

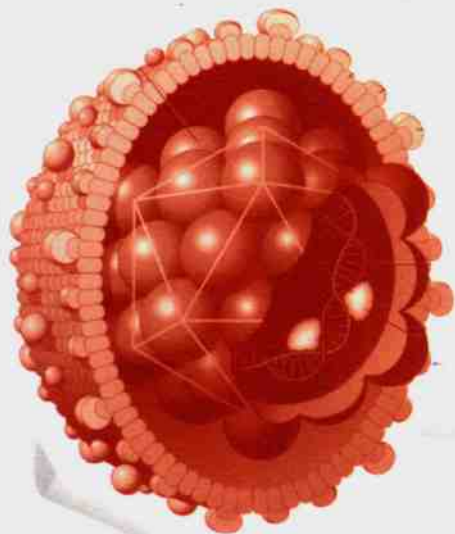
Broadview[®]
www.broadview.com.cn

信息安全领域多年经验的总结和提炼!

安全技术
大系

计算机病毒 分析与防范大全

韩筱卿 王建锋 钟 玮 等编著



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

安全技术
大系

计算机病毒 分析与防范大全

韩筱卿 王建锋 钟 玮 等编著

内 容 简 介

本书是作者在信息安全领域多年经验的总结和提炼。本书从计算机病毒的定义及特征开始,将目前发现的所有计算机病毒加以分类,总结出每一类病毒的共性和特征,提出具有针对性的防范建议,以便普通读者揭开病毒的神秘面纱,构建自己的防范体系。

本书适合计算机安全领域的从业者及爱好者阅读,对计算机普通用户更深入地了解计算机病毒也有莫大的帮助。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

计算机病毒分析与防范大全 / 韩筱卿, 王建锋, 钟玮等编著. —北京: 电子工业出版社, 2006.3

(安全技术大系)

ISBN 7-121-02157-9

I. 计… II. ①韩… ②王… ③钟… III. 计算机病毒—防治 IV. TP309.5

中国版本图书馆 CIP 数据核字 (2005) 第 152779 号

责任编辑: 朱沐红 zsh@phei.com.cn

印 刷: 北京智力达印刷有限公司

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

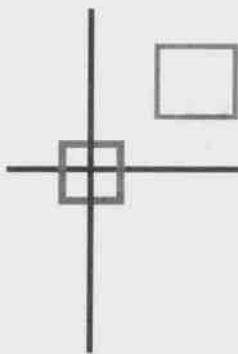
经 销: 各地新华书店

开 本: 787×980 1/16 印张: 32 字数: 800 千字

印 次: 2006 年 3 月第 1 次印刷

印 数: 4000 册 定价: 59.00 元 (含光盘 1 张)

凡购买电子工业出版社的图书,如有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系。
联系电话: (010) 68279077。质量投诉请发邮件至 zlts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。



作者简介



韩筱卿，1971年生，现任北京瑞星公司客户服务总经理。从1995年开始涉足计算机反病毒技术研究领域；1997年，参与开发的瑞星杀毒软件第一代产品获中国国家科委（现科技部）国家科技成果奖；参与了CIH病毒、BO黑客、红色代码、尼姆达、Happy Time等多种典型流行病毒的解决处理过程。2000年组织筹备成立了瑞星数据修复中心，经过多年的发展，使之成为计算机用户数据灾难恢复的首选之地。先后在清华大学、北京大学、北京理工大学、北京航空航天大学、上海同济大学、四川科技大学等多所高校做关于计算机反病毒技术的专题报告。



王建锋，1971年生，现任北京瑞星公司客户服务副总经理。多年来一直从事反病毒技术研究及技术支持工作。2000年以来，主要负责重大恶性计算机病毒的应急处理工作，组织并参与创建瑞星客户服务中心呼叫中心系统及计算机病毒应急处理平台，在新型病毒预警、分析以及反病毒策略研究等领域具有丰富的经验。



钟玮，1976年生，现任北京瑞星公司数据安全部经理，全面负责信息安全增值服务的管理与拓展工作。2002年以来，参与国务院新闻办、港澳办、中组部、华远集团等国内20余家政府部门及大型企业信息安全整体解决方案及安全外包方案的制定与实施；为中粮集团、中央电视台、微软公司、国务院中直管理局、联合国驻京机构等30余家重点单位长期提供数据安全、数据恢复咨询及数据安全项目；多次组织并参与信息产业部电子教育中心、清华大学、中科院计算所等国内权威机构信息安全培训项目的实施，具有丰富的信息安全项目实践经验。





序

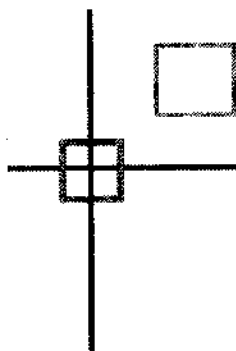
计算机病毒是一个社会性的问题，仅靠信息安全厂商研发的安全产品而没有全社会的配合，是无法有效地建立信息安全体系的。因此，面向全社会普及计算机病毒的基础知识，增强大家的病毒防范意识，“全民皆兵”并配合适当的反病毒工具，才能真正地做到防患于未然。我们很高兴地看到战斗在反病毒领域第一线专业人士，将自己多年的反病毒经验加以总结，与大家共享，帮助普通的计算机使用者揭开计算机病毒的神秘面纱，这无疑是一件有利于促进信息化发展的事情。

这本书实用性比较强，较为全面地介绍了计算机病毒的基本知识，分析了典型病毒的特征，很适合初中级水平的计算机使用者参考。希望这本书的发行，能够在普及计算机防病毒知识方面发挥积极的作用，并根据实际情况不断更新，将最新的技术和发展趋势带给广大的读者。

瑞星公司董事长

王莘

2005年11月于北京



写在前面



提起计算机病毒，绝大多数计算机的使用者都会深恶痛绝，因为没有“中过招”的人已经是凤毛麟角了。但在谈虎色变之余，很多人对计算机病毒又充满了好奇，对病毒的制造者既痛恨又敬畏。这种复杂的感情实际上很容易理解，就像古人面对大自然的感情一样，因为无法解释风雨雷电，也就只能制造神话，崇拜图腾了。

计算机病毒当然不值得崇拜，它给社会信息化的发展制造了太多的麻烦，每年因为计算机病毒造成的直接、间接经济损失都超过百亿美元。但同时，它也催化了一个新兴的产业——信息安全产业。反病毒软件、防火墙、入侵检测系统、网络隔离、数据恢复技术……这一根根救命稻草，使很多企业和个人用户免遭侵害，在很大程度上缓解了计算机病毒造成的巨大破坏，同时，越来越多的企业加入到信息安全领域，同层出不穷的黑客和病毒制造者做着顽强的斗争。

但稻草毕竟是稻草，救得一时不一定救得一世。目前市场上主流厂商的信息安全产品经过多年的积累和精心的研发，无论从产品线还是从技术角度来讲，都已经达到了相当完善的程度。但是，再好的产品，如果不懂得如何去使用，发挥不了产品真正的优势，又与稻草有什么区别呢？很多用户在被病毒感染以后才想起购买杀毒软件，查杀以后就再也不管，没有定期的升级和维护，更没有根据自己的使用环境的特点，制定相应的防范策略，可以说把产品的使用效率降到了最低，这样的状态，怎能应付日新月异的病毒攻击呢？

那么，如何将手中的稻草变成强大的武器，当危险临近时，能够主动出击，防患于未然呢？笔者认为，关键的问题在于对“对手”的了解。正如我们上面举过的例子，我们现在之所以对

很多自然现象习以为常，是因为我们对其成因有了最基础的了解，这样才可能未雨绸缪，配合手中的工具，防患于未然。

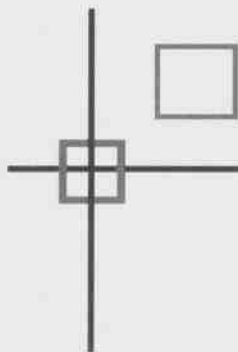
本书的创作初衷正是将笔者在信息安全领域多年的经验加以总结、提炼，从计算机病毒的定义及特征开始讲起，将病毒的起源、发展历史、发展趋势及造成的危害系统而全面地介绍给读者，并将目前发现的所有计算机病毒加以分类，总结出每一类病毒的共性和特征，提出具有针对性的防范建议，以便于普通读者揭开病毒的神秘面纱，构建自己的防范体系。同时，本书还根据杀毒软件行业的特点，以专业的视角介绍了反病毒行业病毒分析的流程，帮助读者构建自己的病毒分析实验室，从而对计算机病毒进行彻底的剖析。此外，为了更好地将书中提到的知识和技能运用到实践中，我们还特别地为初学者设计了非常实用的小实验，并对实验过程进行了必要的演示，以帮助大家更好地理解计算机病毒的原理。

魔高一尺，道高一丈。我们相信，只要知己知彼，我们一定会在与计算机病毒进行的这场持久战中取得最终的胜利！

读者交流信箱：AntiVR@hotmail.com

作 者

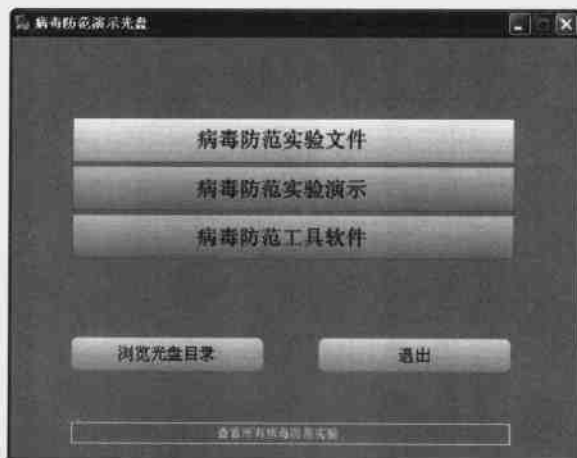
2005年12月8日



病毒防范实验演示说明

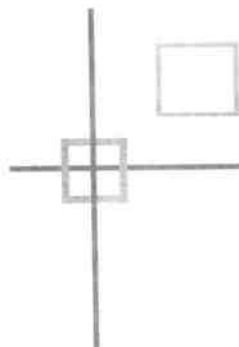


为了使广大读者更好地理解本书的内容，了解计算机病毒的感染和发作原理，作者特意准备了几比较实用的小实验，并录制了实验内容和实验步骤，供读者参考（见光盘）。



由于实验中有部分代码具有一定的危险性，为了避免初学者操作失误，故将代码部分隐去，详细实验步骤和实验效果请见病毒防范演示中的相应内容。

读者在观看演示过程中，单击“”按钮播放录像，单击“”按钮暂停播放，再次单击“”键时继续播放，单击“”按钮或按键盘“ESC”键停止播放，并退出演示屏幕。单击“定位”菜单可以看到录像的每一帧画面。



目 录



第一篇 认识计算机病毒

第1章 什么是计算机病毒.....2	1.6 计算机病毒的命名.....17
1.1 计算机病毒的定义.....2	1.7 计算机病毒的生命周期.....18
1.2 计算机病毒的特征.....3	1.8 计算机病毒的传播.....19
1.3 计算机病毒的结构.....8	1.9 计算机病毒的预防与清除.....19
1.3.1 计算机病毒的程序结构.....8	第2章 计算机病毒发展史.....21
1.3.2 计算机病毒的存储结构.....8	2.1 计算机病毒的起源.....21
1.4 计算机病毒的分类.....10	2.1.1 病毒的发展过程.....21
1.4.1 根据寄生的数据存储方式划分.....11	2.1.2 当前流行的蠕虫病毒的发展.....25
1.4.2 根据感染文件类型划分.....12	2.2 计算机病毒的发展阶段.....27
1.4.3 根据病毒攻击的操作系统划分.....12	2.2.1 根据病毒的特点划分.....27
1.4.4 根据病毒攻击的计算机类型划分.....13	2.2.2 根据病毒的技术性划分.....29
1.4.5 根据病毒的链接方式划分.....13	2.3 计算机病毒大事记.....31
1.4.6 根据病毒的破坏情况划分.....14	2.4 计算机病毒的发展趋势.....38
1.4.7 根据传播途径分类.....14	2.4.1 智能化.....38
1.4.8 根据运行的连续性分类.....15	2.4.2 人性化.....38
1.4.9 根据激发机制划分.....15	2.4.3 隐蔽化.....39
1.4.10 根据病毒自身变化性分类.....15	2.4.4 多样化.....39
1.4.11 根据与被感染对象的关系分类.....15	2.4.5 专用病毒生成工具的出现.....39
1.4.12 其他几种具有代表性的病毒类型.....16	2.4.6 攻击反病毒软件.....39
1.5 计算机病毒的入侵方式.....17	第3章 计算机病毒的危害.....40
	3.1 计算机病毒编制者的目的.....40

3.1.1 恶作剧（开玩笑）	40	3.2.7 计算机病毒给用户造成严重的心理压力	45
3.1.2 报复心理	41	3.3 计算机病毒发作症状	45
3.1.3 保护版权	42	3.4 计算机故障与病毒现象的区分	47
3.1.4 娱乐需要	42	3.4.1 计算机病毒的现象	47
3.1.5 政治或军事目的	42	3.4.2 与病毒现象类似的硬件故障	48
3.2 计算机病毒对计算机应用的影响	43	3.4.3 与病毒现象类似的软件故障	49
3.2.1 破坏数据	43	3.5 计算机病毒造成的经济损失	49
3.2.2 占用磁盘存储空间	43	3.6 计算机病毒在军事上的影响	53
3.2.3 抢占系统资源	44	3.6.1 直面军事信息安全的挑战	53
3.2.4 影响计算机运行速度	44	3.6.2 高度依赖信息系统的美军青睐计算机病毒武器	54
3.2.5 计算机病毒错误与不可预见的危害	44	3.6.3 防患未然要从细节做起	55
3.2.6 计算机病毒的兼容性对系统运行的影响	44	3.7 计算机病毒的预防	56

第二篇 计算机病毒分析

第4章 追根溯源——传统计算机

病毒概述	58
4.1 早期的DOS病毒介绍	58
4.1.1 DOS操作系统简介	58
4.1.2 DOS病毒	58
4.2 Office杀手——宏病毒	59
4.2.1 什么是“宏”	59
4.2.2 宏病毒的定义	60
4.2.3 宏病毒的特点	61
4.2.4 宏病毒的发作现象及处理	61
4.2.5 典型的宏病毒——“七月杀手”病毒	63
4.2.6 防范宏病毒的安全建议	64
4.3 变化多端的文件型病毒	65
4.3.1 文件型病毒的复制机制	65
4.3.2 文件型病毒的分类	66
4.3.3 文件型病毒的发展史	66
4.3.4 文件型病毒简介	68

4.3.5 典型的文件型病毒——WIN95.CIH病毒解剖	71
4.4 攻击磁盘扇区的引导型病毒	75
4.4.1 引导型病毒背景介绍	75
4.4.2 引导型病毒的主要特点和分类	77
4.4.3 引导型病毒的发作现象及处理	78
4.4.4 典型的引导型病毒——WYX病毒解析	80
4.4.5 防范引导区病毒的安全建议	84

第5章 互联网时代的瘟疫——蠕虫病毒

5.1 背景介绍	85
5.1.1 蠕虫病毒的起源	86
5.1.2 蠕虫病毒与普通病毒的比较	87
5.1.3 蠕虫病毒造成的破坏	87
5.1.4 蠕虫病毒的特点和发展趋势	87
5.1.5 蠕虫病毒的传播	88
5.2 病毒的特点及危害	88
5.2.1 蠕虫病毒的特点	88

5.2.2 蠕虫病毒造成的社会危害.....91	7.4.1 HAPPYTIME 病毒分析.....130
5.3 蠕虫病毒的发作现象及处理方法.....92	7.4.2 情人谷恶意网页分析.....133
5.3.1 尼姆达 (Nimda) 病毒.....93	7.5 防范脚本病毒的安全建议.....136
5.3.2 W32.Sircam 病毒.....96	7.6 脚本及恶意网页实验.....138
5.3.3 SCO 炸弹 (Worm.Novarg).....97	7.6.1 实验目的.....138
5.3.4 恶性蠕虫病毒	7.6.2 实验内容.....138
“斯文 (Worm.Swen)”.....98	7.6.3 实验用工具软件及操作系统.....138
5.4 典型蠕虫病毒 Worm.Japanize 解析.....99	7.6.4 实验背景知识及说明.....138
5.4.1 Worm.Japanize 病毒解析.....99	7.6.5 实验流程.....144
5.5 防范蠕虫病毒的安全建议.....106	7.7 注册表维护实验.....146
5.6 蠕虫病毒防范实验.....108	7.7.1 实验目的.....146
5.6.1 实验目的.....108	7.7.2 实验内容.....146
5.6.2 实验大纲.....108	7.7.3 实验工具软件.....146
5.6.3 实验工具软件.....108	7.7.4 实验步骤.....146
5.6.4 实验内容.....109	7.7.5 实验流程.....155
5.6.5 实验步骤.....111	
第6章 隐藏的危机——木马病毒分析.....112	第8章 不要和陌生人说话——即时通讯病毒分析.....157
6.1 木马病毒的背景介绍.....112	8.1 即时通讯病毒背景介绍.....157
6.2 木马病毒的隐藏性.....113	8.1.1 什么是 IM.....157
6.3 典型的木马病毒——冰河病毒	8.1.2 主流即时通讯软件简介.....157
解析.....118	8.1.3 IM 软件的基本工作原理.....159
6.3.1 冰河病毒简介 (v8.2).....118	8.2 即时通讯病毒的特点及危害.....160
6.4 防范木马病毒的安全建议.....120	8.3 即时通讯病毒发作现象及
	处理方法.....162
第7章 网页冲浪的暗流——网页脚本病毒分析.....122	8.4 典型的即时通讯病毒——“MSN
7.1 脚本病毒的背景知识介绍.....122	性感鸡”解析.....165
7.1.1 VBScript 概述.....122	8.5 防范即时通讯病毒的安全建议.....167
7.1.2 “WSH”概述.....123	
7.1.3 有关注册表的基本知识.....123	第9章 无孔不入——操作系统漏洞攻击病毒分析.....168
7.2 脚本病毒的特点.....124	9.1 漏洞攻击病毒背景介绍.....168
7.3 脚本病毒的发作现象及处理.....125	9.2 漏洞攻击病毒造成的危害.....169
7.4 典型脚本病毒——欢乐时光	9.2.1 冲击波病毒造成的危害.....169
病毒解析.....130	9.2.2 震荡波病毒造成的危害.....170

9.2.3 严防微软 MS05-040 漏洞.....	170
9.3 漏洞攻击病毒发作现象及处理	171
9.3.1 红色代码发作现象.....	171
9.3.2 冲击波病毒的发作现象.....	172
9.3.3 震荡波病毒发作现象.....	176
9.4 防范漏洞攻击病毒的安全建议	178
第 10 章 病毒发展的新阶段——移动 通讯病毒分析	180
10.1 移动通讯病毒背景介绍	180
10.2 移动通讯病毒的特点.....	182
10.2.1 手机病毒的传播途径.....	182
10.2.2 手机病毒的传播特点.....	184
10.3 移动通讯病毒的发作现象	184
10.4 防范移动通讯病毒的安全建议	185
第 11 章 防人之心不可无——网络 钓鱼概述	187
11.1 网络钓鱼背景介绍	187
11.2 网络钓鱼的手段及危害.....	188
11.2.1 利用电子邮件“钓鱼”	188
11.2.2 利用木马程序“钓鱼”	188
11.2.3 利用虚假网址“钓鱼”	189
11.2.4 假冒知名网站钓鱼.....	189

11.2.5 其他钓鱼方式	190
11.3 防范网络钓鱼的安全建议	190
11.3.1 金融机构采取的网上安全 防范措施	190
11.3.2 对于个人用户的安全建议	191
第 12 章 强买强卖——流氓软件概述	192
12.1 流氓软件背景介绍	192
12.2 流氓软件的分类及其流氓行径	193
12.3 流氓软件的危害	194
12.4 防范流氓软件的安全建议	195
12.4.1 IE 插件管理专家 Upiea	195
12.4.2 超级兔子魔法设置	196
12.4.3 瑞星卡卡安全助手	196
12.4.4 微软反间谍软件 (Microsoft Antispyware)	197
第 13 章 其他操作系统病毒	198
13.1 操作系统概述	198
13.1.1 Linux 操作系统	198
13.1.2 苹果公司的 MAC OS	199
13.2 Linux 与 Unix 病毒	200
13.3 MAC OS 系统病毒	201
13.4 其他新型病毒简介	201

第三篇 反病毒技术

第 14 章 反病毒技术发展趋势	204
14.1 反病毒保护措施日益全面和 实时	204
14.2 反病毒产品体系结构面临突破	205
14.3 对未知病毒的防范能力日益增强	205
14.4 企业级别、网关级别的产品 越来越重要	206
14.5 关注移动设备和无线产品的安全	206

第 15 章 基础知识——常见文件格式	207
15.1 病毒与文件格式	207
15.1.1 常见的文件格式	207
15.1.2 文档能够打开但无法正常 显示时采取的措施	215
15.1.3 文档打不开时采取的措施	216
15.1.4 常见的文件后缀	217
15.1.5 双扩展名——病毒邮件所带 附件的特点之一	223

15.2 PE 文件格式.....	224	17.1.1 自动脱壳.....	317
15.2.1 PE 文件格式一览.....	224	17.1.2 手动脱壳.....	326
15.2.2 检验 PE 文件的有效性.....	225	17.1.3 脱壳技巧.....	329
15.2.3 File Header.....	226	17.2 邮件蠕虫.....	337
15.2.4 OptionalHeader.....	227	17.2.1 邮件蠕虫的局限与解决方法.....	337
15.2.5 Section Table.....	228	17.2.2 垃圾邮件的关键技术.....	340
15.2.6 Import Table (引入表).....	229	17.3 追踪邮件来源.....	342
15.2.7 Export Table (引出表).....	231	17.3.1 邮件头分析.....	342
第 16 章 搭建病毒分析实验室.....	233	17.3.2 邮件传输过程.....	343
16.1 神奇的虚拟机.....	233	17.3.3 邮件头分析实例.....	344
16.1.1 硬件要求与运行环境.....	233	17.3.4 邮件伪造.....	346
16.1.2 VMware.....	234	17.3.5 垃圾邮件分析.....	346
16.1.3 Virtual PC.....	238	17.3.6 总结.....	348
16.1.4 VMWare 与 Virtual PC 的 主要区别.....	243	17.4 病毒分析常用工具实验.....	349
16.1.5 病毒“蜜罐”.....	244	17.4.1 实验目的.....	349
16.2 常用病毒分析软件.....	245	17.4.2 实验内容.....	349
16.2.1 系统监测工具.....	245	17.4.3 实验工具.....	349
16.2.2 文本编辑器.....	266	17.4.4 实验步骤.....	350
16.2.3 综合软件.....	273	17.4.5 实验流程.....	355
16.3 静态分析技术.....	282	第 18 章 捕捉计算机病毒.....	357
16.3.1 基础知识.....	282	18.1 计算机病毒的症状.....	357
16.3.2 W32Dasm 简介.....	283	18.1.1 计算机病毒发作前的 表现现象.....	357
16.3.3 IDA Pro.....	291	18.1.2 计算机病毒发作时的 表现现象.....	359
16.3.4 破解教程.....	294	18.1.3 计算机病毒发作后的 表现现象.....	361
16.4 动态分析技术.....	296	18.2 Windows 的自启动方式.....	362
16.4.1 SoftICE 和 TRW2000 的 安装与配置.....	296	18.2.1 自启动目录.....	362
16.4.2 SoftICE 与 TRW2000 操作入门.....	306	18.2.2 系统配置文件启动.....	363
16.4.3 常用的 Win32 API 函数.....	312	18.2.3 注册表启动.....	366
16.4.4 破解实例.....	314	18.2.4 其他启动方式.....	368
第 17 章 计算机病毒惯用技术解密.....	317	18.2.5 自启动方式.....	370
17.1 压缩与脱壳.....	317	18.3 名词解释.....	372

18.3.1 恶意软件	372	19.4 “莫国防”病毒 (win32.mgf) 的 源程序	422
18.3.2 恶意软件类别详述	373	19.5.1 相关技术	422
18.3.3 恶意软件的特征	374	19.5.2 危害估计	422
18.3.4 携带者对象	374	19.5.3 源代码	422
18.3.5 传输机制	375		
18.3.6 负载	376	第 20 章 反病毒技术剖析	449
18.3.7 触发机制	378	20.1 病毒诊治技术剖析	449
18.3.8 防护机制	378	20.1.1 反病毒技术概述	449
第 19 章 典型病毒的源代码分析	380	20.1.2 病毒诊断技术	450
19.1 Funlove 的源代码	380	20.1.3 虚拟机在反病毒技术中 的应用	455
19.2 2003 蠕虫王 (SQL Server 蠕虫)	406	20.2 反病毒引擎技术剖析	458
19.3 冲击波 (MSBlast) 蠕虫	408	20.2.1 反病毒引擎在整个杀毒软件 中的地位	458
19.3.1 蠕虫脱壳	408	20.2.2 反病毒引擎的发展历程	459
19.3.2 蠕虫浅析	408	20.2.3 反病毒引擎的体系架构	460
19.3.3 开始跟踪	411	20.2.4 反病毒引擎的技术特征	460
19.3.4 深入分析	412	20.2.5 反病毒引擎的发展方向	463
19.4 “震荡波” (Worm.Sasser) 病毒 代码	416		

第四篇 反病毒产品及解决方案

第 21 章 中国反病毒产业发展概述	466	23.1.1 法律	478
第 22 章 主流反病毒产品特点介绍	470	23.1.2 思想意识	480
22.1 瑞星杀毒软件	470	23.1.3 技术手段	480
22.2 KV 杀毒软件	472	23.1.4 管理手段	481
22.3 金山毒霸	473	23.1.5 技能手段	482
22.4 诺顿杀毒软件	474	23.2 如何选择反病毒产品	483
22.5 趋势杀毒软件	475	23.2.1 使用方面	483
22.6 熊猫卫士	476	23.2.2 服务方面	483
22.7 卡巴斯基杀毒软件	476	附录 A 计算机安全法规	484
22.8 安博士杀毒软件	477	附录 B 新病毒处理流程	495
第 23 章 反病毒安全体系的建立	478		
23.1 建设安全体系遵循的原则	478		

PART

One

第一篇

认识计算机病毒

第 1 章 什么是计算机病毒

第 2 章 计算机病毒发展史

第 3 章 计算机病毒的危害

第 1 章 什么是计算机病毒

1.1 计算机病毒的定义

我们知道,生物界的“病毒”(Virus)是一种没有细胞结构、只有由蛋白质的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、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看得到,而且不能独立生存,必须寄生在其他生物的活细胞里才能生存。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。

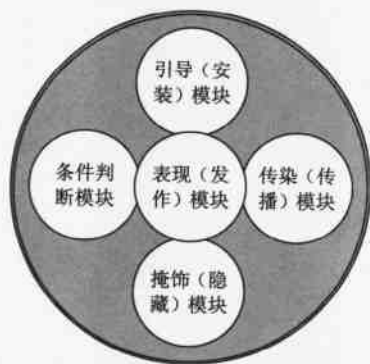


图 1-1 计算机病毒的结构

我们通常所说的“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学上的病毒有着很多的相同点(如图 1-1 所示)。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。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的普遍观点,我们可以总结出计算机病毒

的十大特征,即非法性、隐蔽性、潜伏性、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,我们将在下一节对计算机病毒的十大特征进行详细论述。

需要指出的是,单独根据以上某一个特征是不能判断某个程序是否是病毒的。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:“指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”。

1.2 计算机病毒的特征

1. 非法性

正常情况下,计算机用户调用执行一个合法程序时,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透明和可知的,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“悄悄地”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。从这种意义上讲,计算机病毒具有“非法性”。

例如我们将在第6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. 隐蔽性

隐蔽性是计算机病毒最基本的特征,正像我们上面讲到的,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蔽性,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。

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,使之非常不易被察觉,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出现;还有一种比较常见的隐藏方式是将病毒文件放在Windows等系统目录下,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。

不同类型的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,在系统启动前就发作。一些蠕虫病毒非常注重隐藏和伪装自己,它们不但伪造邮件的主题和正文,利用