

电脑防毒杀毒绝招

苏武荣 编著

365 问



人民邮电出版社

电脑实用技巧问答丛书

电脑防毒杀毒绝招 365 问

苏武荣 编著

人民邮电出版社

内 容 提 要

本书以问答形式,通俗地介绍了电脑病毒的概念、来历、命名、分类、危害,病毒防范与管理措施,流行病毒现象及识别方法,以及实用杀毒工具使用方法。同时还介绍了病毒解剖基础知识、新病毒捕获采集方法与病毒实例分析技术。

本书通俗、易懂,注重实用性和可操作性。读者对象为广大电脑用户,包括电脑初学者、非计算机专业师生和工程技术人员、普通办公人员和管理人员,以及所有电脑爱好者。

3532 / 11

电脑实用技巧问答丛书 电脑防毒杀毒绝招 365 问

苏武荣 编著
责任编辑 贾福新

*

人民邮电出版社出版发行
北京崇文区夕照寺街 14 号
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

*

开本:850×1168 1/32 1996 年 5 月第 1 版
印张:10.125 1997 年 5 月北京第 2 次印刷
字数:259 千字 印数:8 001—13 000 册

ISBN7-115-06074-6/TN·283

定价:16.00 元

前 言

为什么要学？

电脑病毒给电脑应用带来的危害和不良影响,是广大电脑用户人所共知的。

几年来,尽管人们做了许多反病毒工作,但病毒问题仍然困扰着电脑用户。本人从 1989 年发现“小球”病毒以来,一直关注着病毒问题,曾设计过一些防毒、杀毒程序,也写过一些病毒专文,对 SCAN & CLEAN、CPAV、NAV、KILL、KV100/KV200、DBNET/DB95、TNTVIRUS、F-PROT 等杀毒软件都作过分析,对一些出名的防病毒卡也作过研究,也走过软件固化成卡的路。但总觉得,杀毒软件仍难对付日益增多的新病毒,防毒技术也仍难控制新机理病毒的传播,并且一些通用的、广泛使用的防毒软件/防病毒卡更会受到新病毒的攻击,人们寄希望以一个防病毒卡和杀毒软件来解决病毒问题的愿望变得渺茫了。因此,作为电脑操作使用、开发应用与管理人员,能够自己掌握一些必要的电脑病毒知识和病毒防治技术,无疑是至关重要的。

应该学什么？

作为电脑用户，必须了解电脑病毒的概念、来历、命名、分类、危害，以便认清电脑病毒的真面目，并采取必要的病毒防范与管理措施。当病毒突破防线，入侵电脑系统时，应该认识是什么病毒在行动，这时必须懂得选择最有效的杀毒工具来消灭它。如果现有的杀毒工具还无法对付它，应该懂得怎样追杀新病毒，并捕获、采集新病毒样本，向有关部门或专家发出求救信号。《电脑防毒杀毒绝招 365 问》正是从这方面入手，系统地为读者提供了一个学习的教材。

本书有什么特点？

采用问答形式又强调系统性。书中列出 365 问，分为 6 个部分，按基本概念、防毒、识别病毒、杀毒、查新病毒等顺序，比较符合病毒防治的系统原则，条理性较强，也突出了防毒的重要性。同时，还将一些集成反病毒工具分成防毒程序和杀毒程序，分列在防毒部分和杀毒部分介绍，便于读者对同类工具软件加以比较、选择。在前言和每一部分的开头，都对该部分的主要内容作些简介，同时在目录中对主要问题加星号，以便读者能够抓住重点，避免问答式编目给读者带来的零乱感。

力求通俗、易懂，突出实用性。书中既回答了一些知识性、指导性的问题，又重点介绍了各种查毒、防毒、杀毒工具软件的操作使用，而在介绍时并不是对这些软件使用说的简单汇编或翻版，而是力图站在用户的角度上，讲解实用功能的综合使用方法，对于一些不常用的功能就不作介绍。目的是使读者能够轻松地学习如何防毒、杀毒，认识常见病毒，了解病毒的结构和行为。

本书有什么内容？

全书各部分安排如下：

第一招：了解电脑病毒基本知识。介绍电脑病毒的起源与由来，

病毒概念与特性,病毒的定名与分类,以及病毒的激发破坏与危害情况。希望读者能够较全面地了解电脑病毒的本质,认清其真面目。

第二招:建立预防观念采取防毒措施。通过实例强调树立“预防为主、消防结合”的病毒消防观念的重要性,并指明了防毒原则。介绍了广谱防病毒程序 TIG.SYS、VSAFE、BOOTSAFE,以及防病毒卡的使用技巧与注意事项。特别指出了防毒技术的机理,并比较了 TIG.SYS 等防毒软件与通用防病毒卡的性能特点。希望读者能够建立正确的病毒消防观念,并采取正确的防毒措施,防患于未然。

第三招:识别百种常见病毒现象。介绍由病毒引起的系统异常现象,百种常见病毒现象和主要特征,以及推荐使用的杀毒工具。希望读者能够识别常见病毒,以便及早发现病毒。

第四招:掌握实用工具杀毒技能。指出杀毒技术的机理,给出了“杀毒原则”。介绍了 KILL、KV200/KV100、DB95/DBNET、SCAN & CLEAN、CPAV/MSAV、NAV、TNT、SDSCAN/UTSCAN 和 F-PROT 等常用杀毒工具使用技巧与注意事项。希望读者能够掌握实用工具杀毒技能,以便在发现病毒时能够使用合适的杀毒工具来清除病毒。

第五招:学习病毒解剖基础知识。介绍一些与病毒有关的 DOS 系统结构和重要参数,并简介了 DEBUG、PCTOOLS、NORTON 等调试工具软件的使用方法。希望读者能够掌握病毒解剖的基础知识,为捕杀新病毒作准备。

第六招:追杀捕获各种新的病毒。介绍人工识别病毒的方法,以及采集新病毒样本的技术。按病毒的寄生对象和传染机理,用不同方法从不同角度剖析了每一种类型的代表性病毒,并分析了它们各自的共性和特点。所归纳的诊治机理对于新病毒具有普遍的适用性。希望读者能够掌握各类病毒的特点和防治方法,能够对现有的杀毒、防毒工具还无法清除的新病毒或变种病毒予以诊治、排除。该部分对于希望用 DEBUG 等工具获取、分析病毒源程序并自行消除病毒的读者,无疑具有很好的参考价值。

您应该怎么学？

本书 6 招 365 问,您既可以按顺序系统地阅读,也可以选择感兴趣的问题查阅。如果您是一个初学电脑的用户,您应该认识电脑病毒的真面目,学习如何防毒、杀毒,以便增进您学习使用电脑的兴趣。那么,您应该学习第一至四招。如果您是一位在校学生,或者是一个电脑迷,您们是接触病毒最多的一群,认识常见的病毒,学习如何防毒、杀毒,并了解病毒的结构,了解病毒的行为,成为查毒能手,您便又获得一种特别的本领,这很可能是您求职、交友的敲门砖。那么,您不妨练习一至六招,特别是要攻读最具挑战性的第六招。当然,本书也可能会作为您应付“信息安全与病毒防治”课程的作业、考试的奇招。如果您是一个电脑专业工程师,您应该认识常见的病毒,了解病毒的结构,了解病毒的行为,做出更安全的信息系统。这是您责无旁贷的责任。那么,您应该赶快学完第一至四招。有空的时候,不妨再看看第五、六招。临时抱佛脚,也灵!如果您是一位办公人员,或者是一个家庭电脑使用者,您应该认识病毒可能有的破坏行为,建立防毒杀毒常识,以便获得上级或亲友的赞赏。那么,您最需要了解第一、二、三招,发现病毒时,马上学习第四招,也可以依样画葫芦。如果您是一个部门领导,您应该了解病毒所破坏的是无价的数据,如何使员工建立正确的防毒杀毒观念,创造一个无病毒的环境。那么,您最起码要看看第一、二招。有兴趣的时候,还可以查阅一下第三、四招。

一年 365 天,但愿《电脑防毒杀毒绝招 365 问》天天伴随您,让您摆脱电脑病毒的烦恼。

苏武荣

1996 年 1 月于福州

目 录

第一招 了解电脑病毒基本知识	1
1. 电脑病毒是什么?	1
2. 电脑病毒起源于“磁心大战”吗?	1
3. 电脑病毒是看不见摸不着的吗?	2
4. 电脑病毒与生物病毒有什么异同?	4
※5. 电脑病毒会传染给人吗?	4
6. 什么是特洛伊木马?	4
7. 什么是逻辑炸弹?	5
8. 电脑病毒与逻辑炸弹有什么异同?	5
9. 衡量病毒的标准是什么?	6
※10. 电脑病毒是怎样传播的?	6
11. 电脑病毒是由哪些部分组成的?	6
12. 电脑病毒是如何运作的?	7
13. 电脑病毒是硬件故障或编程失误吗?	7
※14. 谁制造电脑病毒?	7
15. 电脑病毒是如何定名的?	8
16. 病毒定名有哪些方法?	9

※17. 为什么一种病毒会有多个名称?	10
18. 电脑病毒有哪些分类?	10
※19. PC 病毒如何分类?	11
20. 什么是引导型病毒?	12
21. 引导型病毒有哪些主要特点?	13
22. 什么是文件型病毒?	13
23. 文件型病毒有哪些驻留内存方式?	13
24. 不驻留内存型病毒与驻留型有什么不同?	14
25. 电脑病毒有哪些激发方式?	15
※26. 电脑病毒有哪些破坏方式?	15
27. 哪些病毒是定时病发的?	16
28. 什么是蠕虫?	23
29. INTERNET 网络事件是怎么回事?	23
30. 病毒制造者的结果如何?	25
第二招 建立预防观念 采取防毒措施	27
31. 电脑染上病毒是正常现象吗?	27
32. 杀毒软件能解决一切病毒问题吗?	28
※33. 为什么要树立病毒消防观念?	29
34. 病毒都是由玩游戏传染的吗?	30
※35. 电脑用户能不能玩游戏?	30
36. 电脑安全管理应采取哪些措施?	30
37. 电脑病毒是难以控制的吗?	31
※38. 如何预防病毒?	31
39. 为什么数据盘会传染病毒?	32
40. 如何控制数据盘传染病毒?	32
41. 现有哪些防毒工具?	33
※42. 为什么说防毒是主动的?	34
43. 如何选择一个可靠的反病毒系统?	35
44. 病毒防护策略应有哪些准则?	36

45. 防治引导型病毒有什么通用方法?	37
※46. 为什么 BOOTSAFE 能防治引导型病毒?	37
47. BOOTSAFE 有哪些使用格式?	37
48. BOOTSAFE 如何备份 MBR 和 BR?	38
49. BOOTSAFE 如何比较备份文件?	39
50. BOOTSAFE 如何重建备份文件?	39
51. BOOTSAFE 如何恢复 MBR 和 BR?	40
52. 使用 BOOTSAFE 应注意哪些?	40
※53. 通用防毒 VSAFE 有什么特点?	40
54. VSAFE.COM 与 VSAFE.SYS 有什么区别?	41
※55. 病毒监查 VWATCH 有什么特点?	41
56. 如何启动 VSAFE?	41
57. 如何激活 VSAFE 控制窗口?	42
58. 如何选用 VSAFE 的控制项?	43
59. VSAFE 可以用命令行参数启动吗?	45
60. 使用 VSAFE 应注意什么?	46
61. 是否有永远有效的防毒技术?	47
62. 电脑病毒有哪些本质弱点?	47
63. 引导型病毒防范有哪些依据?	48
64. 文件型病毒防范有哪些依据?	49
※65. 广谱防病毒程序 TIG.SYS 有什么特点?	51
66. 如何安装和启动 TIG?	52
67. 如何对待 TIG 报毒信息?	52
68. TIG.SYS 怎样与 VSAFE.SYS 联用?	53
69. TIG.SYS 怎样与 CPAV 文件免疫功能联用?	54
70. VCHECK.SYS 是什么?	54
※71. VCHECK.SYS 有什么特点?	54
72. 为什么 VCHECK.SYS 有较高的兼容性?	55
※73. 防毒 VIRSTOP.EXE 有什么特点?	55

74. 如何启动与安装 VIRSTOP?	56
75. 什么是 PC-cillin(电脑疫苗)?	56
※76. PC-cillin 如何操作?	56
77. 硬件“免疫锁”有什么作用?	57
※78. 笔记本电脑 MobileProtect 有什么特点?	57
79. 国内有哪些防病毒卡?	58
※80. 防病毒卡是怎样工作的?	58
81. 什么是防病毒卡的广谱抗病毒性?	59
82. 什么是防病毒卡的主动防御性?	59
83. 什么是防病毒卡的工作时机的及时性?	59
84. 什么是防病毒卡的自身抗毒的坚固性?	59
85. 什么叫“误报”?	60
86. 什么叫“漏报”?	60
87. 什么叫“肯定式报毒”?	60
88. 什么叫“疑问式报警”?	60
※89. “带毒运行”有哪些利弊?	60
90. 如何设置防病毒卡开关?	61
91. 如何安装防病毒卡?	61
92. 如何解决与 TVGA 显示卡的兼容问题?	61
93. 如何处理肯定式报毒?	61
94. 如何处理疑问式报警?	62
※95. 如何认识防病毒卡的问题?	63
96. 防病毒卡能杀毒吗?	64
97. 选用防病毒卡应注意什么?	64
※98. 如何建立安全的防毒系统?	65
99. 病毒防范为什么要使用法律武器?	66
100. 如何制定法律来惩治病毒传播者?	66
第三招 识别百种常见病毒现象	67
101. 系统引导时有哪些病毒现象?	67

102. 文件异常有哪些病毒现象?	68
103. 外部设备异常有哪些病毒现象?	69
※104. 引导型病毒有什么共性?	69
105. 怎样识别“小球”病毒?	70
106. 怎样识别“大麻”/Stoned 病毒?	70
107. 怎样识别“米氏”病毒?	71
108. 怎样识别 6.4/Bloody 病毒?	72
109. 怎样识别“广州一号”病毒?	72
110. 怎样识别 Brain 病毒?	73
111. 怎样识别“磁盘杀手”(DiskKiller)?	74
112. 怎样识别“火炬”/1901 病毒?	75
113. 怎样识别 2708/Azusa 病毒?	76
114. 怎样识别 Break 病毒?	77
115. 怎样识别 Mask 病毒?	77
116. 怎样识别 Joshi/“生日快乐”病毒?	78
117. 怎样识别 AirCop(“空中警察”)病毒?	78
118. 怎样识别 BOOT 255 病毒?	79
※119. CMOS 病毒是寄生在 CMOS 中吗?	79
※120. GenB 病毒是什么?	80
121. GenP 病毒是什么?	80
122. 怎样识别 INT60/“新 MBR”病毒?	81
※123. 文件型病毒有什么共性?	81
124. 怎样识别“黑色星期五”?	81
125. 怎样识别“星期天”(Sunday)病毒?	82
126. 怎样识别 1701/Cascade 病毒?	83
127. 怎样识别“中国炸弹”(Chinese Bomb)?	84
128. 怎样识别“旅游者”(Traveller)病毒?	84
129. 怎样识别 1575/“毛毛虫”病毒?	84
130. 怎样识别 N64 病毒?	85

131. 怎样识别 DaBi/“小红”病毒?	86
132. 怎样识别 934/“无光标”病毒?	87
133. 怎样识别 Alabama/1560 病毒?	87
※134. 怎样识别 INOC/AntiVirus 病毒?	88
135. 怎样识别“音乐”/Oropax 病毒?	88
136. 怎样识别“百年”(The 100 Years)病毒?	89
137. 怎样识别“数据犯罪”(Data Crime)病毒?	90
138. 怎样识别 dBASEII 病毒?	90
139. 怎样识别 STORY TELLER(“讲故事者”)病毒?	90
140. 怎样识别 RS232/CHGLGH 病毒?	91
141. 怎样识别 BACKFORM 病毒?	92
142. 怎样识别 V888 病毒?	92
143. 怎样识别 SRI848 病毒?	93
144. 怎样识别 1759/“写保护”病毒?	93
145. 怎样识别 2048 病毒?	94
146. 怎样识别 Gene/“大连”病毒?	95
※147. 怎样识别 PRGKILLER(“数据库杀手”)?	95
148. 怎样识别“维也纳”/648 病毒?	96
149. 怎样识别 DIR2 病毒?	97
150. 怎样识别 Casino/“娱乐场”病毒?	98
151. 怎样识别 Taiwan(“台湾”)病毒?	99
152. 怎样识别 DieHard/SW 病毒?	99
153. 怎样识别“红心”病毒?	100
154. 怎样识别 Marauder(“抢匪”)病毒?	101
155. 怎样识别 Suriv/“愚人节”病毒?	101
156. 怎样识别 Yankee/洋基病毒?	102
157. 怎样识别 1099/“随机格式化”病毒?	102
158. 怎样识别 Maltese Amoba 病毒?	103
159. 怎样识别 Tiny/Kennedy 病毒?	104

160. 怎样识别“黑色复仇者”(Dark Avenger)病毒?	104
※161. 什么是混合型病毒?	105
162. 怎样识别“侵略者”(Invader)病毒?	105
163. 怎样识别“新世纪”/XqR 病毒?	106
164. 怎样识别“秋水”/ChangSha94 病毒?	106
165. 怎样识别 Flip/“热甜啤酒”病毒?	107
166. 怎样识别 Liberty/MYSTIC 病毒?	108
167. 怎样识别 BUPT 9146 病毒?	109
※168. 怎样识别 1971/“香烟”病毒?	110
※169. 为什么 1971 病毒会反 CPAV?	111
※170. 什么是变形病毒?	111
171. 怎样识别 Doctor(“医生的忠告”)病毒?	111
172. 怎样识别“幽灵”病毒?	113
173. 怎样识别 Casper 病毒?	114
174. 怎样识别 HXH-2106 病毒?	114
175. 怎样识别 ZGB/2128 病毒?	115
176. 怎样识别 Dong/1741 病毒?	115
177. 怎样识别 CMOS 1999 病毒?	116
※178. 什么是病毒生成器?	117
179. 目前国内已发现多少种病毒?	117
※180. 怎样清除国内出现的病毒?	117
第四招 掌握实用工具杀毒技能	125
※181. 发现病毒, 怎么办?	125
182. 杀毒软件是如何工作的?	126
183. 为什么说杀毒是被动的?	127
※184. 为什么要不断更新杀毒软件?	127
185. 杀毒过程中应注意哪些问题?	128
186. 国产杀毒软件 KILL 有哪些特点?	128
187. 如何启动 KILL?	129

188. KILL 如何杀除病毒?	131
※189. 用 KILL 杀毒时死机, 怎么办?	131
190. 为什么旧版 KILL 能杀的病毒而“新”版却不能杀?	131
191. KILL 是如何加密而又能方便升级的?	132
192. 使用 KILL 要注意哪些问题?	132
193. “超级巡警”KV200/KV100 有什么特点?	132
※194. 如何使用 KV200/KV100 查毒杀毒?	133
195. 如何巧用 KV200/KV100 修复硬盘分区表?	135
196. KV200/KV100 如何清除所有引导型病毒?	136
197. 如何使用扩展的病毒特征码?	136
198. KV200/KV100 如何快速搜索病毒?	137
199. 为什么 KV200/KV100 能由用户自己升级查新病毒?	137
200. 如何编写 KV200/KV100 查新病毒的特征串?	138
201. 增加病毒特征码时应注意什么?	138
202. KV200/KV100 如何查解变形病毒?	139
203. 怎样获得病毒特征码和扩展的杀毒程序?	141
※204. 为什么 KV200 能由用户自己升级杀新病毒?	146
205. 如何加载扩展程序杀新病毒?	148
206. KV200/KV100 受感染时, 如何自我修复?	149
207. 使用 KV200/KV100 应注意什么?	149
208. KV200 提供哪些接口地址及调用方法?	150
209. 用户怎样编写 KV200 杀毒程序代码?	151
※210. “帝霸”DB95 有什么特点?	154
211. 如何安装 DB95?	154
212. DB95 第一次启动应注意什么?	155
213. 如何使用 DB95?	155
214. 为什么 DB95 能清除新的病毒?	155

215. 扫描软件 SCAN 有什么特点?	155
216. SCAN 有哪些命令行参数?	156
※217. 如何使用 SCAN 查毒?	158
218. SCAN.EXE 本身被感染了, 怎么办?	159
219. 杀毒软件 CLEAN 是什么?	159
220. CLEAN 有哪些命令行参数?	159
※221. 如何使用 CLEAN 杀毒?	160
222. 集成杀毒工具 CPAV 有什么特点?	161
223. 如何安装 CPAV?	162
224. 如何启动 CPAV?	162
※225. CPAV 能在汉字系统下运行吗?	163
226. 如何使用 CPAV 查毒?	164
227. 如何使用 CPAV 杀毒?	165
228. CPAV 如何检测“新的操作驱动器”?	165
229. 什么是 CPAV“全屏菜单”?	165
※230. 如何在 CPAV 全屏菜单中杀毒免疫?	167
231. CPAV 免疫代码如何解毒?	168
232. 哪些文件不能加 CPAV 免疫代码?	168
233. 如何设置 CPAV 全屏菜单的操作参数?	169
234. 出现完整性校验错误, 怎么办?	172
235. 如何配置 CPAV 全屏菜单工作环境?	172
236. 如何取消 CPAV 的口令?	173
237. 如何使用 CPAV 全屏菜单帮助功能?	174
238. 如何使用 CPAV/MSAV 命令行方式?	175
※239. 如何用 CPAV 制作应急软盘?	175
240. 什么情况下使用应急软盘?	176
241. 共享杀毒软件 F-PROT 有什么特点?	177
242. 如何启动 F-PROT?	177
※243. 如何使用 F-PROT 查毒杀毒?	177

244. 怎样查阅 F-PROT 病毒资料?	180
245. F-PROT 如何对 F-PROT 增加新病毒特征串? ...	180
246. 如何了解 F-PROT 程序的版本信息?	180
247. 如何使用 F-PROT 命令行方式?	180
248. Norton AntiVirus3.0 有什么特点?	181
249. 如何启动 NAV 菜单?	182
250. 如何使用 NAV 杀毒?	182
251. 如何改变 NAV 检测参数?	183
252. 如何查看 NAV 病毒资料?	184
※253. NAV 如何检测被压缩的文件?	184
254. 如何以 DOS 命令行方式运行 NAV?	184
255. 如何在 Windows 环境下运行 NAV?	185
256. 如何启动扫描消毒程序 SDSCAN/UTSCAN?	186
※257. 如何修改 SDSCAN 的操作参数?	186
258. 如何使用 SDSCAN 杀毒?	187
259. 如何启动快速杀毒工具 TNT?	188
260. 如何修改 TNT 操作参数?	189
※261. 如何使用 TNT 杀毒?	190
262. 如何使用 TNT 免疫功能?	190
第五招 学习病毒解剖基础知识	192
263. 什么是 DEBUG?	192
264. 如何启动 DEBUG 程序?	193
※265. 如何使用 DEBUG 命令?	193
266. 什么是 PCTOOLS?	199
267. 如何启动 PCTOOLS?	200
※268. 如何使用 PCTOOLS?	200
269. 什么是 Norton Utility?	202
270. 如何启动 Norton Utility?	202
※271. 如何使用 Norton Utility?	202