电脑报 东方工作室

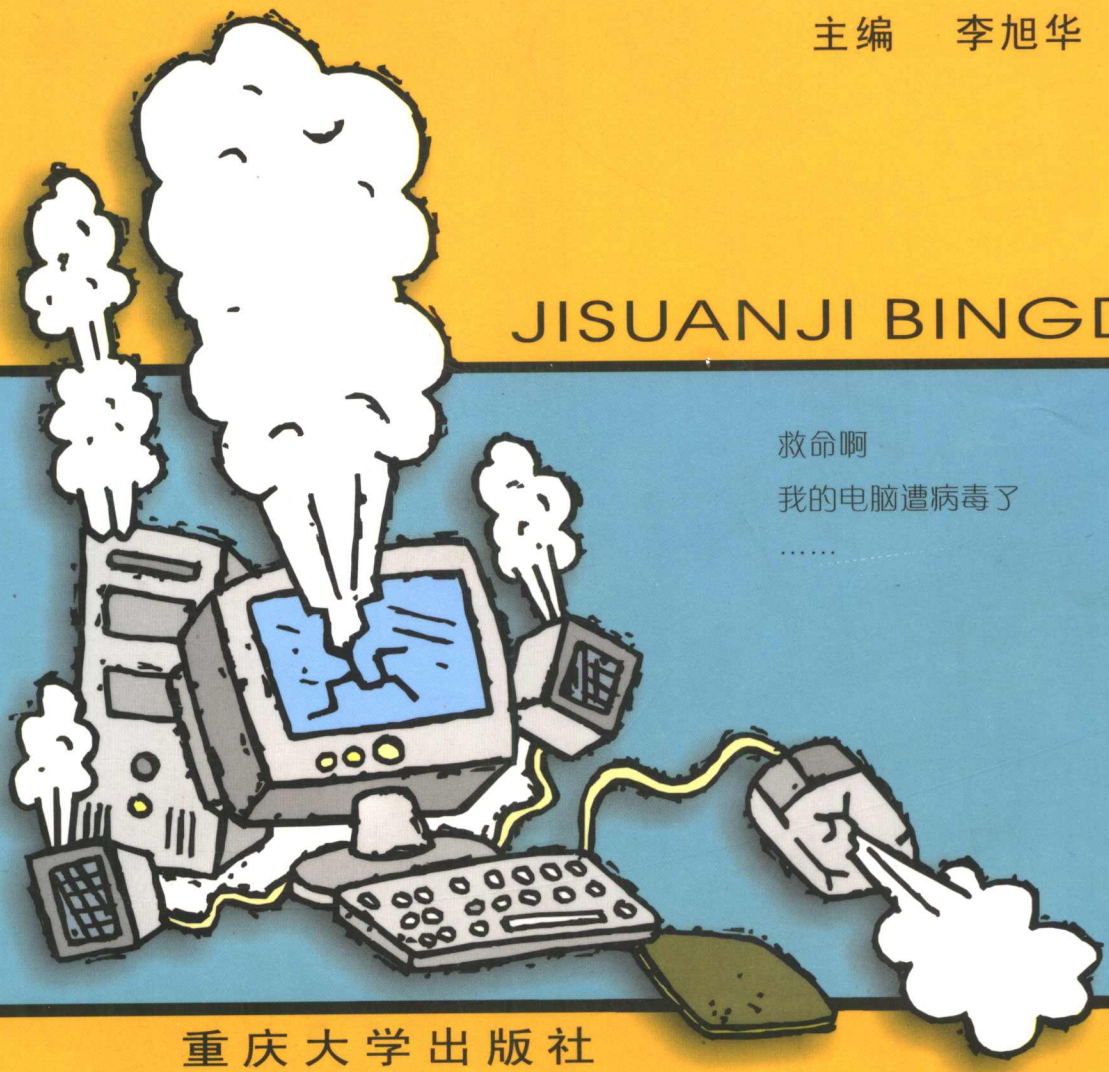
轻松玩转系列
It is easy

计算机病毒

病毒机制与防范技术

主编 李旭华

JISUANJI BINGDU



重庆大学出版社

轻松玩转系列

计算机病毒

——病毒机制与防范技术

李旭华 主编

重庆大学出版社

内容提要

本书在保证必须的基础知识、基本理论的基础上，深入地探讨了病毒的机制和防范技术。本书在内容的组织上，不追求包罗万象、面面俱到，而着重保证把最基本、最适用的部分包含进来，重点分析当今互联网上各种典型的病毒源代码，病毒的新编制技术和新对抗技术。通过阅读本书，可使读者较为全面地了解计算机病毒，认识计算机病毒，分析计算机病毒，预防计算机病毒，对抗计算机病毒。希望读者能在使用中不用花太多精力，利用书中的手段去解决在网络或单机中所遇到的大部分计算机病毒故障 。

本书适合于广大计算机用户，特别是计算机维护人员和信息安全领域的工作人员。

图书在版编目（CIP）数据

计算机病毒 / 李旭华主编. - 重庆:
重庆大学出版社，2002.4
(轻松玩转系列)
ISBN 7-5624-2554-X

Ⅰ.计… Ⅱ.李… Ⅲ.计算机病毒-防治-基本知识 Ⅳ.TP309.5

中国版本图书馆 CIP 数据核字（2002）第 007858 号

轻松玩转系列

计算机病毒

——病毒机制与防范技术

李旭华　　主　编
责任编辑　陈 其　汤 琪

*

重庆大学出版社出版发行
新　华　书　店　经　销
重庆电力印刷厂印刷

*

开本：787 × 1092　1/16　印张：22.75　字数：568 千
2002 年 4 月第 1 版　　2002 年 4 月第 1 次印刷

印数：1 — 5 000

ISBN 7-5624-2554-X/TP · 344　定价 30.00 元

序

随着微电子技术和互连网信息的快速发展，计算机的硬件故障率大为降低。相反地，微机系统的大型化和复杂化，使微机的安全性和可靠性越来越难对付，而这些又主要反映在计算机病毒上。所以，毫不夸张地说，计算机病毒是目前计算机安全中的一大威胁。

然而，在广大计算机使用者当中，对计算机病毒有着正确认识的却为数不多，大多数的人谈毒色变，更有甚者以为计算机病毒会传染给人类本身，对计算机避而远之……这些听起来似乎只有在笑话里才会出现的情景，却时常在我们身边发生着……

前不久，编者的一个朋友刚刚购买了一台电脑，却因为害怕病毒而不敢正常使用，电脑大部分处于闲置状态，因为我的这位朋友坚信“只要不开电脑就不会被传染病毒。所以，为了避免病毒侵害计算机，就尽量少开机或干脆不开机。”，这些话使我哭笑不得，于是本人决定给这位朋友上一课。其实基本上是我强行要求的，想过一把当老师的瘾，哈哈哈……

星期日一大早这位朋友就来到我的工作室，对了，还没告诉大家，我的这位其实是个美媚哟 *_^ 我们就称呼她为“美媚”吧，至于我嘛，以“小编”自居。

小编：“美媚，来的真早啊！”

美媚：“哎……想起今天你要给我上课，害的我昨天整整一夜没睡好。”

小编：“（神采飞扬，有点害羞）原来你那么盼着听我上课啊！真没看出来，我原来还是当老师的材料，其实……我看得出你对我有意思。”

美媚：“（狂翻白眼）你说什么呢？！我只不过是想到你那张脸，难过的睡不着，别自作多情了。”

小编：“（整了整发型）好了，好了，言归正传，让我来给你说说电脑杀手——病毒吧。”

美媚：“好的，我洗耳恭停。”

小编：“（得意洋洋）美媚，我先考考你，你知道计算机病毒的概念是谁先提出来的吗？”

美媚：“（暗喜，昨天正好在报上看到，脸上装出迷茫的表情）好像是1977年一个美国科普作家叫……叫“雷恩”的提出来的吧。

小编：“（惊讶，尴尬）你……，说得差不多。那你知道病毒有什么特点吗？”

美媚：“特点？有毒！绝对有毒！”

小编：“（晕倒）又瞎说，让我来告诉你吧！电脑病毒一般有四大特点。第一，寄生性。也就是说，计算机病毒一般寄生在其他程序之中，当你执行这个程序时，病毒就起破坏作用，而在未启动这个程序之前，它是不易被人发觉的。

美媚："那第二点呢？"

小编："计算机病毒的第二点特征是传染性，一旦它被复制或产生变种，其速度之快令人难以预防，嘿嘿嘿……"

美媚："（若有所思）哦！那第三点肯定是潜伏性，潜伏在机体内，不到发作的时候很难发现。"

小编："（诧异）你怎么知道？！"

美媚："（得意）你忘了，我爸可是医生，我听你越说越象感冒症状。"

小编："呵呵呵，孺子可教也！要不然怎么会叫计算机病毒呢？不过，它可比感冒复杂多了。"

美媚："我乱说的，还真对了。那第四点特点呢？

小编："这第四点就是，隐藏性，计算机病毒具有很强的隐藏性，有的可以通过病毒软件检查出来，有的根本就查不出来，有的时隐时现，变化无常，这类病毒处理起来通常很困难。"

美媚："那计算机感染上病毒后，会再现出什么症状呢？"

小编："症状很多，我大致总结了一些，只要留心，就一定能发现病毒的珠丝马迹。"

美媚："你说说看。"

小编："大致有以下几点……"

小编用了一上午的时间，总算让美媚对计算机病毒有了一点大致的了解，现在美媚终于可以放心使用计算机了，还时常将她的"病毒"知识向身边朋友们传授着，小编看着甚是欣慰，好歹我也是美媚的半个老师嘛。但小编想到，我可以用一上午的时间教懂美媚，而其他那些对计算机世界充满好奇而对计算机病毒又十分畏惧的朋友们又怎么办呢？我们都知道，恐惧的产生是来自对事物的无知，人类总是对神秘的东西感到害怕，然而，当你揭开那层神秘的面纱时，你会发觉，其实那东西并不可怕。只是，我们通常缺少一种去揭开那层神秘面纱的工具……

小编经过一段时间的思考，终于决定倾尽所能写一本有关计算机病毒的书，于是这本书就这样诞生了，编写这本书是为了适应广大读者，力求通俗易懂，能解决实际问题，在内容的组织上，不追求包罗万象，面面俱到，而着重保证把最基本，最适用的部分包含进来，重点分析当今互连网上典型的各种病毒原代码，病毒的新编制技术和新对抗技术。小编衷心的希望本书可使你较为全面地了解计算机病毒，认识计算机病毒，分析计算机病毒，预防计算机病毒，对抗计算机病毒。希望读者能在使用中不用花太多精力，利用书中的手段去解决在网络或单机中所遇到的大部分计算机病毒故障。

由于编者水平有限，书中难免有疏漏和错误之处，敬请广大读者批评指正。

编　者

2002年3月3日

此为试读，需要完整PDF请访问：www.ertongbook.com

目录

第 1 章　计算机病毒概述 1
1.1　计算机病毒的概念 2
1.2　计算机病毒的特点 2
1.2.1　传染性 2
1.2.2　非授权性 2
1.2.3　隐蔽性 2
1.2.4　潜伏性 2
1.2.5　破坏性 2
1.2.6　不可预见性 2
1.3　计算机病毒的分类 2
1.3.1　按照计算机病毒攻击的系统分类 4
1.3.2　按照计算机病毒的攻击机型分类 4
1.3.3　按照计算机病毒的链接方式分类 4
1.3.4　按照计算机病毒的破坏情况分类 5
1.3.5　按照计算机病毒激活的时间分类 5
1.3.6　按照传播媒介分类 6
1.3.7　按照寄生方式和传染途径分类 6
1.4　计算机病毒的检测方法 7
1.4.1　特征代码法 7
1.4.2　校验和法 8
1.4.3　行为监测法 9
1.4.4　软件模拟法 10
第 2 章　计算机病毒分析 11
2.1　病毒技术基础 12
2.1.1　内存 12
2.1.2　中断 15
2.1.3　自加密 16
2.1.4　反跟踪 18
2.1.5　其他 18

2.2 病毒代码结构浅析 19
2.3 tpvo 003-1 Stealth 隐藏类型病毒代码分析 32
2.4 3783 病毒原代码分析 48
2.4.1 病毒介绍 48
2.4.2 病毒分析 48
2.4.3 杀毒要点 50
2.5 典型邮件型病毒代码分析 52
2.6 “万花谷”网页病毒代码分析 56
2.6.1 该病毒的技术特征 57
2.6.2 具体的表现形式 57
2.7 爱虫病毒代码和杀毒方法分析 61
2.8 伴随型病毒代码分析 78
第3章 计算机病毒的编制 95
3.1 病毒工作流程 96
3.2 病毒引导原理 96
3.2.1 分区的一般概念 97
3.2.2 问题的提出 97
3.2.3 分区的深入理解 97
3.2.4 理解硬盘自举 98
3.2.5 问题的解决 98
3.3 病毒的传播途径 99
3.3.1 硬盘 99
3.3.2 软盘 99
3.3.3 光盘 99
3.3.4 网络 99
3.4 病毒的传播机理 99
3.5 DOS 病毒的编制原理 100
3.5.1 COM 文件结构及原理 100
3.5.2 EXE 文件结构及原理 101
3.5.3 引导型病毒原理 102
3.5.4 文件型病毒原理 110
3.5.5 病毒感染 COM 文件的方法 111
3.6 Win9X 病毒的编制原理 116
3.6.1 Win9X 系统平台信息 116
3.6.2 Win9X 下病毒工作原理 119
3.7 简单病毒编写范例 121
第4章 计算机病毒与故障的区别 133
4.1 计算机病毒的现象与查解方法 134
4.2 与病毒现象类似的硬件故障 135

4.3 与病毒现象类似的软件故障 136
第5章 计算机病毒防范 139
5.1 技术预防措施 140
5.2 引导型病毒的防范措施 142
5.3 文件型病毒的防范措施 143
5.4 宏病毒的识别和防范措施 144
5.5 电子邮件病毒的识别和防范 145
5.6 单机病毒防范措施 147
5.6.1 杀毒软件的选择 147
5.6.2 主要的防护工作 149
5.7 网络病毒防范措施 149
5.7.1 网络病毒的特点 149
5.7.2 基于网络安全体系的防毒管理措施 150
5.7.3 基于工作站与服务器的防毒技术 151
5.7.4 网络病毒清除方法 153
5.7.5 网络病毒的预防与管理措施 154
第6章 计算机病毒破坏及修复 161
6.1 计算机病毒的破坏行为 162
6.2 计算机病毒的一般修复处理方法 163
6.3 病毒破坏后的硬盘修复方法 163
6.3.1 硬盘盘卷结构 164
6.3.2 DOS 盘卷结构 164
6.3.3 硬盘分区表详解 165
6.3.4 病毒破坏硬盘全剖析 169
6.3.5 基础知识 173
6.3.6 恢复被 CIH 破坏的硬盘数据几种方法 173
6.4 其他硬件的修复方法 176
第7章 新病毒分析与对抗技术 179
7.1 新病毒捕获与取样 180
7.1.1 采集新病毒样本 180
7.1.2 识别主引导型病毒 181
7.1.3 识别引导型病毒 182
7.1.4 识别 DOS 系统文件病毒 182
7.1.5 识别文件型病毒 182
7.2 新病毒分析与诊治实例 183
7.2.1 HXH 病毒的引导过程 183
7.2.2 HXH 病毒的传染过程 184
7.2.3 HXH 病毒的病发过程 185
7.2.4 HXH 病毒的诊断 185

7.2.5 HXH病毒的清除 186
7.3 最新病毒解决方案 187
7.3.1 蓝色代码解决方案 187
7.3.2 红色代码解决方案 189
7.3.3 欢乐时光解决方案 192
7.3.4 流行邮件病毒I_WORM.MTX的解决方案 193
第8章 反病毒软件技术及产品介绍 195
8.1 反病毒软件的作用原理 196
8.1.1 病毒检测软件的作用原理 196
8.1.2 病毒消除软件的作用原理 196
8.1.3 病毒预防软件的作用原理 197
8.1.4 防病毒卡的作用原理 198
8.2 杀毒机理与杀毒原则 200
8.3 反病毒软件技术 200
8.3.1 常见反病毒技术 200
8.3.2 流行反病毒技术 203
8.4 反病毒产品在使用中的必须要求 204
8.5 对反病毒产品服务的必须要求 204
8.6 对反病毒产品的选购建议 205
8.7 知名杀毒软件介绍 206
8.7.1 金山毒霸2002 206
8.7.2 诺顿防毒 2001中文版 209
8.7.3 KILL2000 210
8.7.4 瑞星杀毒软件2002版 213
8.7.5 KV3000 214
8.7.6 扫描杀毒工具SCAN & CLEAN 216
8.7.7 超级杀毒工具NAV 217
8.7.8 集成杀毒工具CPAV/MSAV 217
8.7.9 共享杀毒程序F-PROT 218
第9章 典型计算机病毒介绍 219
9.1 Win32/Updatr.worm.12288病毒 220
9.2 Win32/Goner.worm.38912病毒 223
9.3 Win32/Eira.worm病毒 226
9.4 Win32/Badtrans.worm.29020病毒 228
9.5 Win32/Klez.worm.91978病毒 230
9.6 Win32/Klez.worm病毒 232
9.7 TROJ_MELTING.A蠕虫病毒 234
9.8 W2k.Infis.4608的病毒 234
9.9 Win32.Kriz（圣诞杀手）病毒 235

9.10 HAPPY99 病毒 236
9.11 Melissa（“美丽莎”）病毒 236
9.12 Win95.Notes 病毒 237
9.13 BO 病毒 237
9.14 July.killer 病毒 238
9.15 CIH 病毒 239
9.16 旋律病毒 VBS.Tune.A 240
9.17 “美丽公园”病毒 W32/pretty.worm.ump 240
9.18 罗密欧与朱丽叶病毒 240
9.19 电子邮件蠕虫病毒 Badtrans.b 242
9.20 网络病毒 “冰冷世界” 244
9.21 “求职信”病毒 245
9.22 Worm.Sircam.137216 蠕虫病毒（金山毒霸命名） 247
9.23 VBS_Homepage.A 烘焙鸡病毒 248
9.24 VBS.HappyTime 病毒 250
附 录 253
附录 1 汇编语言的常用源程序结构 254
附录 2 常用端口大全表 255
附录 3 DEBUG 的便用方法 264
附录 4 “欢乐时光”病毒源代码详细分析 265
附录 5 CIH 病毒 1.4 版本源代码详细分析 279
附录 6 3783 病毒源码清单 305
附录 7 相关的法律及其标准 350

计算机病毒
——病毒机制与防范技术

1 第1章 计算机病毒概述

21世纪刚刚拉开序幕，已陆续出现了许多种新计算机病毒，包括以“新年”(New Year)为电子邮件主题的VBS_TQLL.A病毒，它选在新旧世纪交替时现身，着实令计算机用户虚惊了一场；NAVIDAD.A——圣诞节病毒的“变身”，以其大量散播垃圾邮件的破坏力，在我国台湾造成中度感染灾情。由于病毒的花样不断翻新，编程手段越来越高，特别是Internet的广泛应用，促进了病毒的空前活跃，网络蠕虫病毒传播更快更广，Windows病毒更加复杂，带有黑客性质的病毒和特洛伊木马等大量涌现，更是当前网络面临的一大威胁。因此，我们有必要了解病毒知识及其编制方法，以有利于我们推进互联网的安全发展。在本章中，首先重点介绍病毒的基础知识，层层深入地让读者对病毒有一个全面的认识。

此为试读，需要完整PDF请访问：www.ertongbook.com

1.1 计算机病毒的概念

“计算机病毒”与医学上的“病毒”不同，它不是天然存在的，而是某些人利用计算机软、硬件所固有的脆弱性，编制的具有特殊功能的程序。它能通过某种途径潜伏在计算机存储介质(或程序)里，当达到某种条件时即被激活。它以修改其他程序的方法将自己的精确拷贝或者可能演化的形式放入其他程序中，从而感染它们，对计算机资源进行破坏。

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《条例》第28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。”

1.2 计算机病毒的特点

1.2.1 传染性

计算机病毒的传染性是指病毒具有把自身复制到其他程序中的特性。

正常的计算机程序一般是不会将自身的代码强行连接到其他程序上的。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上。计算机病毒可通过各种可能的途径，如软盘、计算机网络去传染其他的计算机。当在一台计算机上发现了病毒时，往往曾在这台计算机上用过的软盘也已感染上了病毒，而与这台计算机联网的其他计算机也许也被该病毒传染上了。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。

1.2.2 隐蔽性

一般正常的程序是由用户调用，再由系统分配资源，完成用户交给的任务，其目的对用户来说是可见的、透明的。而病毒具有正常程序的一切特性，它隐藏在正常程序中，当用户调用正常程序时，它窃取到系统的控制权，先于正常程序执行，病毒的动作、目的对用户来说是未知的，是未经用户允许的。

1.2.3 潜伏性

病毒一般是具有很高编程技巧、短小精悍的程序，通常附在正常程序中或磁盘较隐蔽的地方。也有个别的以隐含文件形式出现，目的是不让用户发现它的存在。如果不经过代码分析，病毒程序与正常程序是不容易区别开来的。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，使用户不会感到任何异常。正是由于这种隐蔽性，计算机病毒才得以在用户没有察觉的情况下传播到上百万台计算机中。

大部分的病毒的代码之所以设计得非常短小，也是为了便于隐藏。病毒一般只有几百或上千字节，而PC机对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，使人非常不易察觉。

1.2.4 潜伏性

大部分的病毒感染系统之后一般不会马上发作，它可长期隐藏在系统中，只有在满足特定条件时才启动其表现（破坏）模块。只有这样它才能进行广泛地传播。如“PETER-2”在每年2月27日会提3个问题，用户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。国内的“上海一号”会在每年3，6，9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。

1.2.5 破坏性

任何病毒只要侵入系统，都会对系统及应用程序产生程度不同的破坏。轻者会降低计算机工作效率，占用系统资源，重者可导致系统崩溃。由此特性可将病毒分为良性病毒与恶性病毒。良性病毒可能只显示些画面或出点音乐、无聊的语句，或者根本没有任何破坏动作，但会占用系统资源。这类病毒较多，如GENP、小球、W-BOOT等。恶性病毒则有明确的目的，或破坏数据、删除文件，或加密磁盘、格式化磁盘，有的对数据造成不可挽回的破坏。这也反映出病毒编制者的险恶用心。

1.2.6 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。不同种类的病毒，它们的代码千差万别，但有些操作是共有的（如驻内存，改中断）。有些人利用病毒的这种共性，制作了声称可查所有病毒的程序。这种程序的确可查出一些病毒，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。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地提高，病毒对反病毒软件常常是超前的。

1.3 计算机病毒的分类

从第一个计算机病毒出世以来，究竟世界上有多少种计算机病毒，说法不一。无论多少种，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，另据我国公安部统计，国内以每月4～6种的速度递增。

根据计算机病毒的特点，它的分类方法有许多种。因此，同一种病毒可能有多种不同的分法，也就是说，同一种病毒有可能同属于几种不同的类别。

1.5.1 [illegible]

按照计算机病毒攻击的系统不同，可把它分为以下几类。

- **攻击DOS系统的病毒** 这类病毒出现最早、最多，变种也最多，目前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%。
- **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系统正逐渐取代DOS系统，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Windows95/98病毒。
- **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。
- **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，但也是一个不祥之兆。

1.5.2 [illegible]

按照计算机病毒攻击机型的不同，可把它分为以下几类。

- **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。
- **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，也可以作为小的计算机网络的主机。起初，人们认为计算机病毒只有在微型计算机上才能发作而小型机则不会受到病毒的侵扰，但自1988年11月份Internet受到worm程序的攻击后，人们认识到小型机也同样不能免遭计算机病毒的攻击。
- **攻击工作站的计算机病毒** 近几年，计算机工作站有了较大的进展，并且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。

1.5.3 [illegible]

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。按照计算机病毒的链接方式不同，可把它分为以下几类。

- **源码型病毒** 该病毒攻击高级语言编写的程序，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。
- **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。

外壳型病毒　外壳型病毒将其自身包围在主程序的四周，对原来的程序不作修改。这种病毒最为常见，易于编写，也易于发现，一般测试文件的大小即可查出该种病毒。

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，具有很强的破坏性，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的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方式等，对操作系统进行破坏。

1.3.4 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把它分为 2 类：

良性计算机病毒　是指不包含有立即对计算机系统产生直接破坏作用的代码的计算机病毒。这类病毒为了表现其存在，只是不停地进行传播，并不破坏计算机内的数据。有些人对这类计算机病毒的传染不以为然，认为这只是恶作剧，没什么关系。其实良性、恶性都是相对而言的。良性病毒取得系统控制权后，会导致整个系统运行效率降低，系统可用内存总数减少，使某些应用程序不能运行。它还与操作系统和应用程序争抢 CPU 的控制权，时时导致整个系统死锁，给正常操作带来麻烦。有时系统内还会出现几种病毒交叉感染的现象，一个文件不停地反复被几种病毒所感染。例如原来只有10kB的文件变成90kB，就是被几种病毒反复感染了数十次。这不仅消耗掉大量宝贵的磁盘存储空间，而且整个计算机系统也由于多种病毒寄生于其中而无法正常工作。因此也不能轻视良性病毒对计算机系统造成的破坏。

恶性计算机病毒　指在代码中包含有损伤和破坏计算机系统操作，在其传染或发作时会对系统产生直接的破坏作用的计算机病毒。这类病毒很多，如米开朗基罗病毒。当米氏病毒发作时，硬盘的前 17 个扇区将被彻底破坏，使整个硬盘上的数据无法恢复，造成的损失是无法挽回的。有的病毒还会对硬盘做格式化等破坏。这些操作代码都是刻意编写进病毒的，这是其本性之一。因此这类恶性病毒是很危险的，应当注意防范。所幸防病毒系统可以通过监控系统内的这类异常动作识别出计算机病毒的存在与否，或至少发出警报提醒用户注意。

1.3.5 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把它分为定时计算机病毒和随机计算机病毒。定时病毒仅在某一特定时间才发作，而随机病毒一般不是由时钟来激活的。

1.3.6 按照传播媒介分类

按照计算机病毒的传播媒介来分类，可分为单机计算机病毒和网络计算机病毒。

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，然后再传染其他软盘，软盘又传染其他系统。

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，这种病毒的传染能力更强，破坏力更大。

1.3.7 按照寄生方式和传染途径分类

人们习惯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2类，一是引导型病毒，二是文件型病毒。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还可细分。

混合型病毒集引导型和文件型病毒特性于一体。引导型病毒会去改写（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。或者改写硬盘上的分区表（FAT）。如果用已感染病毒的软盘来启动，就会感染硬盘。

引导型病毒

引导型病毒是一种在ROM BIOS之后，系统引导时出现的病毒，它先于操作系统，依托的环境是BIOS中断服务程序。引导型病毒是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行，而病毒已经隐藏在系统中伺机传染、发作。

引导型病毒按其寄生对象的不同又可分为2类，即MBR（主引导区）病毒和BR（引导区）病毒。MBR病毒又称为分区病毒，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面0道第1个扇区）。典型的病毒有Brain，小球病毒等。

文件型病毒

文件型病毒主要以感染文件扩展名为.COM,.EXE和.OVL等可执行程序为主。它的安装必须借助于病毒的载体程序，即要运行病毒的载体程序，方能把文件型病毒引入内存。已感染病毒的文件执行速度会减缓，甚至完全无法执行。有些文件被感染后，一执行就会被删除。大多数的文件型病毒都会把它们自己的程序码复制到其宿主的开头或结尾处。这会造成已感染病毒文件的长度变长，但用户不一定能用DIR命令列出文件感染病毒前的长度。也有部分病毒是直接改写“受害文件”的程序码，因此感染病毒后文件的长度仍然保持不变。感染病毒的文件被执行后，病毒通常会趁机再对下一个文件进行感染。高明一点的病毒，会在每次进行感染的时候，针对其新宿主的状况而编写新的病毒码，然后才进行感染，因此，这种病毒没有固定的病毒码。以扫描病毒码的方式来检测病毒的查毒软件，遇上这种病毒就一点用没有了。但反病毒软件随着病毒技术的发展而发展，针对这种病毒

现在也有了有效手段。

大多数文件型病毒都是常驻在内存中的。文件型病毒分为源码型病毒、嵌入型病毒和外壳型病毒。源码型病毒是用高级语言编写的，若不进行汇编、链接则无法传染扩散。嵌入型病毒是嵌入在程序的中间，它只能针对某个具体程序，如dBASE病毒。这2类病毒受环境限制尚不多见。目前流行的文件型病毒几乎都是外壳型病毒，这类病毒寄生在宿主程序的前面或后面，并修改程序的第一个执行指令，使病毒先于宿主程序执行，这样随着宿主程序的使用而传染扩散。

文件外壳型病毒按其驻留内存方式可分为高端驻留型、常规驻留型、内存控制链驻留型、设备程序补丁驻留型和不驻留内存型。

混合型病毒综合系统型和文件型病毒的特性，它的“性情”比系统型和文件型病毒更为“凶残”。此种病毒通过这2种方式来感染，更增加了病毒的传染性以及存活率。不管以哪种方式传染，只要中毒就会经开机或执行程序而感染其他的磁盘或文件，此种病毒是很难杀灭的。

引导型病毒相对文件型病毒来讲，破坏性较大，但为数较少，直到20世纪90年代中期，文件型病毒还是最流行的病毒。

随着微软公司Word字处理软件的广泛使用和计算机网络尤其是Internet的推广普及，病毒家族又出现一种新成员，这就是宏病毒。据美国国家计算机安全协会统计，宏病毒已占目前全部病毒数量的80%以上。另外，宏病毒还可衍生出各种变形变种病毒，这种“父生子子生孙”的传播方式实在让许多系统防不胜防，这也使宏病毒成为威胁计算机系统的“第一杀手”。宏病毒是一种寄存于文档或模板的宏中的计算机病毒。一旦打开这样的文档，宏病毒就会被激活，转移到计算机上，并驻留在Normal模板上，从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

1.4 计算机病毒的检测方法

在与病毒的对抗中，及早发现病毒很重要。早发现，早处置，可以减少损失。检测病毒方法有：特征代码法、校验和法、行为监测法、软件模拟法。这些方法依据的原理不同，实现时所需费用不同，检测范围不同，因此各有所长。

1.4.1 特征代码法

特征代码法早期应用于SCAN，CPAV等著名病毒检测工具中。国外专家认为特征代码法是检测已知病毒的最简单、开销最小的方法。

特征代码法的实现步骤如下：

- **采集已知病毒样本，病毒如果既感染.COM文件又感染.EXE文件，对这种病毒要同时采集.COM型病毒样本和.EXE型病毒样本。**

此为试读，需要完整PDF请访问：www.ertongbook.com