

计算机病毒分析与防范大全



[计算机病毒分析与防范大全_下载链接1](#)

著者:韩筱卿

出版者:电子工业出版社

出版时间:2006-3

装帧:平装

isbn:9787121021572

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。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。

作者介绍:

目录: 第一篇 认识计算机病毒.
第1章 什么是计算机病毒 2
1.1 计算机病毒的定义 2
1.2 计算机病毒的特征 3
1.3 计算机病毒的结构 8

1.3.1 计算机病毒的程序结构	8
1.3.2 计算机病毒的存储结构	8
1.4 计算机病毒的分类	10
1.4.1 根据寄生的数据存储方式划分	11
1.4.2 根据感染文件类型划分	12
1.4.3 根据病毒攻击的操作系统划分	12
1.4.4 根据病毒攻击的计算机类型	
1.4.4 划分	13
1.4.5 根据病毒的链接方式划分	13
1.4.6 根据病毒的破坏情况划分	14
1.4.7 根据传播途径分类	14
1.4.8 根据运行的连续性分类	15
1.4.9 根据激发机制划分	15
1.4.10 根据病毒自身变化性分类	15
1.4.11 根据与被感染对象的关系分类	15
1.4.12 其他几种具有代表性的病毒	
1.4.12 类型	16
1.5 计算机病毒的入侵方式	17..
1.6 计算机病毒的命名	17
1.7 计算机病毒的生命周期	18
1.8 计算机病毒的传播	19
1.9 计算机病毒的预防与清除	19
第2章 计算机病毒发展史	21
2.1 计算机病毒的起源	21
2.1.1 病毒的发展过程	21
2.1.2 当前流行的蠕虫病毒的发展	25
2.2 计算机病毒的发展阶段	27
2.2.1 根据病毒的特点划分	27
2.2.2 根据病毒的技术性划分	29
2.3 计算机病毒大事记	31
2.4 计算机病毒的发展趋势	38
2.4.1 智能化	38
2.4.2 人性化	38
2.4.3 隐蔽化	39
2.4.4 多样化	39
2.4.5 专用病毒生成工具的出现	39
2.4.6 攻击反病毒软件	39
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
3.1.2 报复心理	41
3.1.3 保护版权	42
3.1.4 娱乐需要	42
3.1.5 政治或军事目的	42
3.2 计算机病毒对计算机应用的影响	43
3.2.1 破坏数据	43
3.2.2 占用磁盘存储空间	43
3.2.3 抢占系统资源	44
3.2.4 影响计算机运行速度	44
3.2.5 计算机病毒错误与不可预见	
3.2.5 的危害	44
3.2.6 计算机病毒的兼容性对系统	
3.2.5 运行的影响	44
3.2.7 计算机病毒给用户造成严重	

3.2.7 的心理压力	45
3.3 计算机病毒发作症状	45
3.4 计算机故障与病毒现象的区分	47
3.4.1 计算机病毒的现象	47
3.4.2 与病毒现象类似的硬件故障	48
3.4.3 与病毒现象类似的软件故障	49
3.5 计算机病毒造成的经济损失	49
3.6 计算机病毒在军事上的影响	53
3.6.1 直面军事信息安全的挑战	53
3.6.2 高度依赖信息系统的美军	
3.6.2 青睐计算机病毒武器	54
3.6.3 防患未然要从细节做起	55
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	
第4章 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”	
4.2.5 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	
4.3.5 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	
4.4.4 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	85
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
5.3 蠕虫病毒的发作现象及处理方法	92
5.3.1 尼姆达 (Nimda) 病毒	93
5.3.2 W32.Sircam病毒	96

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

8.4 性感鸡” 解析	165
8.5 防范即时通讯病毒的安全建议	167
第9章 无孔不入——操作系统漏洞	
第9章 漏洞攻击病毒分析	168
9.1 漏洞攻击病毒背景介绍	168
9.2 漏洞攻击病毒造成的危害	169
9.2.1 冲击波病毒造成的危害	169
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	
第10章 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	
第11章 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	
11.3.1 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	
12.4.4 (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
- 14.1 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
- 14.4 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——知识常见文件
- 第15章 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
- 15.1.2 显示时采取的措施 215
- 15.1.3 文档打不开时采取的措施 216
- 5.1.4 常见的文件后缀 217
- 15.1.4 双扩展名——病毒邮件所带
- 15.1.4 附件的特点之一 223
- 15.2 PE文件格式 224
- 15.2.1 PE文件格式一览 224
- 15.2.2 检验PE文件的有效性 225
- 15.2.3 File Header 226
- 15.2.4 OptionalHeader 227
- 15.2.5 Section Table 228
- 15.2.6 Import Table (引入表) 229
- 15.2.7 Export Table (引出表) 231
- 第16章 搭建病毒分析实验室 233
- 16.1 神奇的虚拟机 233
- 16.1.1 硬件要求与运行环境 233
- 16.1.2 VMware 234
- 16.1.3 Virtual PC 238
- 16.1.4 VMWare与Virtual PC的
- 16.1.4 主要区别 243
- 16.1.5 病毒“蜜罐” 244
- 16.2 常用病毒分析软件 245
- 16.2.1 系统监测工具 245
- 16.2.2 文本编辑器 266
- 16.2.3 综合软件 273
- 16.3 静态分析技术 282
- 16.3.2 W32Dasm简介 283
- 16.3.3 IDA Pro 291
- 16.3.4 破解教程 294
- 16.4 动态分析技术 296
- 16.4.1 SoftICE和TRW2000的
- 16.4.1 安装与配制 296
- 16.4.2 SoftICE与TRW2000
- 16.4.1 操作入门 306
- 16.4.3 常用的Win32 API函数 312
- 16.4.4 破解实例 314
- 第17章 计算机病毒惯用技术解密 317
- 17.1 压缩与脱壳 317
- 17.1.1 自动脱壳 317
- 17.1.2 手动脱壳 326
- 17.1.3 脱壳技巧 329
- 17.2 邮件蠕虫 337

- 17.2.1 邮件蠕虫的局限与解决方法 337
- 17.2.2 垃圾邮件的关键技术 340
- 17.3 追踪邮件来源 342
 - 17.3.1 邮件头分析 342
 - 17.3.2 邮件传输过程 343
 - 17.3.3 邮件头分析实例 344
 - 17.3.4 邮件伪造 346
 - 17.3.5 垃圾邮件分析 346
 - 17.3.6 总结 348
- 17.4 病毒分析常用工具实验 349
 - 17.4.1 实验目的 349
 - 17.4.2 实验内容 349
 - 17.4.3 实验工具 349
 - 17.4.4 实验步骤 350
 - 17.4.5 实验步骤 355
- 第18章 捕捉计算机病毒 357
 - 18.1 计算机病毒的症状 357
 - 18.1.1 计算机病毒发作前的表现现象 357
 - 18.1.2 计算机病毒发作时的表现现象 359
 - 18.1.3 计算机病毒发作后的表现现象 361
 - 18.2 Windows的自启动方式 362
 - 18.2.1 自启动目录 362
 - 18.2.2 系统配置文件启动 363
 - 18.2.3 注册表启动 366
 - 18.2.4 其他启动方式 368
 - 18.2.5 自动启动相关 370
 - 18.3 名词解释 372
 - 18.3.1 恶意软件 372
 - 18.3.2 恶意软件类别详述 373
 - 18.3.3 恶意软件的特征 374
 - 18.3.4 携带者对象 374
 - 18.3.5 传输机制 375
 - 18.3.6 负载 376
 - 18.3.7 触发机制 378
 - 18.3.8 防护机制 378
- 第19章 典型病毒的源代码分析 380
 - 19.1 Funlove的源代码 380
 - 19.2 2003蠕虫王 (SQL Server蠕虫) 406
 - 19.3 冲击波 (MSBlast) 蠕虫 408
 - 19.3.1 蠕虫脱壳 408
 - 19.3.2 蠕虫浅析 408
 - 19.3.3 开始跟踪 411
 - 19.3.4 深入分析 412
 - 19.4 “震荡波” (Worm.Sasser) 病毒代码 416
 - 19.4 “莫国防”病毒 (win32.mgf) 的源程序 422
 - 19.5.1 相关技术 422
 - 19.5.2 危害估计 422
 - 19.5.3 源代码 422
- 第20章 反病毒技术剖析 448
 - 20.1 病毒诊治技术剖析 449

20.1.1 反病毒技术概述 449
20.1.2 病毒诊断技术 450
20.1.3 虚拟机在反病毒技术中
20.1.3 的应用 455
20.2 反病毒引擎技术剖析 458
20.2.1 反病毒引擎在整个杀毒软件
20.2.1 中的地位 458
20.2.2 反病毒引擎的发展历程 459
20.2.3 反病毒引擎的体系架构 460
20.2.4 反病毒引擎的技术特征 460
20.2.5 反病毒引擎的发展方向 463
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
第22章 主流反病毒产品特点介绍 470
22.1 瑞星杀毒软件 470
22.2 KV杀毒软件 472
22.3 金山毒霸 473
22.4 诺顿杀毒软件 474
22.5 趋势杀毒软件 475
22.6 熊猫卫士 476
22.7 卡巴斯基杀毒软件 476
22.8 安博士杀毒软件 477
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
23.1.1 法律 478
23.1.2 思想意识 480
23.1.3 技术手段 480
23.1.4 管理手段 481
23.1.5 技能手段 482
23.2 如何选择反病毒产品 483
23.2.1 使用方面 483
23.2.2 服务方面 483
附录A 计算机安全法规 484
附录B 反病毒公司紧急病毒处理流程 495
· · · · · (收起)

[计算机病毒分析与防范大全_下载链接1](#)

标签

计算机

病毒

编程

评论

汇编与反汇编

Rising's AD

[计算机病毒分析与防范大全_下载链接1](#)

书评

[计算机病毒分析与防范大全_下载链接1](#)