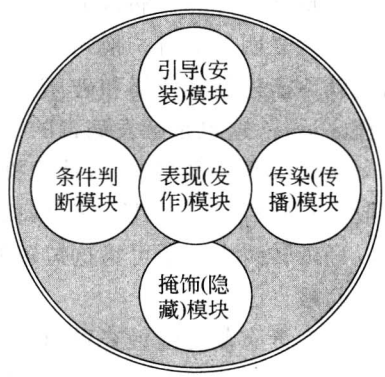

图 1-1　计算机病毒的结构

需要指出的是,单独根据以上某一个特征不能判断某个程序是否为病毒。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,也不具有病毒的其他大部分特征。

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："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"。此定义具有法律性和权威性。但是由于立法较早，为了涵盖近年来出现的新型恶意代码，例如蠕虫、木马等，国家又陆续颁布了《中华人民共和国计算机信息网络国际联网管理暂行规定》、《计算机病毒防治管理办法》等相应的法律法规。尽管如此，随着计算机技术日新月异的发展，在现行法律中，目前仅有少数法律条文可以适用于现在的计算机病毒技术发展现状。因此为使法律法规跟上计算机技术的迅猛发展，必须统一完善法律法规、明确执法主体，使国家信息安全得到真正的保障。

1.2 计算机病毒的特征

1. 非法性

在正常情况下，当计算机用户调用执行一个合法程序时，会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或调用正常数据时，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"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"。

例如第 4 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，正像前面讲到的，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运行，这也是触发病毒的一种手段。

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 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，使之很难被察觉，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被标为坏簇的扇区中，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存在；还有一种比较常见的隐藏方式是将病毒文件放在 Windows 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，在系统启动前就会发作。一些蠕虫病毒非常注重隐藏和伪装自己，例如某些通过邮件传播的蠕虫病毒，不但伪造邮件的主题和正文，还会利用社会工程学知识引诱用户打开邮件，

并且可以使用双扩展名的病毒文件作为附件，例如将病毒体命名为 ABC.jpg.exe，使用户以为病毒是一个图形文件，从而丧失警惕。还有些病毒借助系统的漏洞传播，利用漏洞来隐藏和传播病毒体，如果用户没有对操作系统添加或安装相应的补丁程序，病毒便无法被彻底清除。

如果不经过代码分析，很难区分病毒程序与正常程序。一般在没有防护措施的情况下，计算机病毒程序取得系统控制权后，可以在很短的时间里传染大量程序。而且受到传染后，计算机系统通常仍能正常运行，用户不会感到任何异常。总之，病毒会使用更巧妙的方法隐藏自己，使之不容易被发现。正是由于具有隐蔽性，计算机病毒得以在用户没有察觉的情况下扩散到上百万台计算机中。计算机用户如果掌握了这些病毒的隐藏方式，加强对日常文件的管理，计算机病毒便无处藏身了。

3. 潜伏性

计算机病毒具有依附于其他媒体而寄生的能力，把这种媒体称为计算机病毒的宿主。依靠病毒的寄生能力，病毒传染合法的程序和系统后，不立即发作，而是悄悄隐藏起来，然后在用户不察觉的情况下进行传染。这样，病毒的潜伏性越好，它在系统中存在的时间也就越长，病毒传染的范围也越广，其危害性也越大。

计算机病毒在传染计算机系统后，其触发时间是由发作条件来确定的。在发作条件满足前，病毒可能在系统中没有表现症状，从而不影响系统的正常运行。

大部分病毒在感染系统之后一般不会马上发作，它可长期隐藏在系统中，只有在满足其特定条件时才启动其表现(破坏)模块。只有这样它才可进行广泛传播。如 PETER-2 在每年 2 月 27 日会提三个问题，答错后会将硬盘加密。著名的“黑色星期五”在逢 13 号的星期五发作。中国的“上海一号”会在每年 3 月、6 月及 9 月的 13 日发作。当然，最令人难忘的便是 26 日发作的 CIH，这些病毒在平时会隐藏得很好，只有在发作日才会露出本来面目。

4. 可触发性

计算机病毒一般都有一个或者几个触发条件，满足其触发条件或者激活病毒的传染机制就会使病毒发作或使之进行传染。激发的本质是一种条件控制，病毒体根据病毒炮制者的设定，被激活并发起攻击。病毒被激发的条件可以与多种情况联系起来，如满足特定的时间或日期，期待特定用户识别符出现，特定文件的出现或使用，一个文件使用的次数超过设定数等。

按照时间触发的病毒很多，如 CIH 病毒。它的 v1.2 版本的发作日期是每年的 4 月 26 日，这个时间指的是计算机的系统时间；而 CIH 病毒的 v1.3 版本的发作日期是每年的 6 月 26 日；v1.4 版本的发作日期是每月的 26 日。很多人都有一个错误的想法，以为只要将系统时间调整到其他的日期，就可以避免病毒的发作。其实按照时间发作只是病毒触发的条件之一，而且系统时间没有及时调整回来，或者满足病毒的其他触发条件时，病毒还是会被触发的。调整时间只是应急的办法，根本的解决办法还是彻底清除病毒体。

按照一定条件触发的病毒也很多，比如，当你试图更改或运行某些文件时病毒就发作。Happytime(欢乐时光)病毒发作的条件是月份与日期之和等于 13，这是按照一定的逻辑条件来发作的病毒。另外，“求职信”病毒在单月的 6 日和 13 日发作。但绝大多数病毒是随机发作或者运行后发作的。

要注意的是，病毒的传播和发作是两个完全不同的问题，平时所遇到的大多数问题是病

毒发作引起的，因为病毒发作的现象比较明显，比如文件被删除或计算机无法使用。而病毒传播时由于其所具有的隐蔽性和潜伏性，通常不被人们注意，但其一旦发作就会造成重大的损失。所以要尽可能在病毒传播时及时清除病毒，等到病毒发作时才意识到，可能为时已晚了。

5. 表现性

无论何种病毒程序，一旦侵入系统，都会对操作系统的运行造成不同程度的影响。即使不直接产生破坏作用的病毒程序也要占用系统资源（如占用内存空间、占用磁盘存储空间、系统运行时间等）。而绝大多数病毒程序要显示一些文字或图像，影响系统的正常运行；还有一些病毒程序会删除文件、加密磁盘中的数据，甚至摧毁整个系统和数据，使之无法恢复，从而造成无可挽回的损失。因此，病毒程序的表现发作轻则降低系统工作效率，重则导致系统崩溃和数据丢失。病毒程序的表现性或破坏性体现了病毒设计者的真正意图。

一般来讲，带有个人情绪或者政治目的的病毒往往表现力比较强，例如比较著名的“中国黑客”病毒，病毒会利用聊天工具 QQ 发送即时信息，如图 1-2 所示。

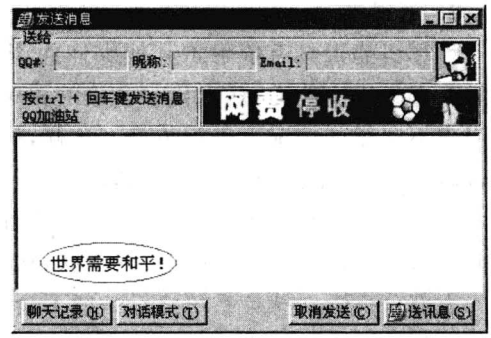

图 1-2 “中国黑客”病毒发作现象

6. 破坏性

计算机病毒造成的最显著后果是破坏计算机系统，并使之无法正常工作或删除用户保存的数据。无论是占用大量系统资源导致计算机无法正常使用，还是破坏文件，甚至毁坏计算机硬件，都会影响用户正常使用计算机。

病毒根据其破坏性可分为良性病毒和恶性病毒。

绝大多数被认定为病毒的程序都具有恶意破坏性的特征，但也有一些病毒程序并不具有恶意破坏性，我们把没有恶意破坏性的程序称为良性病毒。例如，某些良性病毒运行后会在屏幕上出现一些可爱的卡通形象，或演奏一段音乐。编写这类小程序也许仅仅是因为好玩，或开个玩笑，甚至可以被看做一个小游戏。但是，这并不代表其没有危害性。这类病毒有可能占用大量的系统资源，导致系统无法正常使用。

除了良性病毒以外，绝大多数病毒是恶性病毒，这类恶性病毒对计算机系统来说是很危险的。比如 WYX 病毒，该病毒是典型的引导区病毒，其发作时会改写计算机硬盘引导扇区的信息，使系统无法找到硬盘上的分区。由于硬盘上的所有数据都是通过硬盘分区表和文件分配表来确定的，所以如果计算机硬盘上的这些重要信息丢失或发生错误，用户不但无法正常访问硬盘上的所有数据，甚至在开机时，计算机会显示找不到引导信息，出现硬盘没有分区等错误信息提示，给用户的工作、生活造成很大的损失。

病毒的破坏方式是多种多样的。例如，Happytime 病毒在发作时会删除文件，并启动大量的病毒进程，导致计算机系统资源的严重缺乏直至计算机无法工作。还有破坏并且覆盖文件的 CIH 和“求职信”病毒，发作时会用垃圾代码来覆盖用户的文件，这种破坏造成的危害比简单的删除或格式化硬盘更为严重，往往会造成不可修复的破坏，这也反映出病毒编制者的险恶用心。有的病毒以恶作剧的形式破坏系统，如“白雪公主”病毒（见图 1-3），病毒在发作时用巨大的黑白螺旋图案占据屏幕的大部分位置，使计算机使用者无法进行任何操作。

图 1-3 “白雪公主”病毒发作现象

7. 传染性

传染性是计算机病毒最重要的特征，是判断一段程序代码是否为计算机病毒的依据。生物病毒通过传染从一个生物体扩散到另一个生物体，在适当的条件下，它可以大量繁殖，并使被感染的生物体表现出病症甚至死亡。同样，计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。只要一台计算机染毒，如不及时处理，那么病毒会在这台计算机上迅速扩散，其中的大量文件（一般是可执行文件）会被感染。而被感染的文件又成了新的传染源，再与其他机器进行数据交换或通过网络接触，病毒会继续进行传染。由于目前计算机网络日益发达，计算机病毒可以在极短的时间内通过 Internet 传遍世界。正常的计算机程序一般不会将自身的代码强行连接到其他程序之上，而病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。计算机病毒可通过各种可能的渠道传染其他的计算机。当你在一台计算机上发现了病毒时，曾在这台计算机上用过的移动硬盘、U 盘往往已经感染上了病毒，而与这台计算机联网的其他计算机也许也被感染上了该病毒。因此传染性是计算机病毒最重要的特征，是否具有传染性是判断一个程序是否为计算机病毒的最重要条件之一。

近一段时期，蠕虫类病毒可以说是传播速度最快、传播范围最广的病毒了。近年来，随着 Internet 的迅速发展，人们在工作和生活中也越来越依赖互联网，E-mail 这种联系方式也因其方便快捷的优点被人们广泛采用。不仅个人用户使用，正式的商业联系和各类组织、政府机构之间传递信息也是通过 E-mail 完成的。因此病毒的编制者就利用了 E-mail 的这个特点，使所编制的病毒通过 E-mail 的方式来传播，这种传播方式不仅传播范围广，而且传播的速度也非常快。此类病毒通常会盗取计算机中保存的邮件联系人地址信息，通过向这些地址发送带病毒邮件来大量复制自身。所以，蠕虫病毒有时也被称为 E-mail 病毒。

“美丽莎”、SirCam、Nimda、“求职信”等病毒就是通过这种方式传播的，它们的传播速度和范围是非常惊人的，据统计 24 小时之内便可通过 E-mail 传播遍全世界。而且 Nimda 和“求职信”病毒不仅通过邮件传播，还可以通过局域网文件共享和操作系统的漏洞等多种方式进行传播，其传播能力更强。

8. 针对性

计算机病毒具有针对特定计算机系统或计算机程序进行感染的特性。一种计算机病毒(版本)并不能感染所有的计算机系统或计算机程序，有的病毒是感染 Apple 公司的 Macintosh 机的，有的病毒是感染 IBM PC 的，有的病毒感染磁盘引导区，有的病毒感染可执行文件等。

9. 变异性

计算机病毒在发展、演化过程中可以产生变种。有些病毒能够产生几十种甚至上百种变种。既然计算机病毒是一段特殊的程序，了解病毒程序的人就可以根据其个人意图随意改动，从而衍生出另一种不同于原版病毒的新病毒或称“变种”，这种衍生出的病毒可能与原先的计算机病毒有很相似的特征，所以被称为原病毒的一个变种。如果衍生的计算机病毒已经与以前的计算机病毒有了很大差别甚至是根本性的差别，则此时就会将其认为是一种新的计算机病毒。变种或新的计算机病毒可能比原计算机病毒有更大的危害性。

10. 不可预见性

从对病毒的检测方面来看，病毒还有不可预见性。不同种类病毒的代码千差万别，但有些行为是共有的(如驻留内存、修改中断等)。有些人利用病毒的这种共性，制作了声称可检查所有病毒的程序。这种程序的确可以查出一些新病毒，但由于目前的软件种类极其丰富，且某些正常程序也使用了类似病毒的操作甚至借鉴了某些病毒的技术，所以使用这种方法对病毒进行检测势必会造成较多的误报情况。而且病毒的制作技术也在不断提高，病毒对反病毒软件来说永远是超前的，因此从病毒检测方面来看，计算机病毒还具有一定的不可预见性。

1.3 计算机病毒的分类

从第一个病毒问世以来，病毒的数量就在不断增加。根据每年从计算机用户反馈的有关病毒的信息分析，计算机病毒数量的增长已经从 20 世纪 90 年代初的每月几种达到了现在的每天 200 种以上。

从已经发现的计算机病毒来看，小的病毒程序只有几十条指令，不到上百个字节，而大的病毒程序简直像个操作系统，由上万条指令组成。有些病毒传播速度很快，并且一旦侵入计算机，就会立即摧毁系统；而另外一些病毒则有较长的潜伏期，感染后需要经过两年至三年甚至更长时间才发作；有些病毒感染系统内所有的程序和数据；有些病毒只对某些特定的程序或数据感兴趣；而有的病毒则对程序或数据毫无兴趣，只是不断地自身繁衍，抢占硬盘空间，不做其他任何事情。

由于计算机病毒及其所处环境的复杂性，以某种方式遵循单一标准为病毒分类已无法达到对病毒的准确认识，也不利于对病毒的分析与防治。在本节中，将从多个角度对计算机病毒进行详细分类。

需要说明的是，按照计算机病毒的特点及特性，其分类方法有许多种。由于同一种病毒可能同时具备多种特征，因此在分类隶属关系上会产生交叉。

1.3.1 根据寄生的数据存储方式划分

根据寄生的数据存储方式计算机病毒可划分为三种类型：引导区型、文件型和混合型。

1. 引导区型病毒

直到20世纪90年代中期，引导区型病毒一直是最流行的计算机病毒类型，主要通过软盘在DOS操作系统里传播。引导区型病毒会感染软盘中的引导区，蔓延到用户硬盘，并能感染到用户盘中引导区的“主引导记录”。一旦硬盘中的引导区被病毒感染，病毒就试图感染每一个插入计算机软盘的引导区。

引导区型病毒是这样工作的：磁盘引导区传染病毒主要将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磁盘的其他地方。引导区型病毒会改写(即一般所说的“感染”)磁盘上的引导扇区(Boot Sector)的内容，软盘或硬盘都有可能感染病毒，再不然就是改写硬盘上的分区表(FAT)。如果用已感染病毒的软盘来启动，则会感染硬盘。引导区型病毒是一种在ROM BIOS之后，系统引导时出现的病毒，它先于操作系统的运行，依托的环境是BIOS中断服务程序。引导区型病毒利用操作系统的引导模块被放在某个固定的位置，并且其控制权的转交方式以物理地址为依据，而不是以操作系统引导区的内容为依据，因而病毒占据该物理位置即可获得控制权，而将真正的引导区内容转移或替换，待病毒程序被执行后，将控制权交给真正的引导区内容，使得这个带病毒的系统看似正常运转，而实际上病毒已隐藏在系统中伺机传染和发作。

当计算机启动完成POST上电自检后，就将主引导记录装入内存，并且系统程序开始执行，因此引导区代码的完整性和正确性是系统能够正常运行的先决条件。引导区型病毒隐藏在磁盘的第一扇区，使它可以在系统文件装入内存之前先进入内存，在运行的一开始(如系统启动)就能获得控制权，从而使它获得对操作系统的完全控制。并且由于在磁盘的引导区内存储着许多重要信息，如果对磁盘上被移走的正常引导记录不进行保护，则在运行过程中就会导致引导记录遭到破坏，因而引导区型病毒的传染性和危害性相对较大。通过引导区传染的计算机病毒较多，例如，“大麻”和“小球”病毒就是这类病毒。

引导区型病毒按其寄生对象的不同又可分为两类，即MBR(主引导区)病毒和BR(引导区)病毒。MBR病毒也称为分区病毒，将病毒寄生在硬盘分区主引导程序所占据的硬盘0头0柱面第1个扇区中。典型的病毒有“大麻”(Stoned)、2708等。BR病毒是将病毒寄生在硬盘逻辑0扇区或软盘逻辑0扇区(即0柱面0磁道第1个扇区)。典型的病毒有Brain、“小球”病毒等。

2. 文件型病毒

文件型病毒是文件的感染者，它运行在计算机存储器里，通常会感染扩展名为.com、.exe、.drv、.dll、.bin、.ovl、.sys、.doc、.dot、.exl的文件。每一次激活时，感染文件会把自身复制到其他文件中，能在存储器里保存很长时间，并在特定条件下进行表现或破坏。

与引导区型病毒不同的是，文件型病毒不但可以感染DOS系统文件，还可以感染Windows系统、IBM OS/2系统和Macintosh系统的文件。

随着计算机操作系统的不断更新换代和Internet在社会生活中的不断普及，文件型病