

计算机用户手册丛书(一)



著：梅筱琴
蒲韵
廖凯生

计算机病毒防治 与网络安全手册



海洋出版社

计算机用户手册丛书（一）

著：梅筱琴
蒲韵
廖凯生

计算机病毒防治 与网络安全手册



海洋出版社

计算机病毒防治

与网络安全手册

编著：梅筱琴
蒲 韵
廖凯生



海洋出版社

2001·北京

235310/04

内 容 提 要

本书比较全面地介绍了计算机病毒的防治方法和计算机安全保障技术。在计算机病毒防治方面,介绍了计算机病毒的基本常识和病毒的机理,以及防治计算机病毒的方法和典型计算机病毒的预防技术;在网络安全方面,介绍了计算机软件的安全和数据加密技术,以及保障计算机网站和计算机网络通讯安全的技术。

本书对计算机病毒和网络安全的理论和概念表述清楚、准确,语言表达流畅,图文并茂,易学易用,是一本防治计算机病毒和保障计算机安全的实用教程。

图书在版编目(CIP)数据

计算机病毒防治与网络安全手册 / 梅筱琴编著. — 北京:
海洋出版社, 2001.6
ISBN 7-5027-5290-0

I. 计… II. 梅… III. ①计算机病毒—防治—手册
②计算机网络—安全技术—手册 IV. TP309.5-62

中国版本图书馆 CIP 数据核字 (2001) 第 032679 号

责任编辑:冯 磊

责任印制:刘志恒

<http://www.chinaoceanpress.com>

海洋出版社 出版发行

(100081 北京市海淀区大慧寺路 8 号)

北京蓝空印刷厂印刷 新华书店经销

2001 年 6 月第 1 版 2001 年 6 月北京第 1 次印刷

开本: 850mm × 1168mm 1/48 印张: 11.5

字数: 450 千字 印数: 1~10000 册

定价: 16.00 元

海洋版图书印、装错误可随时退换



本书作者根据长期对计算机安全的研究和对计算机病毒的防治经验，基于对当前国内外计算机病毒尤其是计算机网络安全技术发展现状的深刻了解，为了满足广大用户对防治计算机病毒和保障计算机安全的迫切要求编写了这本实用技术教程。

全书共分9章。

第1章介绍了计算机病毒的基础知识，使读者了解什么是计算机病毒、计算机病毒的来源、计算机病毒的特征、传播途径和危害等基本知识。

第2章介绍了计算机病毒的机理及发展趋势，使读者了解计算机病毒的结构、作用机理和发展趋势。

第3章介绍了计算机病毒的防治方法，读者通过学习将了解计算机病毒的防治原理和方法，掌握反计算机病毒的实用技术。

第4章介绍了常用计算机防治病毒软件的使用技术，使读者能够掌握这些反病毒软件的使用方法，尤其是懂得如何保护自己的计算机不受病毒的侵害，提高反病毒的能力。



第5章介绍了几种典型计算机病毒的预防方法,通过对典型计算机病毒的分析认识,读者可以进一步掌握预防计算机病毒的方法。

第6章介绍了计算机安全和访问控制的基本方法,引导读者从更高层次上认识计算机的安全问题,了解计算机安全的级别,掌握计算机访问控制的原理。

第7章介绍了保障计算机软件安全的技术,使读者掌握软件加密技术、动态跟踪与反跟踪技术和保障操作系统安全的技术等等。

第8章介绍了数据加密技术,读者通过学习将掌握数据加密技术及其应用。

第9章介绍了因特网网络站点的安全保障方法,向读者提供了最新的因特网安全保障技术,尤其是对付黑客的技术。

本书附录列出了与计算机安全相关的网络资源,为读者进一步查询计算机安全知识和技术提供了方便。

本书编者是长期从事计算机基础教学的教师,具有丰富的教学实践经验。本书凝聚了编者多年来的教学经验和成果,注重计算机技术的实用性和可操作性,着重培养学生的动手能力,本书深入浅出、通俗易懂、图文并茂,把相对复杂的计算机操作技术,简明扼要、生动有趣地呈现在读者面前。

本书由梅筱琴、蒲韵和廖凯生编写,全书由何跃审定。在编写过程中,作者参考了大量的专业书籍,并得到了许多同行的真诚帮助,在此一并向他们表示衷心地感谢。

编者





第1章 计算机病毒基础知识

1.1	计算机病毒的发展史	1
1.1.1	计算机病毒产生的背景及主要来源	2
1.1.2	计算机病毒的发展进程	5
1.2	计算机病毒的基本概念和特征	8
1.2.1	计算机病毒的定义	8
1.2.2	计算机病毒的特征	8
1.2.3	计算机病毒的分类	12
1.2.4	计算机病毒的传播途径	26
1.2.5	计算机病毒的危害及症状	29





第2章 计算机病毒的机理及发展趋势

2.1	计算机病毒的结构	39
2.1.1	计算机病毒程序举例	40
2.1.2	计算机病毒的逻辑结构	50
2.1.3	计算机病毒的磁盘存储结构	53
2.1.4	计算机病毒的内存驻留结构	58
2.2	计算机病毒的作用机理	61
2.2.1	计算机病毒与中断	61
2.2.2	计算机病毒的引导机理	64
2.2.3	计算机病毒的传染机理	66
2.2.4	计算机病毒的破坏机理	73
2.2.5	计算机病毒的触发机理	74
2.3	计算机病毒的发展趋势	78
2.3.1	当前计算机病毒的最新特点	78
2.3.2	计算机病毒的新动向	79

第3章 计算机病毒的防治原理

3.1	防治病毒的基本原则	87
3.2	防治计算机病毒的基本原理	91
3.2.1	检测计算机病毒的基本原理和方法 ..	91
3.2.2	清除计算机病毒的原理和方法	98
3.2.3	计算机病毒的预防	129
3.2.4	计算机病毒的免疫	134

3.3 计算机反病毒产品介绍	137
3.3.1 初识反病毒产品	138
3.3.2 反病毒产品的作用原理	141
3.3.3 选择反病毒产品的原则	149

第4章 走近反病毒软件

4.1 认识反病毒软件	161
4.1.1 当今流行的反病毒软件	162
4.1.2 反病毒产品的杀毒原理	163
4.2 KV300	163
4.2.1 KV300 的应用	164
4.2.2 硬盘主引导信息的备份与恢复	167
4.2.3 扩展病毒特征库查毒	169
4.2.4 KV300 主要英文提示解说	170
4.2.5 KV3000W 的使用	175
4.2.6 KV 系列最新版本 KV3000 简介	180
4.3 Norton Antivirus 2001	186
4.3.1 Norton Antivirus 的安装	186
4.3.2 Norton Antivirus 的使用	190
4.3.3 Norton Antivirus 的卸载	200
4.4 McAfee VirusScan	202
4.4.1 McAfee VirusScan 的安装	203
4.4.2 检查计算机病毒	206
4.4.3 数据备份和程序升级	216



4.5	瑞星杀毒软件千禧世纪版	219
4.5.1	瑞星杀毒软件的安装和卸载	220
4.5.2	使用瑞星杀毒软件查杀病毒	222
4.6	KILL98	225
4.6.1	KILL98 的安装和卸载	226
4.6.2	KILL98 的使用	227
4.7	KILL2000	230
4.7.1	KILL2000 的安装	231
4.7.2	KILL2000 的使用	233

第5章 几种典型的病毒及其防治

5.1	宏病毒	239
5.1.1	宏病毒的起源	240
5.1.2	宏病毒的防治	246
5.2	CIH 病毒	249
5.2.1	CIH 病毒的破坏作用及机理	250
5.2.2	对 CIH 病毒的防治	253
5.3	电子邮件病毒	255
5.3.1	网络蠕虫病毒	256
5.3.2	Happy99	261
5.3.3	“美丽杀”(W97M-Melissa)	265
5.3.4	“爱虫”病毒	269
5.4	黑客程序	274
5.4.1	黑客简介	274



5.4.2	黑客程序 B0 简介	276
5.4.3	黑客程序 B0 的传播途径	279
5.4.4	黑客程序 B0 的危害性	280
5.4.5	黑客程序 B0 的防治	282
5.5	世界流行的 MS-DOS 病毒	283

第 6 章 计算机系统的安全和访问控制

6.1	什么是计算机安全	297
6.1.1	计算机安全的内涵	298
6.1.2	数据保密性	300
6.1.3	数据的完整性和真实性	301
6.1.4	数据的可用性	302
6.2	计算机安全级别	303
6.2.1	D 级安全	304
6.2.2	C 级安全	304
6.2.3	B 级安全	306
6.2.4	A 级安全	307
6.3	系统访问控制	308
6.3.1	如何登录到计算机上	308
6.3.2	身份认证	320
6.3.3	怎样保护系统的口令	322
6.4	文件和资源的访问控制	328
6.4.1	Windows NT 的资源访问控制	329
6.4.2	UNIX 系统文件访问控制	334



6.5	访问控制的类型	337
6.5.1	选择性访问控制	337
6.5.2	强制性访问控制	339

第7章 计算机软件的安全技术

7.1	计算机软件安全的基本要求	341
7.1.1	计算机安全保密概念	341
7.1.2	软件的本质及特征	343
7.2	软件防拷贝的技术	345
7.2.1	软件保护与加密	345
7.2.2	软件加密的必要性	346
7.2.3	软件的加密和解密过程	347
7.3	软件加密口令与限制技术	354
7.3.1	加密软件的工作方式	354
7.3.2	口令加密技术	355
7.3.3	限制技术	358
7.4	动态跟踪与反跟踪技术	362
7.4.1	动态跟踪工具 DEBUG	362
7.4.2	软件运行中的反跟踪技术	372
7.5	保证软件质量的安全体系	377
7.5.1	概述	377
7.5.2	软件故障的分类	378
7.5.3	软件测试工具	381
7.6	系统软件安全技术	382



7.6.1	计算机软件故障的分类	382
7.6.2	计算机系统软故障的分析	387
7.6.3	基于 DOS 操作系统的安全技术	388
7.6.4	基于 Windows 操作系统的安全技术	399
7.6.5	基于 Windows NT 操作系统的安全技术	402

第 8 章 数据加密技术

8.1	加密的历史	411
8.2	什么是数据加密	412
8.2.1	为什么需要进行加密	412
8.2.2	换位和置换的编码方法	414
8.2.3	加密密钥技术	416
8.2.4	密钥的管理技术	420
8.2.5	一次性密码技术	422
8.3	数据加密标准	424
8.4	数据加密的应用	426
8.4.1	电子商务	426
8.4.2	虚拟私用网络	427
8.5	PGP 邮件加密软件	428
8.5.1	数字签名技术	429
8.5.2	PGP 的密钥管理技术	432



第9章 网络站点的安全

9.1	因特网的安全	437
9.1.1	因特网介绍	438
9.1.2	TCP/IP 协议	439
9.1.3	因特网服务的安全隐患	439
9.1.4	因特网的安全问题及其原因	444
9.1.5	Internet 和 Intranet 的区别	449
9.2	Web 站点的安全	451
9.2.1	Web 站点的安全	452
9.2.2	Web 站点的风险类型	453
9.2.3	Web 站点安全策略	455
9.3	黑客的防范技术	464
9.3.1	黑客与入侵者	464
9.3.2	黑客攻击的三个阶段	466
9.3.3	对付黑客入侵的手段	468
9.4	口令安全问题	472
9.4.1	口令破解过程	472
9.4.2	对根用户的忠告	476
9.5	网络监听与反监听技术	480
9.5.1	网络监听	480
9.5.2	在以太网中的监听	481
9.5.3	网络监听的检测	484
9.6	黑客入侵工具扫描器	489
9.6.1	什么是扫描器	489



9.6.2	端口扫描	490
9.6.3	扫描工具	493
9.7	保障 E-mail 的安全方法	497
9.7.1	E-mail 工作原理及安全漏洞	497
9.7.2	匿名转发	499
9.7.3	E-mail 欺骗	500
9.7.4	E-mail 轰炸和炸弹	501
9.7.5	保护 E-mail	504
9.8	IP 电子欺骗技术	506
9.8.1	盗用 IP 地址	506
9.8.2	什么是 IP 电子欺骗	507
9.8.3	IP 欺骗的对象及实施	509
9.8.4	IP 欺骗攻击的防备	511
9.9	文件传输安全服务	512
9.9.1	FTP 安全措施	512
9.9.2	匿名 FTP 安全漏洞及检查	513
9.9.3	在 UNIX 系统下设置匿名 FTP	515
附录 A	反病毒软件厂商及其产品介绍	519
附录 B	与计算机安全相关的网站	525

第 1 章



计算机病毒基础知识

“知己知彼、百战不殆”。这句至理名言在我们今天对抗计算机病毒的战争中仍发挥着重要的指导作用。

要防治计算机病毒，首先必须对计算机病毒有个基本的了解，搞清其来龙去脉，为防范和清除计算机病毒做好必要的知识储备。



1.1 计算机病毒的发展史

近几年来，有关计算机病毒的报道和消息很多，尤其是 1999 年 4 月 26 日，CIH 病毒大范围发作甚至引起了信息业的震动。究竟是什么原因使人们对计算机病毒如此关注呢？原来，计算机病毒如同人类机体上的疾病，它对计算机系统



有着十分强大的破坏力。病毒能够破坏计算机系统内珍贵的信息资料，甚至能够损坏计算机硬件。由此可以看出，了解一些有关计算机病毒的知识，对于使用计算机的人们来说是十分必要的。

1.1.1 计算机病毒产生的背景及主要来源

1.1.1.1 计算机病毒的产生背景

计算机病毒的产生是计算机技术和以计算机为核心的社会信息化进程发展到一定阶段的必然产物。它产生的背景是：

◆ 计算机软硬件产品的脆弱性是计算机病毒产生的根本技术原因

据调查表明，目前广泛流行的各种计算机病毒中，30%以上是针对 IBM PC 系列及其兼容机的。因为 PC 机所广泛使用的 MS-DOS 操作系统非常简单，透明度也高，很易为用户所掌握；而且 PC 机上硬件的安全机制也很差。整个微机系统是为用户任务而设计的，在软硬件上基本没有什么安全措施，容易被病毒侵入。而在 UNIX 操作系统上则较少发现病毒，因为它有较为完善的安全和保密机制，而且系统较为复杂，不易被一般用户发现其缺点和易攻击处。一些工作站、中型机等在硬件上均设有安全措施，使得病毒很难侵入。此外，计算机软件有没有错误，只能在运行中发现、修改，这就为病毒的侵入提供了方便。

◆ 计算机的广泛应用是计算机病毒产生的必要环境
计算机（尤其是微机）的普及使得病毒得以大面积的传

