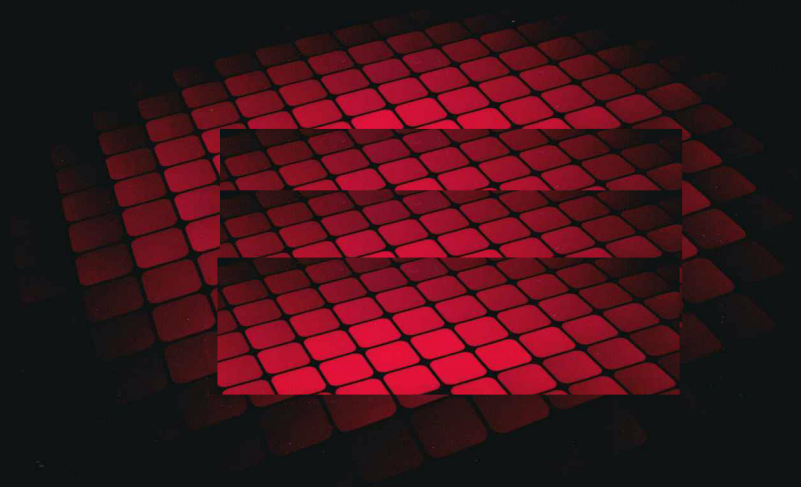
Jisuanji Bingdu Yuanli Yu Fangzhijishu

计算机病毒原理与防治技术

主编 韩兰胜 副主编 刘铭 彭冰 付才



華中科技大學出版社
http://www.hustp.com

计算机病毒原理与防治技术

主　编　韩兰胜
副主编　刘　铭　彭　冰　付

华中科技大学出版社
中国·武汉

内容简介

本书分为基础篇、防治篇、提高篇和实验篇。基础篇介绍了计算机病毒的概念、基本原理，详细阐述了病毒的自我复制、感染和传播机制，其中还包括蠕虫、木马和移动设备病毒的基本原理。防治篇讲述了计算机病毒的检测、清除技术及当前处于发展中的一些检测和防治办法。提高篇从机器、整体网络宏观的角度，讲述了计算机病毒的计算特性、传播模型和病毒的危害性测量。本书对病毒原理的讲解细致而具体，对防治技术的讲解具体而又可操作，实验部分侧重具体技术的实现。本书既注重基本原理的细致讲解，又能从宏观角度来把握病毒的规律，从发展的观点看待病毒新变化，对读者有一定的启示。

本书适合信息安全专业的本科生、研究生的教学，也可作为广大的计算机专业人士深入了解计算机病毒的参考用书。

图书在版编目(CIP)数据

计算机病毒原理与防治技术/韩兰胜　主编. —武汉：华中科技大学出版社，2010.11
ISBN 978-7-5609-6636-6

Ⅰ.计…　Ⅱ.韩…　Ⅲ.计算机病毒-防治

中国版本图书馆 CIP 数据核字(2010)第 193431 号

计算机病毒原理与防治技术　　韩兰胜　主编

策划编辑：万亚军
责任编辑：姚　幸
封面设计：范翠璇
责任校对：朱　霞
责任监印：熊庆玉
出版发行：华中科技大学出版社(中国·武汉)
　　武昌喻家山　　邮编：430074　　电话：(027)87557437
录　　排：华中科技大学惠友文印中心
印　　刷：湖北恒泰印务有限公司
开　　本：787mm×1092mm　1/16
印　　张：15.5
字　　数：415 千字
版　　次：2010 年 11 月第 1 版第 1 次印刷
定　　价：28.00 元

本书若有印装质量问题，请向出版社营销中心调换
全国免费服务热线：400-6679-118　竭诚为您服务
版权所有　侵权必究

前　言

当前，信息安全涉及社会、国家和个人的方方面面，成为社会安全的突出问题，而计算机病毒则是信息安全中最突出的问题之一，许许多多的信息安全问题都牵涉计算机病毒的技术。笔者自 2003 年起就从事计算机病毒相关的研究和教学工作，于 2006 年、2007 年分别获得省、国家自然科学基金资助，近年来又申请了本领域的软件著作权和发明专利。“计算机病毒原理及防治技术”是信息安全专业大学生的必修课程，但全面而又深入的计算机病毒类教材很少。鉴于此，特编写了本书，将对计算机病毒的专业认知整理出来，与广大读者共享。

相比于同类教材，本书具有以下突出特点。

(1) 对病毒原理的讲解细致而具体，内容安排由浅入深，列举了大量有代表性的病毒示例，循序渐进，便于读者学习。

(2) 涵盖内容广。不仅介绍了早期的单机病毒原理，还详细分析了当前的蠕虫、木马、变种病毒及未来移动设备病毒的技术原理及发展趋势。

(3) 侧重实验环节，强调具体的动手能力的培养。本书共安排四大类实验，其中包括了病毒的自我繁殖，病毒的感染，病毒的网络传播，病毒的查找和清除等主要的技术实验。

(4) 内容分类新颖，有自己的见解。这主要体现在对网络病毒的命名与分类、病毒的几个新的传播模型介绍、病毒的危害性测量等其他教材所没有涉及的内容。本书既注重基本原理的细致讲解，又能从宏观角度来把握病毒的规律，从发展的观点看待病毒新变化，对读者有一定的启示。

本书共分 11 章，第 1 章至第 4 章为基础篇，详细讲述了计算机病毒的基本原理；第 5 章至第 7 章为防治篇，主要介绍了计算机病毒的防治技术；第 8 章至第 10 章为提高篇，主要从机器角度、网络宏观角度和病毒的危害角度分别讲述了计算机病毒的计算特性、网络传播规律和危害性的度量问题；第 11 章为实验篇，介绍了四个典型的计算机病毒实验。本书第 1 章至第 10 章由韩兰胜编写，第 11 章实验部分由刘铭、付才负责编写；全书的插图、表格、参考文献等由彭冰负责。在本书的编写过程中，华中科技大学信息安全实验室的 2008、2009 级研究生刘其文、邹梦松、金雄斌、刘勇昌、李炜、吕艺、刘科等 10 多位同学做了许多内容和文献的收集、分类工作。

本书基础篇和防治篇主要讲述计算机病毒的基本原理和防治技术，并配备了具体的实验，适合信息安全专业的本科生使用；提高篇侧重对计算机病毒逻辑组成、宏观规律的刻画，适合计算机、信息安全专业的研究生使用，也可作为信息安全专业人士的研究参考用书。总之，对广大的计算机专业人士和信息安全专业人士了解、认识计算机病毒来说，阅读本书是不错的选择。

在本书的编写过程中，参考了大量文献资料，其中有不少来自网络，对此，谨向提供网络搜索服务的 Google、Baidu 等公司表示感谢，并向涉及的作者表示诚挚的谢意。在本书的出版过程中，华中科技大学教务处、华中科技大学出版社、华中科技大学计算机学院的领导及相关老师给予了关心和帮助，在此一并表示衷心的感谢。

限于编者的水平和能力，本书难免有不足之处，恳请广大读者批评指正。

韩兰胜

2010 年 5 月于武汉

目　录

基　础　篇

防　治　篇

此为试读，需要完整PDF请访问：www.ertongbook.com

提 高 篇

实 验 篇

基础篇

对计算机病毒的哲学思考刚刚起步，作为一种特殊的人工生命，它在未来的变化或进化，以及对环境（计算机网络世界）的影响和后果是不可预测的，即使只是原则上的预测可能也会不得要领。这就需要公众对它进行思考和讨论，而决不是只想着怎样对付它。就象生物病毒在现实世界中不能被彻底地消灭一样，计算机病毒也不可能被彻底地消灭。人类应该让计算主体学会如何适应病毒，就象生物通过进化而获得对生物病毒的免疫能力一样。这意味着，对待计算机病毒，人类要改变原有的一些基本观念。

第 1 章　计算机病毒的概念

1.1　计算机病毒的由来及定义

在信息时代，计算机已经渗透各行各业，在社会的各个领域和生活的方方面面都起着举足轻重的作用。Internet 改变了人们的生活方式和工作方式，改变了全球的经济结构、社会结构，Internet 逐渐成为人类社会的最重要组成部分。开放性和灵活丰富的应用是 Internet 的特色，但它们也带来了许多潜在的安全问题。随着网络的发展，计算机病毒利用网络全球互联的特点和计算机系统及网络系统安全上的漏洞，已经成为威胁计算机系统安全最主要的因素，给人们的生活和工作带来了很大的困惑与损失。现在计算机病毒在 Internet 上到处传播和蔓延，使得接入 Internet 的计算机处于随时可能被攻击的风险中。

1.1.1　计算机病毒的由来

早在 1949 年，距离第一部商用计算机的出现仍有好几年，计算机的先驱者冯·诺伊曼（Von Neumann）在他所提出的一篇论文《复杂自动装置的理论及组织的进行》中勾勒出病毒程序的蓝图。他指出，数据和程序并无本质区别，如果不运行它或不理解它，则根本无法分辨出一个数据段和一个程序段。

十年后，在美国电话电报公司（AT&T）的贝尔（Bell）实验室中，程序员道格拉斯·麦耀莱（Douglas Mcllroy）、维特·维索斯基（Victor Vysottsky）和罗伯特·莫里斯（Robert Morris）开发出一种名为“磁芯大战”（core war）的电子游戏，这是计算机病毒公认的祖先。但由于那时的计算机还没形成网络，只能在单机上运行，故并没有产生太大的影响。但即便如此，由于病毒的无穷繁殖，使得单机不堪重负而关机。因此，长久以来懂得玩“磁芯大战”的计算机工作者都严守一项不成文的规定：严禁对普通大众公开“磁芯大战”程序的内容。

1977 年，Thomas Ryan 的科学幻想小说 *The Adolescence of P - 1* 轰动了美国科普界。作者在这部书中幻想出世界上第一个计算机病毒，它可以从一台计算机传染到另一台计算机，最终控制 7 000 台计算机的操作系统，酿成一场灾难。这个幻想，有人认为它实际上是计算机病毒的思想基础。

但在 1983 年，科恩·汤普逊（Ken Thompson）在一项杰出计算机奖的颁奖典礼上不但公开证实了计算机病毒的存在，而且还告诉听众如何写自己的病毒程序。他的同行吓坏了，然而这个秘密已经流传出去了。到了 1984 年，情况更加复杂。这一年的 5 月，《科学美国人》月刊（Scientific American）的专栏作家杜特尼（Dewdney）写了一篇讨论“磁芯大战”的文章，并且只要寄上两美元，任何读者都可以收到他所写的有关写程序的纲领，然后在自己家里的计算机中开辟战场。

1983 年 11 月 3 日，弗雷德·科恩（Fred Cohen）博士研制出一种运行过程中可以复制的破坏性程序，伦·艾德勒曼（Len Adleman）将它命名为计算机病毒（computer viruses），并在每周一次的计算机安全讨论会上正式提出来。8 个小时后，计算机专家们在 VAX 11/750 计算机系统上运行了此程序，第一个计算机病毒实验成功。一周后，又获准进行了 5 个实验的演示，

从而在实验上验证了计算机病毒的存在。这是世界上第一次计算机病毒实验性发作。

在 1985 年 3 月份的《科学美国人》里，杜特尼再次讨论“磁芯大战”和病毒，在文章的开头第一次提到“病毒”这个名称。他说，意大利的 Roberto Cerruti 和 Marco Morocutti 发明了一种破坏软件的方法。他们想用病毒而不是蠕虫，感染 Apple Ⅱ计算机。Roberto Cerruti 写了一封信给杜特尼说：Marco Morocutti 想写一个像病毒一样的程序，可以从一部苹果计算机传染到另一部苹果计算机，使其受到感染，可是我们没法这样做。直到我想到：这病毒要先使磁盘受到感染，而计算机只是媒介，这样病毒就可以从一片磁盘传染到另一片磁盘了。

其实，早在 1980 年，施乐柏路阿图研究中心（Xerox PARC）的研究人员 John Shoch 和 Jon Hupp 写了一篇使用程序进行网络维护和分布式计算的论文。该程序可检测到网上其他计算机是否工作和空闲。该程序向空闲计算机提交一份自身拷贝，从而充分利用计算机的资源。利用该程序对一个问题可以分而治之求解，如加密和解密问题。但该程序后来出现了一个编程错误，此程序不断被发送到许多计算机，导致该所的计算机死机。后来，人们称之为“Xerox 蠕虫”，这也是最早的蠕虫。

1986 年，巴基斯坦的两位软件开发人员为了搞清楚自己编制的软件究竟都跑到了谁的手里，于是炮制了一个“巴基斯坦智囊（Pakistan brain）”病毒，这可能是最早广泛流行的计算机病毒。

1988 年，当年玩“磁芯大战”出了名的罗伯特·莫里斯的儿子小莫里斯受到“Xerox 蠕虫”的启发，利用当时大型机主流操作系统 Unix 的一个小漏洞编写了一个小程序，这个程序像蠕虫一样在 ARPANET（Internet 的前身）网上四处蠕动，不停地自我复制，在短短的 12 小时内就使系统内 6 200 台计算机瘫痪，造成的经济损失将近上亿美元。直到如今，“莫里斯蠕虫”仍被认定是计算机病毒发展史上最具影响力的事件。

1989 年 10 月 16 日，WANK 蠕虫表现出强烈的政治意味，它自称是抗议核武器威胁的蠕虫（worms against the nuclear killers，WANK），将被攻击的 DEC VMS 计算机的提示信息改为“表面高喊和平，背地里却准备战争”（You talk of times of peace for all，and then prepare for the war）。WANK 蠕虫是通过系统弱口令漏洞进行传播的。

1989 年 11 月 13 日，黑色星期五“Jerusalem”病毒长期潜伏后发作，祸及全世界数十万台计算机，该病毒每运行一次便删除一个文件，最终导致计算机系统被迫终止运行，许多重要的文件丢失，造成的损失难以估计。

1996 年底，我国首例宏病毒在深圳被发现。随后在 1997 年春节前后，北京某著名 ISP（互联网服务提供商）向它所有的用户发送了一份电子邮件，邮件附件中的“台湾一号”宏病毒几乎是在一天之内感染了该 ISP 全部用户。宏病毒的出现，是计算机病毒有史以来最大的技术突破，加上 Internet 此时迅速在全世界范围的普及，造成宏病毒以前所未有的速度传播。

1998 年，CIH 病毒让计算机用户再次吃尽了苦头。CIH 最早出现在中国台湾，先通过盗版光盘在美国和欧洲等地广泛流行，后通过 Internet 等在全球泛滥。最初 CIH 只在 4 月 26 日发作，但是其作者对 CIH 造成的破坏并不满意，继而将其发作日期改为每月的 26 日。时至今日，恐怕很多装有 Windows 98 的计算机用户对于 26 日仍是心有余悸。

自此以后，计算机的病毒在 Internet 上的泛滥更是一发不可收拾。比如后续的爱虫（Love Bug）、梅莉莎（Melissa）、红色代码（Red Code）、尼姆达（Nimda）、冲击波（Blaster）、震荡波（Sasser）等诸多病毒似浪潮一般，一次猛于一次，给全球计算机用户和企业带来了不可估量的损失。

1.1.2 病毒的定义

“计算机病毒”一词源于生物病毒，是指那些具有寄生性、传染性和破坏性的可执行程序代码。但随着病毒制造技术的发展，现在的病毒已经不是传统意义上的病毒，出现了许多新的病毒种类，计算机病毒的概念变得更加宽广。

计算机病毒的定义有很多，一般分为狭义定义与广义定义。狭义定义也就是计算机病毒发展的早期，一般指20世纪90年代中期以前比较流行通俗的一种定义：计算机病毒是一段附着在其他程序上的，可以自我繁殖的程序代码，复制后生成的新病毒同样具有感染其他程序的功能。

在我国，专家和研究者也对计算机病毒做过一些定义，但一直没有公认的明确定义。直至1994年2月18日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》。在该“条例”第二十八条中明确指出：“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能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、权威性。根据这个定义，计算机病毒是一种计算机程序，它不仅能破坏计算机系统，而且还能够传染到其他系统。计算机病毒通常隐藏在其他正常程序中，能生成自身的拷贝并将其插入其他的程序中，对计算机系统进行恶意的破坏。

经过近二十多年的发展，传统的计算机病毒定义已经不符合当前Internet的实际情况，因而不少学者提出了计算机病毒广义定义，泛指那些能够引起计算机故障、破坏计算机数据的恶意程序。依据此定义，诸如逻辑炸弹、蠕虫、木马等均可称为计算机病毒。很多法学领域的专家曾提出对计算机病毒的概念做一些调整，现在有些法学专家提出更广义的说法：任何方式以非法的目的入侵目标计算机，影响这台计算机的使用、窃取数据，或者没有影响使用，但是存在这种风险的，甚至存在这种可能性的程序和代码，不管它是不是能够自我进行复制，它都算作计算机病毒。这种提法把计算机病毒的概念延伸了很多，但是这一提法在理论上却没有作为法律的依据。

广义定义将特洛伊木马、宏病毒、网络蠕虫等具有一定争议的“程序/代码”均作为病毒，这与众多杀毒软件对病毒的定义是一致的。如果要严格区分，可以将这些病毒称为“后计算机病毒”。也就是说，某些广义定义下的计算机病毒，如网络蠕虫，它不具有狭义病毒的特征，并不感染其他正常程序，而是通过持续不断地反复复制自己，增加自己的拷贝数量来消耗系统资源（如内存、磁盘存储空间、网络资源等），最终导致系统崩溃。再比如一些木马类病毒，也不感染其他程序，它们可以独立存在，就像一般的应用程序一样，只不过利用了漏洞入侵，能够被远程的操纵者控制。所以这类木马也不算是狭义定义下的计算机病毒。

何鸿君、罗莉等给出的相对性病毒的定义：一个程序之所以被称为“病毒”，是因为它具有损害性。损害性是恶意程序的本质，而是否造成损害一定是对用户而言的。例如病毒V，对于作者来说，如果他是在测试V，那V对他而言是没有损害的，因为V运行的结果就是他所需要的；如果他在不知道的情况下运行了V或被V感染的程序，则V对他而言是有损害的，因为运行结果不是他希望的。再例如，用户已经知道病毒V的功能是删除当前目录下的所有文件，用户经常把它当做一个文件删除工具使用，那么对用户来说V是一个实用程序。

1.1.3 病毒的发展趋势

随着Internet的发展和计算机网络应用的日益普及，计算机病毒出现了一系列新的发展

趋势。

1. 病毒传播更加网络化

新病毒层出不穷，Internet 上的各种网络应用平台如电子邮件等已成为病毒传播的主要途径。病毒家族的种类越来越多，且传播速度大大加快，传播空间大大延伸，呈现无国界的趋势。据统计，以前通过磁盘等有形媒介传播的病毒，从国外发现到国内流行，传播周期平均需要 6 至 12 个月，而 Internet 的普及，使得病毒的传播已经没有国界。从梅莉莎、怕怕、辛迪加、欢乐 99 到美丽公园、探索蠕虫、红色代码、求职信等恶性病毒，通过 Internet 短短几天就可传遍整个世界。

2. 病毒种类更多样化

随着计算机技术的发展和软件的多样性，病毒的种类也呈多样化发展的态势，如今不仅仅有引导型病毒、普通可执行文件型病毒、宏病毒、混合型病毒，还出现专门感染特定文件的高级病毒。特别是 Java、VB 和 ActiveX 的网页技术逐渐被广泛使用后，一些人就利用这些新技术来撰写病毒。由于脚本语言的广泛使用，专用病毒生成工具的流行，计算机病毒已经变成了“小学生的游戏”。例如爱虫病毒是用 VBScript 语言编写的，只要通过 Windows 下自带的编辑软件修改病毒代码中的一部分，就能轻而易举地制造病毒变种，以躲避反病毒软件的追击。以 Java 病毒为例，虽然它并不能破坏硬盘上的资料，但如果使用浏览器来浏览含有 Java 病毒的网页，浏览器就把这些程序抓下来，然后通过使用者自己系统里的资源去执行，这样使用者就在神不知鬼不觉的状态下，就被进入自己机器里的病毒进行针对自己的相关破坏，或者通过网络窃取个人秘密信息。另外，随着 Internet 和现有的手机通信网络的连通，现在还出现了能够在无线网络上传播并破坏手机终端的手机病毒。

3. 综合利用多种新技术

从 Rootkit 技术到映像劫持技术（IFEO，image file execution options，它是位于注册表的 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options，由于这个项主要是用来调试程序用的，对一般用户意义不大。默认是只有管理员和 local system 有权读写修改），磁盘过滤驱动到还原系统 SSDT HOOK 和还原其他内核 HOOK 技术，病毒为达到目的所采取的手段已经无所不用其极。通过 Rootkit 技术和映像劫持技术隐藏自身的进程、注册表键值，通过插入进程、线程避免被杀毒软件查杀，通过实时监测对自身进程进行回写，避免被杀毒软件查杀，通过还原系统 SSDT HOOK 和还原其他内核 HOOK 技术破坏反病毒软件，其中仅映像劫持技术就包括“进程映像劫持”、“磁盘映像劫持”、“域名映像劫持”、“系统 DLL 动态连接库映像劫持”等多种方式。目前几乎所有的盗取网络游戏账号的木马病毒至少具备以上技术特征中的一种。几乎所有最新的程序应用技术都可以被病毒一一采用，计算机一旦感染病毒，普通用户根本无能力彻底清除，只能求助专业技术人员。未来的计算机病毒将综合利用以上新技术，使得杀毒软件查杀难度更大。

4. 病毒破坏性更强

新病毒的破坏力更强，手段比过去更加狠毒和阴险，它可以修改文件（包括注册表）、通信端口，修改用户密码，挤占内存，还可以利用恶意程序实现远程控制等。针对计算机硬件进行破坏的病毒从原来 DOS 下的格式化硬盘数据发展到利用 Windows 的 VXD 技术破坏主板 BIOS 和硬盘数据的 CIH 病毒。CIH 病毒破坏主板上的 BIOS 和硬盘数据，使得用户需要更换主板，由于硬盘数据的不可恢复性丢失，给用户带来巨大损失。例如，白雪公主病毒修改 Wsock32.dll，截取外发的信息，自动附加在受感染的邮件上，一旦收信人执行附件程序，该

此为试读，需要完整PDF请访问：www.ertongbook.com

病毒就会感染个人主机。一旦计算机被病毒感染，其内部的所有数据、信息及核心机密都将在病毒制造者面前暴露，他可以随心所欲地控制受感染的计算机来达到自己的目的。

5. 利用心理学及社会工程学

充分利用了心理学的知识，注重挖掘人类的心理，如好奇、贪婪等。前一阵肆虐一时的裸妻病毒，主题就是英文的“裸妻”，邮件正文为“我的妻子从未这样”，邮件附件中携带一个名为“裸妻”的可执行文件，用户执行这个文件，病毒就被激活。还有出现的 My-baby picture 病毒，通过可爱宝宝的照片传播病毒。而“库尔尼科娃”病毒的大流行，更是由于“网坛美女”库尔尼科娃挡不住的魅力。此外，每次重大事件都会成为病毒传播的良机，2008 北京奥运会全球瞩目，更是成为病毒作者瞄准的目标。

6. 病毒更加智能化

过去，人们的观点是“只要不打开电子邮件的附件，就不会感染病毒”。但是，新一代计算机病毒却令人震惊，例如，大名鼎鼎的维罗纳（Verona）病毒是一个真正意义上的“超级病毒”，它不仅主题众多，而且集邮件病毒的几大特征为一身，令人无法设防。最严重的是它将病毒写入邮件原文。这正是维罗纳病毒的新突破，一旦用户收到了该病毒邮件，无论是无意间用 Outlook 打开了该邮件，还是仅仅使用了预览，病毒就会自动发作，并将一个新的病毒邮件发送给邮件通讯录中的地址，从而迅速传播。这就使得一旦“维罗纳”类的病毒来临，用户将根本无法逃避。该病毒本身对用户计算机系统并不造成严重危害，但是这一病毒的出现已经是病毒技术的一次巨大“飞跃”，它无疑为今后更大规模、更大危害病毒的出现做了一次技术上的试验及预演，一旦这一技术与以往危害更大的病毒技术或恶意程序、特洛伊木马等相结合，将造成无法想象的危害。

7. 病毒将全面进入驱动级

进入 2008 年以后，大部分主流病毒技术都进入了驱动级。病毒已经不再一味逃避杀毒软件的追杀，而是开始与杀毒软件争抢系统驱动的控制权，在争抢系统驱动控制权后，转而控制杀毒软件，使杀毒软件功能失效。病毒通过生成驱动程序，与杀毒软件争抢系统控制权限，通过修改 SSDT（SSDT 是 Windows 系统的系统服务描述表，通过修改此表的函数地址可以对常用 Windows 函数及 API 进行挂钩，从而实现对一些敏感的系统动作进行过滤、监控的目的。一些 HIPS、防毒软件、系统监控、注册表监控软件往往会采用此接口来实现自己的监控模块，目前极个别病毒确实会采用这种方法来保护自己或者破坏防毒软件，如果在这种病毒进入系统前被防毒软件识别并清除，它将没有机会发作）等技术实现 Windows API HOOK，从而使得杀毒软件监控功能失效。

1.2　计算机病毒分类及命名

从第一个病毒问世以来，究竟世界上有多少种病毒，说法不一。但是，有一点可以确定：病毒的数量仍在不断增加。据国外统计，计算机病毒以 10 种/周的速度递增，另据公安部统计，在国内病毒以 4~6 种/月的速度递增。随着计算机病毒数目的增多，危害也不断增加。这就要求对计算机病毒及其行为特征进行规范化的定义，从而对计算机病毒开展科学化的研究。这里从基础开始，先讨论病毒的分类及命名。

1.2.1　病毒的分类

现在，对病毒比较科学的命名是建立在对病毒的分类上的，因此应首先讨论病毒的分类。

按照计算机病毒的特点及特性，计算机病毒的分类方法有许多种。因此，同一种病毒可能有多种不同的归类法。

1. 按照计算机病毒攻击的系统分类

(1) 攻击 DOS 系统的病毒　这类病毒出现最早、最多，变种也最多，早期我国出现的计算机病毒基本上都是这类病毒，此类病毒占病毒总数的 99%。

(2) 攻击 Windows 系统的病毒　由于 Windows 的图形用户界面（GUI）和多任务操作系统深受用户的欢迎，Windows 正逐渐取代 DOS，从而成为病毒攻击的主要对象。目前发现的首例破坏计算机硬件的 CIH 病毒就是一个攻击 Windows 95/98 的病毒。

(3) 攻击 Unix 系统的病毒　当前，Unix 系统应用非常广泛，并且许多大型的操作系统均采用 Unix 作为其主要的操作系统，所以 Unix 病毒的出现，对人类的信息处理也是一个严重的威胁。

(4) 攻击 OS/2 系统的病毒　世界上已经发现第一个攻击 OS/2 系统的病毒，它虽然简单，但是一个不祥之兆。

2. 按照病毒的攻击机型分类

(1) 攻击微型计算机的病毒　这是世界上传染最为广泛的一种病毒。

(2) 攻击小型机的计算机病毒　小型机的应用范围是极为广泛的，它既可以作为网络的一个节点机，也可以作为小型计算机网络的主机。起初，人们认为计算机病毒只有在微型计算机上才能发生，而小型机则不会受到病毒的侵扰，但自 1988 年 11 月份 Internet 网络受到 Worm 病毒的攻击后，使得人们认识到小型机也同样不能免遭计算机病毒的攻击。

(3) 攻击工作站的计算机病毒　近几年来，计算机工作站有了较大的进展，并且其应用范围也有了较大的发展，所以不难想象，攻击计算机工作站的病毒的出现也是对信息系统的一大威胁。

3. 按照计算机病毒的链接方式分类

由于计算机病毒本身必须有一个攻击对象，以实现对计算机系统的攻击。计算机病毒所攻击的对象是计算机系统可执行的部分。

(1) 源码型病毒　该类病毒攻击高级语言编写的程序，该类病毒在高级语言所编写的程序编译前插入到原程序中，经编译成为合法程序的一部分。

(2) 嵌入型病毒　这种病毒是将自身嵌入到现有程序中，把计算机病毒的主体程序与其攻击的对象以插入的方式链接。这种计算机病毒是难以编写的，一旦侵入程序体后也较难消除。如果同时采用多态性病毒技术、超级病毒技术和隐蔽性病毒技术，将给当前的反病毒技术带来严峻的挑战。

(3) 外壳型病毒　外壳型病毒将其自身包围在主程序的四周，对原来的程序不做修改。这种病毒最为常见，易于编写，也易于发现，一般通过测试文件的大小即可知。

(4) 操作系统型病毒　这种病毒用它自己的程序意图加入或取代部分操作系统进行工作，具有很强的破坏力，可以导致整个系统的瘫痪。圆点病毒和大麻病毒就是典型的操作系统型病毒。这种病毒在运行时，用自己的逻辑部分取代操作系统的合法程序模块，根据病毒自身的特点和被替代的操作系统中合法程序模块在操作系统中运行的地位与作用，以及病毒取代操作系

统的取代方式等，对操作系统进行破坏。

4. 按照计算机病毒的破坏情况分类

按照计算机病毒的破坏情况可分为以下两类。

(1) 良性计算机病毒　良性病毒是指其不包含有立即对计算机系统产生直接破坏作用的病毒。这类病毒为了表现其存在，只是不停地进行扩散，从一台计算机传染到另一台，并不破坏计算机内的数据。

(2) 恶性计算机病毒　恶性病毒是指在其代码中含有损伤和破坏计算机系统的操作指令，在其传染或发作时会对计算机系统产生直接的破坏作用。

5. 按照计算机病毒的寄生部位或传染对象分类

传染性是计算机病毒的本质属性，根据寄生部位或传染对象分类，也即根据计算机病毒的传染方式进行分类，有以下几种。

(1) 传染磁盘引导区的计算机病毒　传染磁盘引导区的病毒主要是用病毒的全部或部分逻辑取代正常的引导记录，将正常的引导记录隐藏在磁盘的其他地方。由于引导区是磁盘能正常使用的先决条件，因此，这种病毒在运行的一开始（如系统启动）就能获得控制权，其传染性较大。

由于在磁盘的引导区内存储着需要使用的重要信息，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的破坏。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。

(2) 传染操作系统的计算机病毒　操作系统是一个计算机系统得以运行的支持环境，它包括.com、.exe 等许多可执行程序及程序模块。传染操作系统的计算机病毒就是利用操作系统中所提供的一些程序及程序模块寄生并传染的。通常这类病毒作为操作系统的一部分，只要计算机开始工作，病毒就处在随时可能被触发的状态。而操作系统的开放性和不绝对完善性给这类病毒出现的可能性与传染性提供了方便。操作系统传染的病毒目前已广泛存在，黑色星期五即为此类病毒。

(3) 传染可执行程序的计算机病毒　传染可执行程序的病毒通常寄生在可执行程序中，一旦程序被执行，病毒也就被激活，病毒程序首先被执行，并将自身驻留内存，然后设置触发条件，进行传染。

对于以上三种病毒的分类，实际上可以归纳为两大类：一类是传染引导区的计算机病毒，另一类是传染可执行文件的计算机病毒。

6. 按照计算机病毒激活的时间分类

按照计算机病毒激活的时间可分为定时和随机病毒。

(1) 定时病毒　定时病毒仅在某一特定时间才发作。

(2) 随机病毒　随机病毒一般不是由时钟来激活的。

7. 按照传播媒介分类

按照计算机病毒的传播媒介来分类，可分为单机病毒和网络病毒。

(1) 单机病毒　单机病毒的载体是磁盘，常见的是病毒从软盘传入硬盘，感染系统，然后再传染给其他软盘，软盘又传染给其他系统。

(2) 网络病毒　网络病毒的传播媒介不再是移动式载体，而是网络通道。这种病毒的传染性更强，破坏性更大。

8. 按照寄生方式和传染途径分类

人们习惯于将计算机病毒按寄生方式和传染途径来分类。计算机病毒按其寄生方式大致可分为以下两类。

(1) 引导型病毒　引导型病毒是一种在执行 ROM BIOS 之后，系统引导时出现的病毒，它先于操作系统运行，依托的环境是 BIOS 中断服务程序。引导型病毒利用操作系统的引导模块放在某个固定的位置，并且控制权的转交方式是以物理位置为依据，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，而将真正引导区的内容转移或替换，待病毒程序执行后，将控制权交给真正的引导区内容，使得这个带病毒的计算机系统看似正常运转，而病毒已隐藏其中，并伺机发作、传染。

引导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、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、2708、INT60 病毒等。BR 病毒是将病毒寄生在硬盘逻辑 0 扇或软盘逻辑 0 扇（即 0 面 0 道第 1 个扇区）。典型的病毒有 Brain、小球病毒等。

引导型病毒的主要特征如下。

① 引导型病毒在安装操作系统之前进入内存，寄生对象又相对固定，因此该类病毒基本上不得不采用减少操作系统所掌管的内存容量方法来驻留内存高端。而正常的系统引导过程一般是不减少系统内存的。

② 引导型病毒需要把病毒传染给软盘，一般是通过修改 INT 13H 的中断向量，而新 INT 13H 中断向量段址必定指向内存高端的病毒程序。

③ 引导型病毒感染硬盘时，必定驻留硬盘的主引导扇区或引导扇区，并且只驻留一次，因此引导型病毒一般都是在软盘启动的过程中把病毒传染给硬盘的。而正常的引导过程一般不对硬盘主引导区或引导区进行写盘操作。

④ 引导型病毒的寄生对象相对固定，把当前的系统主引导扇区和引导扇区与干净的主引导扇区和引导扇区进行比较，如果内容不一致，可认定系统引导区异常。

(2) 文件型病毒　文件型病毒与引导型病毒运行的方式完全不同。在各种 PC 机病毒中，文件型病毒占的数目最大，传播得广，采取的手段也多种多样。文件型病毒对源文件进行修改，使其成为新的文件。文件型病毒分为两种：一种是将病毒加在文件的前部，一种是加在文件尾部。

文件型病毒传染的对象主要是.com 和.exe 文件。它们再按其传染途径又可分为驻留内存型和不驻留内存型，驻留内存型按其驻留内存方式又可进一步细分。

9. 按世代分类

病毒自诞生至今，大致可以分为五代，每一代都有新的技术和功能被纳入，每一代都比上一代更加难以检测和查杀。

(1) 第一代病毒（简单型，simple）　这一代病毒都很简单，它们除了自我复制以外并没有其他什么动作，因此造成的危害较小。比如，引导型病毒会造成一些扇区的数据被重写，而一些文件病毒则会占用系统资源等。这类病毒有可能因为自身和软件的不兼容而导致一些破坏，虽然病毒编制者并没有预料到这种情况。而且，第一代病毒没有采取任何保护自己的措施，因而很容易被发现。

(2) 第二代病毒（自我识别型，self-recognition）　由于第一代病毒采取不断自我复制以至使内存急剧增加，从而很容易被识别，第二代病毒引入一种签名技术，来标记每一个被自己

感染的文件，当这种签名不存在时，它们才会继续感染。这种病毒被认为是一种自我认知的，因此被发现概率较第一代病毒低。

(3) 第三代病毒（窃取技术，stealth）　因为大部分病毒都是在查毒软件对二级存储区进行扫描时，通过模式识别的方法扫描出来的，因此，一些驻留病毒采取了类似“偷窃”的技术，即它们会在激活时窃取系统服务调用中断，这样调用这些服务的行为就将导致病毒代码的执行，从而一些服务返回的值是被病毒所操控的。这种病毒显然在隐蔽性方面优于前两代病毒。但是在一些基于行为的扫描中却较容易被发现。

(4) 第四代病毒（加套技术，armored）　越来越多的工具被开发出来，用于研究病毒，以至于很多病毒的代码都可以通过反汇编的手段推测出来，因而“套”技术被运用至病毒中来。病毒的编制者通过在代码中加入许多杂乱的、没有实际意义的代码来使病毒研究者难以对源码进行分析。通常，此类病毒往往也会攻击反病毒软件，可见，第四类病毒的破坏能力是很强的。

(5) 第五代病毒（变形技术，polymorphic）　这代病毒运用的“变形”技术类似于前面所讲的多态病毒，病毒编制者将病毒体加密，而且在每一次感染之后都会对代码序列进行调整，然后再加密，而且有些病毒的加密程序也是会随机改变的，这样使得反病毒软件很难侦测到。

1.2.2　病毒的命名

计算机病毒的命名是由反病毒软件公司或反病毒软件专家来完成的，这里要讲的命名也是从反病毒的角度来讨论的。值的指出的是，从病毒编制者的角度来看，病毒肯定是需要名字的，与其他的软件程序一样，病毒也需要一个文件名，而这个文件名和从反病毒角度讲的命名不是一回事。

1. 计算机病毒的命名规则

很多时候大家已经用杀毒软件查出了自己的计算机中有例如 Backdoor. RmtBomb.12、Trojan.Win32.SendIP.15 等一串英文还带数字的病毒名，这时有些人就懵了，那么长一串的名字，怎么知道是什么病毒啊？其实只要掌握一些病毒的命名规则，就能通过杀毒软件的报告中出现的病毒名来判断病毒的一些共有的特性了。

世界上有那么多的病毒，反病毒软件公司为了方便管理，会按照病毒的特性将病毒进行分类命名。虽然每个反病毒软件公司的命名规则都不太一样，但大体都是采用一个统一的命名方法来命名的。一般格式为

[病毒前缀] + [病毒名] + [病毒后缀]

病毒前缀是指一个病毒的种类，它是用来区别病毒的种族分类的。不同种类的病毒，其前缀也是不同的。比如常见的木马病毒的前缀 Trojan，蠕虫病毒的前缀是 Worm，其他前缀还有 Macro、Backdoor、Script 等。

病毒名是指一个病毒的家族特征，是用来区别和标记病毒家族的，如以前著名的 CIH 病毒的家族名都是统一的“CIH”，还有后来闹得人心不安的振荡波蠕虫病毒的家族名是“Sasser”。

病毒后缀是指一个病毒的变种特征，用来区别具体某个家族病毒的某个变种。一般都采用英文中的 26 个字母来表示，如 Worm.Sasser.b 就是指振荡波蠕虫病毒的变种 B，因此也称为“振荡波 B 变种”或“振荡波变种 B”。如果该病毒变种非常多（也表明该病毒生命力顽强），可以采用数字与字母混合表示变种标记。

综上所述，一个病毒的前缀对于快速地判断该病毒属于哪种类型的病毒有非常大的帮助。通过判断病毒的类型，就可以对这个病毒有个大概的评估。而通过病毒名可以利用查找资料等

方式进一步了解该病毒的详细特征。病毒后缀能告诉你计算机里存在的病毒是哪个变种。

病毒的命名并没有完全统一的规定，每种病毒文件的命名规则都不太一样，但基本都是采用前、后缀法来进行命名的，可以是多个前缀、后缀的组合，中间以“.”分隔，一般格式为

[前缀].[病毒名].[后缀]

有一定基础的读者如果确认发现新的病毒，自己可以按此规则起个有特色的名称。

2. 病毒的命名解释

一个病毒前缀对于快速的判断该病毒属于哪种类型的病毒有非常大的帮助。通过判断病毒的类型，就可以对这个病毒有个大概的评估（当然这需要积累一些常见病毒类型的相关知识，将在后续章节进行讨论）。依据病毒名可以通过查找资料等方式进一步了解该病毒的详细特征。

下面是一些常见的病毒前缀的解释（针对用得最多的 Windows 操作系统）。

(1) 系统病毒　系统病毒的前缀为 Win32、PE、Win95、W32、W95 等。这些病毒的一般共有特征是可以感染 Windows 操作系统的.exe 和.dll 文件，并通过这些文件进行传播，如 CIH 病毒。

(2) 蠕虫病毒　蠕虫病毒的前缀为 Worm。这种病毒的共有特征是通过网络或系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。比如冲击波（阻塞网络）、小邮差（发带毒邮件）等。

(3) 木马病毒、黑客病毒　木马病毒的前缀为 Trojan，黑客病毒前缀名一般为 Hack。木马病毒的共有特征是通过网络或系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息；黑客病毒有一个可视的界面，能对用户的计算机进行远程控制。木马、黑客病毒往往是成对出现的，即木马病毒负责侵入用户的计算机，而黑客病毒则会通过该木马病毒来进行控制。现在这两种类型已趋向于整合了。一般的木马病毒如 QQ 消息尾巴木马 Trojan.QQ3344，还有比较常见的针对网络游戏的木马病毒如 Trojan.LMir.PSW.60。这里补充一点，病毒名中有 PSW 或者什么 PWD（“密码”的英文“password”缩写）之类的一般都表示这个病毒有盗取密码的功能。一些黑客程序如：网络枭雄（Hack.Nether.Client）等。

(4) 脚本病毒　脚本病毒的前缀为 Script。脚本病毒的共有特征是使用脚本语言编写，通过网页进行传播，如红色代码（Script.Redlof）。脚本病毒还会有如下前缀：VBS、JS（表明是何种脚本编写的），如欢乐时光（VBS.Happytime）、十四日（JS.Fortnight.c.s）等。

(5) 宏病毒　宏病毒也是脚本病毒的一种，由于它的特殊性，因此在这里单独算成一类。宏病毒的前缀为 Macro，第二前缀为 Word、Word97、Excel、Excel97（也许还有别的）其中之一。凡是只感染 Word97 及以前版本 Word 文档的病毒采用 Word97 作为第二前缀，格式为 Macro.Word97；凡是只感染 Word97 以后版本 Word 文档的病毒采用 Word 作为第二前缀，格式为 Macro.Word；凡是只感染 Excel97 及以前版本 Excel 文档的病毒采用 Excel97 作为第二前缀，格式是：Macro.Excel97；凡是只感染 Excel97 以后版本 Excel 文档的病毒采用 Excel 作为第二前缀，格式是：Macro.Excel，依此类推。该类病毒的共有特征是能感染 Office 系列文档，然后通过 Office 通用模板进行传播，如：著名的梅莉莎（Macro.Melissa）。

(6) 后门病毒　后门病毒的前缀为 Backdoor。该类病毒的共有特征是通过网络传播，给系统开后门，给用户计算机带来安全隐患。如 540 的很多朋友遇到过的 IRC 后门 Backdoor.IRCBot。

(7) 种植程序病毒　这类病毒的共有特征是运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来的新病毒产生破坏。如：冰河播种者（Dropper.BingHe2.2C）、MSN

此为试读，需要完整PDF请访问：www.ertongbook.com