全国高等职业教育规划教材 信息安全系列

计算机病毒防治实用教程

李治国 主编

电子课件下载
www.cmpedu.com

机械工业出版社
CHINA MACHINE PRESS

本课程是高职高专信息安全专业的必修课程。本书从计算机病毒的概念及其发展趋势开始，分类介绍了网页脚本病毒、宏病毒、蠕虫病毒及木马病毒等典型病毒，每类病毒都结合实例，从病毒防治的技术原理、病毒行为分析及防治措施等方面讲解了几个具有代表性的防治技术，最后还介绍了防病毒软件技术的发展方向和有代表性厂家产品的发展情况。

本书可作为高职高专院校信息安全专业、网络技术专业等的教学用书，也可作为防病毒软件设计者的参考书。

本书配套授课电子课件，需要的教师可登录 www. cmpedu. com 免费注册、审核通过后下载，或联系编辑索取（QQ：81922385，电话：010 - 88379739）。

图书在版编目(CIP)数据

计算机病毒防治实用教程/李治国主编. —北京：机械工业出版社，2010. 7
（全国高等职业教育规划教材·信息安全系列）
ISBN 978 - 7 - 111 - 31201 -7

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

中国版本图书馆 CIP 数据核字(2010)第 128261 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)
责任编辑：鹿 征
责任印制：杨 曦
北京蓝海印刷有限公司印刷

2010 年 9 月第 1 版·第 1 次印刷
184mm×260mm · 14 印张 · 343 千字
0001 - 3000 册
标准书号：ISBN 978 - 7 - 111 - 31201 - 7
定价：24. 00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
社服务中心：(010)88361066
销 售 一 部：(010)68326294
销 售 二 部：(010)88379649
读者服务部：(010)68993821

网络服务
门户网：http://www. cmpbook. com
教材网：http://www. cmpedu. com

全国高等职业教育规划教材计算机专业
编委会成员名单

出 版 说 明

根据《教育部关于以就业为导向深化高等职业教育改革的若干意见》中提出的高等职业院校必须把培养学生动手能力、实践能力和可持续发展能力放在突出的地位，促进学生技能的培养，以及教材内容要紧密结合生产实际，并注意及时跟踪先进技术的发展等指导精神，机械工业出版社组织全国近60所高等职业院校的骨干教师对在2001年出版的“面向21世纪高职高专系列教材”进行了全面的修订和增补，并更名为“全国高等职业教育规划教材”。

本系列教材是由高职高专计算机专业、电子技术专业和机电专业教材编委会分别会同各高职高专院校的一线骨干教师，针对相关专业的课程设置，融合教学中的实践经验，同时吸收高等职业教育改革的成果而编写完成的，具有“定位准确、注重能力、内容创新、结构合理和叙述通俗”的编写特色。在几年的教学实践中，本系列教材获得了较高的评价，并有多个品种被评为普通高等教育“十一五”国家级规划教材。在修订和增补过程中，除了保持原有特色外，针对课程的不同性质采取了不同的优化措施。其中，核心基础课的教材在保持扎实的理论基础的同时，增加实训和习题；实践性较强的课程强调理论与实训紧密结合；涉及实用技术的课程则在教材中引入了最新的知识、技术、工艺和方法。同时，根据实际教学的需要对部分课程进行了整合。

归纳起来，本系列教材具有以下特点：

1）围绕培养学生的职业技能这条主线来设计教材的结构、内容和形式。

2）合理安排基础知识和实践知识的比例。基础知识以“必需、够用”为度，强调专业技术应用能力的训练，适当增加实训环节。

3）符合高职学生的学习特点和认知规律。对基本理论和方法的论述要容易理解、清晰简洁，多用图表来表达信息；增加相关技术在生产中的应用实例，引导学生主动学习。

4）教材内容紧随技术和经济的发展而更新，及时将新知识、新技术、新工艺和新案例等引入教材。同时注重吸收最新的教学理念，并积极支持新专业的教材建设。

5）注重立体化教材建设。通过主教材、电子教案、配套素材光盘、实训指导和习题及解答等教学资源的有机结合，提高教学服务水平，为高素质技能型人才的培养创造良好的条件。

由于我国高等职业教育改革和发展的速度很快，加之我们的水平和经验有限，因此在教材的编写和出版过程中难免出现问题和错误。我们恳请使用这套教材的师生及时向我们反馈质量信息，以利于我们今后不断提高教材的出版质量，为广大师生提供更多、更适用的教材。

机械工业出版社

前　言

计算机病毒在今天已经成为影响信息系统安全最严重的因素之一。因此，社会对计算机病毒防治方面专业人才的需求也在快速增长。全国各大本科高校和高职院校相继开设了计算机病毒防治的相关课程以满足社会对这方面人才的需求。

在全国高职院校中重庆电子工程职业学院较早开设了信息安全专业，并在信息安全行业专家和知名信息安全企业的协助下，编写了信息安全专业的系列教材，本书即为该系列教材中的核心教材之一。

本书首先全面介绍了计算机病毒的基础知识；再以病毒行为分析、病毒源码分析、病毒清除和病毒防治为主线，对多种类型的典型病毒进行了深入剖析；最后系统地阐述了反病毒程序设计和病毒防治策略。

本书共6章，每章的主要内容如下所述：

第1章阐述了计算机病毒的基本原理和基本概念。内容涉及计算机病毒的定义、特点、分类、技术特征和计算机病毒的命名方法等，同时还介绍了计算机病毒的发展过程，并列举了病毒史上公认的十大病毒产生的危害。

第2章介绍了如何搭建计算机病毒分析平台，这是进行病毒行为分析的基础。

第3章对大量典型病毒案例进行了深入剖析。主要内容包括注册表的原理和作用，网页脚本病毒、宏病毒、蠕虫病毒和木马病毒的行为分析、源码分析和清除原理。

第4章介绍了计算机病毒的主要防范措施、计算机病毒的免疫技术和查毒技术，并对多种病毒的查毒方法进行了详细对比，分析了不同查毒方法的自身特点。

第5章介绍了反病毒软件的编制技术。主要内容包括杀毒技术的发展情况、最新的杀毒技术、反病毒软件的体系结构和杀毒软件案例剖析。最后列举了简单杀毒程序实例，指导读者进行反病毒程序的编写训练。

第6章介绍了计算机病毒防治的总体策略和目前市场上的主流病毒防治产品的情况。

作者在编写过程中，得到了龚小勇教授和武春岭老师的帮助和指导，以及趋势科技公司的鼎力支持，在此一并表示衷心的感谢！

笔者分析病毒已有多年，从事这方面的教学工作也已多年，但受水平所限，书中内容难免有不足之处，恳请读者和专家赐教。

编　者

目　录

第1章　计算机病毒概论

学习任务

- 了解计算机病毒的定义
- 了解计算机病毒的特点
- 了解计算机病毒的危害
- 了解计算机病毒的技术特征
- 了解计算机病毒代码的命名方法

当你在计算机里存储的重要数据突然丢失时；当你的计算机突然不能正常使用时；当你的银行账号或游戏账号被盗，造成经济损失时；当你的隐私被暴露在公众面前时，你是否曾想过，这些或许都是由于同一个原因——计算机病毒造成的。

1.1　计算机病毒的定义

通常用户了解最多的病毒可能是生物学上的“病毒”，像 SARS 病毒、H1N1 流感病毒和 HIV 病毒等。如图 1-1 所示是在电子显微镜下看到的 HIV 病毒体。生物病毒通常不能独立生存，必须寄生在其他生物的细胞里才能存活。由于病毒的这种特性，所以给动物和人类造成了极大危害。

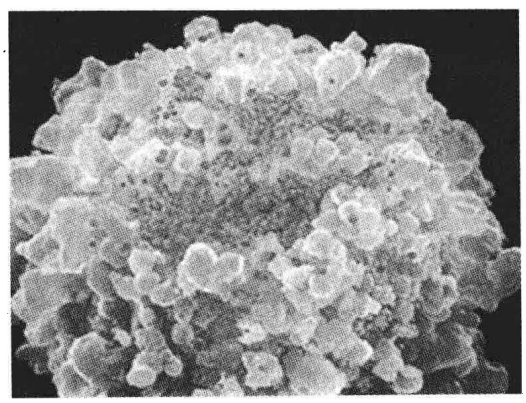

图 1-1　显微镜下的 HIV 病毒体

计算机病毒之所以被称为“病毒”，是因为它们同生物病毒有一些相似之处。计算机病毒从一台计算机传播到另一台计算机，就像生物病毒从一个人身上传播到另一个人身上一样。计算机病毒必须寄生到其他一些程序或文档中才能被执行，就像生物病毒必须寄生到其他生物细胞中一样，而一旦它处于运行状态，就会感染其他程序或文档。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、硬件所固有的安全缺陷有目的地编制而成的。

在1994年2月18日由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 计算机病毒的发展状况

1.2.1 计算机病毒的起源

1949年，计算机之父冯·诺伊曼在《复杂自动机组织论》中便定义了病毒的基本概念。他提出了"一部事实上足够复杂的机器能够复制自身"的前沿理念。这在当时，没有人相信，因为在那个年代，一般的人还认为计算机程序系统的概念根本不靠谱。直到10年之后，在美国电话电报公司（AT&T）的贝尔实验室中，三个年轻程序员在闲暇之余，想出一种电子游戏叫作"磁芯大战"。游戏中通过复制自身来摆脱对方的控制，据说这可能是所谓计算机病毒的第一个雏形。在1977年的夏天，托马斯·捷·瑞安的科幻小说《P-1的青春》成为美国的畅销书，轰动了科普界。作者幻想了世界上第一个计算机病毒，可以从一台计算机传染到另一台计算机，最终控制了7000台计算机，酿成了一场灾难，这实际上是计算机病毒的思想基础。事实上，计算机病毒的起源，确实是源自一些计算机爱好者的恶作剧。

1982年7月13日，世界上第一个计算机病毒诞生了。它就是Elk Cloner，仅仅是美国匹兹堡一位高中生的恶作剧，但它并不会对计算机产生任何危害，只是对不知情的Apple II的使用者进行骚扰。当时的病毒还没有针对个人计算机（PC），最早攻击PC的病毒是Brain，诞生于1986年，攻击的目标是微软当时最受欢迎的操作系统——DOS，由两个巴基斯坦兄弟（Basit Farooq Alvi和Amjad Farooq Alvi）编写，这个计算机病毒可以显示他们的计算机维修商店的电话号码。Brain病毒是一个引导区病毒，可以感染360KB软盘（早期的5.25英寸的软盘，容量只有360KB），这个病毒会填满软盘上未用的空间，而导致它不能再被使用。这个病毒的其他名字还有Lahore、Pakistani和Pakistani Brain。Alvi兄弟俩曾经公开对媒体表示，他们编写这个程序是为了保护自己出售的软件免于被盗版，它的目的仅仅是针对版权侵犯。

经过20多年地发展，计算机病毒数量相当惊人，其技术也越来越先进，大致可分为以下几个阶段。

1. 第一代病毒

通常认为第一代病毒产生的年代在1986～1989年，是计算机病毒的萌芽和滋生时期。这一期间出现的病毒称为传统病毒。此时计算机的应用软件少，且大多是单机运行，因此病毒没有大量流行，种类也很有限，其清除工作相对来说比较容易。这一阶段的计算机病毒具有如下一些特点：

1）病毒攻击的目标比较单一，有些感染磁盘引导扇区，有些感染可执行文件。

2）病毒程序主要采取截获系统中断向量的方式监视系统的运行状态，并在一定条件下对目标进行感染。

3）病毒感染目标以后的特征比较明显，如磁盘上出现坏扇区，可执行文件的长度增加，文件建立的日期和时间发生变化等。这些特征容易被人们发现。

4）因病毒程序不具有自我保护的措施，容易被人们分析和解剖，从而使得人们容易编制相应的杀毒软件。

然而随着计算机反病毒技术的提高和反病毒产品的不断涌现，病毒编制者也在不断地总结自己的编程技巧和经验，千方百计地逃避反病毒产品的分析、检测和查毒，从而出现了第二代计算机病毒。

2. 第二代病毒

第二代病毒又称为混合型病毒，其产生的年代在 1989 ~ 1991 年，它是计算机病毒由简单发展到复杂，由单纯走向成熟的阶段。

1）病毒攻击的目标趋于混合型，即一种病毒既可感染磁盘引导扇区，又可感染可执行文件。

2）病毒程序不采用明显地截获中断向量的方法监视系统的运行，而是采取更为隐蔽的方法驻留内存和感染目标。

3）病毒感染目标后没有明显的特征，如磁盘上不出现坏扇区，可执行文件的长度增加不明显，不改变被感染文件原来的建立日期和时间等。

4）病毒程序往往采取了自我保护措施，如加密技术和反跟踪技术，制造各种障碍，增加了人们发现、剖析及杀除病毒的难度。

5）出现许多病毒的变种，这些变种病毒较原病毒的感染方式更隐蔽，破坏性更大。

总之，这一时期出现的病毒不仅在数量上急剧地增加，更重要的是从编制的方式、方法到驻留内存以及对宿主程序的感染方式与方法等方面都有了较大的变化。

3. 第三代病毒

自 1992 年开始至 1995 年，产生了第三代病毒。此类病毒被人们称为“多态性”病毒或“自我变形”病毒。所谓“多态性”或“自我变形”的含义是指此类病毒在每次感染目标时，侵入宿主程序中的病毒程序大部分都是可变的，即在人们收集到的同一种病毒的多个样本中，病毒程序的代码绝大多数是不同的，这是此类病毒的重要特点。正是由于这一特点，传统的利用特征码法检测病毒的产品很难检测出此类病毒。

4. 第四代病毒

20 世纪 90 年代中后期，随着互联网及远程访问服务的开通，病毒流行面更加广泛，病毒流行迅速突破地域的限制，首先通过广域网传播至局域网内，再在局域网内传播扩散。随着互联网的普及、电子邮件的使用以及微软公司 Office 系列办公软件的广泛应用，夹杂于电子邮件内的 Office 宏病毒成为当时病毒的主流。由于宏病毒编写简单、破坏性强和清除时程序繁杂，加上微软公司对文档结构没有公开，因此给直接基于文档结构的宏病毒的清除带来了诸多不便。

这一时期病毒的最大特点，是利用互联网作为其主要传播途径，传播对象从传统的引导型和依附于可执行程序文件型转向流通性更强的文档文件中，因而病毒传播速度快，隐蔽性强，破坏性大。这些都给病毒防治带来新的挑战。

5. 新一代病毒

人类历史进入 21 世纪以来，互联网渗入每家每户，网络成为人们日常生活和工作中不可缺少的一部分。一个曾经未被人们重视的病毒种类遇到了适合的滋生环境而迅速蔓延，这

就是蠕虫病毒。蠕虫病毒是一种利用网络服务漏洞而主动攻击网络用户的计算机病毒类型。与传统病毒不同，蠕虫病毒不依附在其他文件或媒介上，而是独立存在的病毒程序，利用系统的漏洞通过网络主动传播，可在瞬间传遍全世界。蠕虫病毒已成为目前病毒的主流。

下面是IT史上公认的十大病毒。

（1）CIH（1998年）

该计算机病毒属于Windows 32家族，感染Windows 95/98中以exe为后缀的可执行性文件。它具有极大的破坏性，可以重写BIOS使之无法使用，其后果是使用户的计算机无法启动，唯一的解决方法是替换系统原有的芯片（Chip），该计算机病毒于每年4月26日发作，它还会破坏计算机硬盘中的所有信息。该计算机病毒不会影响MS/DOS、Windows 3.x和Windows NT操作系统。

CIH可利用所有可能的途径进行传播，如软盘、光盘只读储器（CD-ROM）、互联网、文件传输协议（FTP）下载、电子邮件等。它被公认为是有史以来最危险、破坏力最强的计算机病毒之一。1998年6月，它爆发于中国台湾，在全球范围内造成了2000万~8000万美元的损失。

（2）梅丽莎（Melissa，1999年）

这个病毒专门针对微软的电子邮件服务器和电子邮件收发软件，它隐藏在一个Word 97格式的文件里，以附件的方式通过电子邮件传播，善于侵袭装有Word 97或Word 2000的计算机。它可以攻击Word 97的注册器并修改其预防宏病毒的安全设置，使它感染的文件所具有的宏病毒预警功能丧失作用。

在发现Melissa病毒后短短的数小时内，该病毒即通过互联网在全球传染数百万台计算机和数万台服务器，互联网在许多地方瘫痪。它于1999年3月26日爆发，感染了15%~20%的商业PC，给全球带来了3亿~6亿美元的损失。

（3）I love you（2000年）

2000年5月3日，该病毒爆发于中国香港，这是一个用VBScript编写，可通过E-Mail散布的病毒，受感染的计算机平台以Windows 95/98/2000为主。它给全球带来了100亿~150亿美元的损失。

（4）红色代码（Code Red，2001年）

该病毒能够迅速传播，并造成大范围的访问速度下降甚至访问被阻断。这种病毒一般首先攻击计算机网络的服务器，遭到攻击的服务器会按照病毒的指令向政府网站发送大量数据，最终导致网站瘫痪，其造成的破坏主要是涂改网页。有迹象表明，这种蠕虫病毒有修改文件的能力。它于2001年7月13日爆发，给全球带来了26亿美元的损失。

（5）SQL Slammer（2003年）

该病毒利用SQL Server 2000的解析端口1434的缓冲区溢出漏洞，对其服务进行攻击。它于2003年1月25日爆发，全球共有50万台服务器被攻击，但经济损失较小。

（6）冲击波（Blaster，2003年）

该病毒运行时会不停地利用互联网协议（IP）扫描技术寻找网络上系统为Windows 2000和Windows XP的计算机，找到后就利用DCOM RPC缓冲区漏洞攻击该系统，一旦攻击成功，病毒体将会被传送到对方计算机中感染目标，使系统操作异常、不停重启甚至导致系统崩溃。另外，该病毒还会对微软的一个升级网站进行拒绝服务攻击，导致该网站堵塞，使

用户无法通过该网站升级系统。它于2003年夏爆发，数十万台计算机被感染，给全球造成了20亿~100亿美元的损失。

（7）大无极.F（Sobig.F，2003年）

Sobig.F是一个利用互联网进行传播的病毒，当其程序被执行时，它会将自己以电子邮件的形式发给被它感染计算机中找到的所有邮件地址。它使用自身的SMTP引擎来设置所发出的信息。此蠕虫病毒在被感染系统中的目录为C:\WINNT\Winppr 32.exe。它于2003年8月19日爆发，为此前Sobig的变种，给全球带来了50亿~100亿美元的损失。

（8）贝革热（Bagle，2004年）

该病毒通过电子邮件进行传播，运行后，在系统目录下生成自身的拷贝，修改注册表关键值。病毒同时具有后门能力。它于2004年1月18日爆发，给全球带来了数千万美元的损失。

（9）MyDoom（2004年）

MyDoom是一种通过电子邮件附件和P2P网络Kazaa传播的病毒，当用户打开并运行附件内的病毒程序后，病毒就会以用户信箱内的电子邮件地址为目标，伪造邮件的源地址，向外发送大量带有病毒附件的电子邮件，同时在用户主机上留下可以上传并执行任意代码的后门（TCP 3127~3198范围内）。它于2004年1月26日爆发，在高峰时期，导致网络加载时间慢50%以上。

（10）Sasser（2004年）

该病毒是一个利用微软操作系统的Lsass缓冲区溢出漏洞（MS04-011漏洞信息）进行传播的蠕虫病毒。由于该蠕虫病毒在传播过程中会发起大量的扫描，因此对个人用户使用和网络运行都会造成很大的冲击。它于2004年4月30日爆发，给全球带来了数千万美元损失。

1.2.2 国内计算机病毒的发展状况

大约在1988年，随着软件交流，“石头”和“小球”病毒跟随软盘悄悄地通过中国香港和美国进入了中国内地，并在大型企业和研究所间广为传播。由于当时普遍使用软盘启动系统，因此这两个系统病毒成了国内最流行的计算机系统病毒。跟随系统病毒之后，各种文件病毒也迅速登陆，如“巴基斯坦”、“维也纳”和“雨点”等病毒。

那时由于家庭计算机尚未普及，因此各家研究所和高等院校等计算机应用密集的部门成了计算机病毒的重灾区。

与此同时，国内的计算机高手，通过剖析病毒体，迅速掌握了病毒的编写技术，“广州一号”、“中国炸弹”和“毛毛虫”等各种国产病毒也纷纷登场亮相。不过，随着软件技术的发展，人们逐渐了解和掌握了计算机病毒的防治方法，SCAN和TBAV等反病毒软件纷纷从国外引入，并且国人也开始尝试自己编写一些国产反病毒软件。华星等硬件防病毒卡更是风行一时，其硬件防病毒技术当时在全世界范围内处于领先地位。

到了1992年，旧的计算机病毒技术已经完全被掌握，一些防病毒卡甚至宣称可以防范所有的已知和未知的病毒，人们似乎已经看到了计算机病毒的末日了。此时，一个叫做DIR II的病毒横空出世。这个病毒编写得非常巧妙，短短512个字节的程序代码，就“钻”入了DOS操作系统的核心，实现了加密、解密和传染的功能，而且巧妙地躲过了各种防病毒软件和防毒卡的查杀。其高超的编程技术令人叹为观止，至今仍为计算机病毒的典范之作。DIR II病毒迅速摧毁了各种防病毒卡，为防病毒软件的开发开辟了一条新的道路。人们开始

认识到，计算机反病毒技术的发展是一个漫长而曲折的过程，而防病毒软件因为其良好的兼容性、低廉的价格和方便的升级能力，也逐渐得到了广大用户的认可。

1996 年，计算机病毒的破坏能力又有了进一步提高，为了躲避反病毒软件的监视，新的变形病毒应运而生。以前那种采用特征代码串来标识计算机病毒的技术又开始失效。最先传入中国的是“幽灵”，随后是“猴子”等两栖（同时感染系统和文件）变形病毒，这些病毒先后在一定范围内流行，不过由于反病毒软件的及时跟进，以及国人已经习惯于综合使用各种反病毒软件，因此这些病毒都没有能掀起太大的风浪。令人担忧的是，随着国际互连网络的普及，计算机病毒编写者开始通过互联网络来交流编程技术和心得体会。网上也出现了专门的变形病毒引擎，利用这些引擎，任何人都可以编写出带无穷变形功能的计算机病毒。

1997 年，在沉寂了一小段时间以后，病毒又找到了新的突破点，部分计算机用户利用了功能强大的宏语言，编制了各色各样的宏病毒。随后是各种各样的好奇者，简单地利用宏编辑器改造了自己的产品。据一些反病毒软件站点报告，全世界一个星期就有近千只新病毒出现，而其中绝大部分是宏病毒。

1997 年下半年，一个叫做 SPY 的可以攻击 NE（16 位 Windows 格式可执行文件）格式程序的病毒，曾经在南方流行一时，敲响了向 Windows 进攻的警钟。到了 1998 年的年中，CIH 病毒终于攻破了 Windows 95 平台。这个病毒创造了几个第一，即第一个流行的攻击 PE 格式 32 位保护模式程序的病毒；第一个可以破坏计算机硬件的病毒。以前的病毒最多只能破坏软件系统，而 CIH 病毒不但直接利用 IOS 指令摧毁硬盘数据（即使主板具有防病毒功能，也无能为力），而且通过清洗存储在 Flash EPROM 中的 BIOS 指令，导致系统主板无法工作，彻底破坏机器。CIH 病毒利用虚拟设备驱动程序（VXD）技术逃过了当时所有反病毒软件的监测，并且令目前所有宣称可以防病毒的主板大失颜面。

据网上的一封道歉信报道，CIH 病毒是中国台湾的一名学生编写的。通过反编译发现，这个病毒系利用 SIDT 指令来获取系统的核心级执行权限，进而截获系统核心功能的调用。这实际上可以说是 Windows 95 系统（Windows 98 同样有这个问题）的一个漏洞。所幸的是，Windows NT 已经封锁了这一条指令，因此 CIH 病毒无法在 Windows NT 下兴风作浪。

1.3 计算机病毒的传播途径

随着网络技术的快速发展和计算机的广泛普及，计算机病毒的传播途径也越来越多。大致可分为如下几类。

1. 通过软盘、光盘传播

软盘作为最常用的交换媒介，是早期计算机病毒传播的主要手段。因为那时计算机应用比较简单，可执行文件和数据文件都较小，许多都需要通过软盘相互复制、安装，这样就能通过软盘传播病毒文件。

光盘的容量大，可以存储大量的可执行文件，已成为目前软件和数据传输的主要方式之一，而大量的病毒就有可能藏身于光盘之中。对于只读式光盘，由于不能进行写操作，因此光盘上的病毒无法被清除。

2. 通过移动存储设备传播

通过移动存储设备（如 U 盘）传播病毒是目前计算机病毒最流行的传播方式之一。该

类型病毒的形式主要有以下几种：

1）通过 autorun. inf 文件进行传播（U 盘病毒最普遍的传播方式）。

2）伪装成其他文件。病毒把 U 盘下所有文件夹隐藏，并把自己复制成与原文件夹名相同的具有文件夹图标的文件，当点击时病毒会执行自身并且打开隐藏的该名称的文件夹。

3）通过可执行文件感染病毒，虽然是很古老的一种传播手段，但是依然有效。

3. 通过网络传播

计算机网络是目前计算机病毒数量急速增长、种类快速增加的直接动力，几乎任何一种网络应用都可能成为计算机病毒传播的有效渠道，计算机病毒常见网络传播方式如下：

1）通过局域网传播。局域网是由相互连接的一组计算机组成的，这是数据共享和相互协作的需要，组成网络的每一台计算机都能连接到其他计算机，数据也能从一台计算机发送到其他计算机上，如果发送数据方感染了计算机病毒，那么接收方的计算机将自动被感染。

2）通过电子邮件（如邮件附件、带恶意程序的邮件正文等）传播。Outlook 以及 Outlook Express 是最常见的邮件客户端软件，也是非常容易受到邮件病毒攻击的软件。由于这类软件有两个重要漏洞，即预览漏洞和执行漏洞，因此产生了大量利用这两个漏洞的病毒。

3）各类即时通信软件（如 QQ、MSN 和 Skype 等）。即时通信（Instant Massager）软件可以说是目前上网用户使用率最高的软件，由于用户数量众多，再加上即时通信软件本身的安全缺陷，使得病毒可以方便地获取传播目标。

利用发送窗口中的超链接功能进行病毒传播是即时通信软件传播病毒最常使用的方式之一。当用户收到好友发来的一个网址时，只要单击该网址就能直接进入该网页，如图 1-2 所示。由于该功能的方便性，被很多病毒利用，病毒运行时会利用聊天窗口向所有在线好友发送一个病毒网址的活链接，当好友误以为是有用的网址并单击时就会中毒。

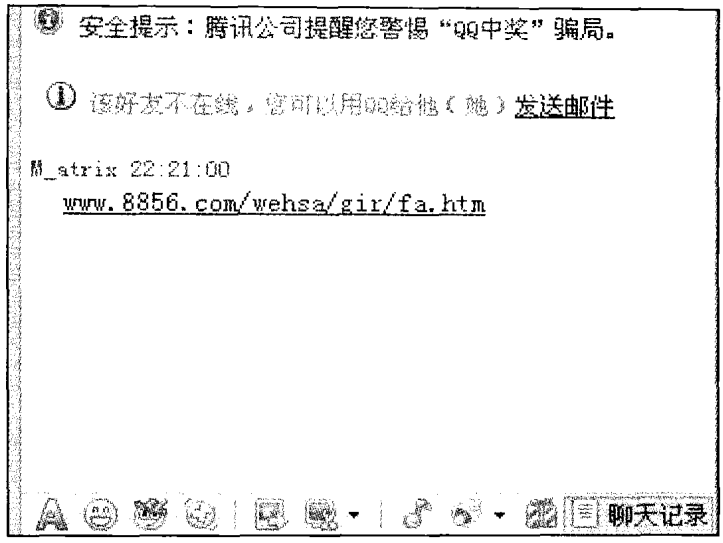

图 1-2　QQ 病毒的传播

4）利用各类浏览器的漏洞（如 IE、Firefox 和 Opera 等）在网页中嵌入木马程序。IE 浏

览器是使用最多的浏览器，它也存在很多安全漏洞并成为病毒攻击的对象。最常见的病毒攻击方式是利用脚本执行漏洞，该漏洞会在用户浏览网页时自动执行网页中的有害脚本程序，或者自动下载一些有害的病毒，从而对用户的计算机造成破坏。由于通过“网页挂马”可以快速地批量入侵大量计算机，获取经济利益，因此“网页挂马”成为黑客常用的攻击手段。

5）点对点传输（P2P）下载渠道（如 BT、电驴等）。P2P 软件是点对点的通信传输工具，只要使用同一个 P2P 软件，用户之间就可以直接进行交流、聊天和交换文件等。随着 P2P 软件使用范围的普及，有越来越多的病毒开始盯着这类软件实现病毒传播。

6）各类应用软件漏洞。很多流行的应用软件都曾出现过安全漏洞。很多用户认为只要这些软件能够正常使用，就不必去升级新版本，这使这些用户的计算机都存在漏洞。

7）各类系统漏洞。漏洞是指操作系统中的某些程序中存在一些人为的逻辑错误。目前，各类操作系统都不可避免地存在安全问题和缺陷。

8）地址解析协议（ARP）欺骗。ARP 是一种常用的网络协议，每台安装有传输控制协议/互联网协议（TCP/IP）的计算机里都有一个 ARP 缓存表，表里的 IP 地址与媒体存取控制（MAC）地址一一对应，如果这个表被修改，则会出现网络无法连通，或者访问的网页被劫持等问题。

9）无线设备传播。目前，这种传播途径随着手机功能的开放和增值服务的拓展，已经成为人们需重点防范的一种病毒传播途径。

1.4 计算机病毒的特点

1. 非法性

在正常情况下，当计算机用户调用执行了某个合法程序时，操作系统就把系统控制权交给这个程序，并给其分配相应的系统资源，如内存等，从而使之能够运行以达到破坏用户系统的目的。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。但当某个程序非正当的获得系统资源而产生破坏性后果时，这种程序就是“非法”的。

2. 隐藏性

隐藏性是计算机病毒最基本的特征之一，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。

如果不经过代码分析，病毒程序与正常程序是不容易区分开来的。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，可以在很短的时间内感染大量程序。而受到感染后，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，病毒会使用很多巧妙的方法隐藏自己，使之不容易被发现。正是由于具有隐藏性，因此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。

3. 潜伏性

计算机病毒具有依附于其他媒体而寄生的能力，一般把这种媒体称为计算机病毒的宿主。依靠病毒的这种寄生能力，病毒在感染程序和系统后，不会立即发作，而是长期隐藏在系统中，只有在满足其特定条件时才启动其破坏模块。如“PETER-2”病毒会在每年的 2

月 27 日提三个问题，答错后会将硬盘加密；著名的“黑色星期五”在每月逢 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，最令人难忘的便是每年 4 月 26 日发作的“CIH”。

4. 可触发性

计算机病毒一般都有一个或者几个触发条件。若满足其触发条件或者激活病毒的传染机制，就会使之进行传染或者激活病毒的表现部分或破坏部分。

在一定的条件之下，通过外界刺激可以使计算机病毒程序活跃起来，激发的本质是一种条件控制。

5. 破坏性

计算机病毒造成的最恶劣的后果便是破坏计算机系统，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。

6. 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。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像互联网这样的网络传遍全世界。

近年来，随着互联网的迅速发展，人们在工作和生活中也越来越依赖网络，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。不仅是个人用户使用，很多正式的商业联系和各类组织、政府机构的信息传递也是通过 E-mail 完成的。因此，病毒的编制者就利用了电子邮件的这个特点，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。

7. 针对性

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，一般都有针对性地感染目标。有的病毒感染 Apple 公司的 MAC 系统，有的病毒感染磁盘引导区，有的病毒感染可执行文件等。

1.5 计算机病毒的分类

1. 根据病毒攻击的系统分类

按照计算机病毒攻击的目标系统分类，可以分为 DOS 病毒、Windows 病毒、UNIX 病毒和 OS/2 病毒。

DOS 病毒：这类病毒出现最早，变种也最多。

Windows 病毒：由于此类操作系统采用图形界面，操作简单，用户数量大，因此此类操作系统逐步成为病毒攻击的主要目标。

UNIX 病毒：由于 UNIX 操作系统的应用范围越来越广泛，并且大多数服务器均采用此操作系统，所以，UNIX 病毒的出现，对信息系统将是一个严重的威胁。

OS/2 病毒：OS/2 操作系统由于用户数量少，相对来说，此类病毒数量较少。

2. 根据计算机病毒的寄生部位或感染对象分类

传染性是计算机病毒的本质属性。根据寄生部位或感染对象（即根据计算机病毒的传