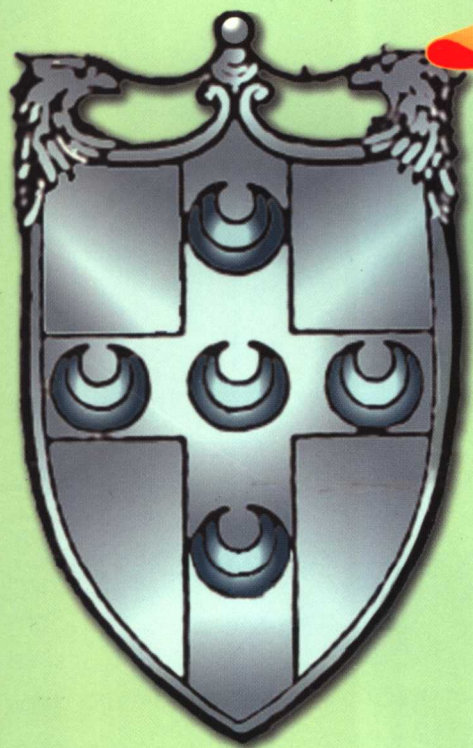


计算机病毒

防治与信息安全知识

300 问

张 洁 张学志 王 鹏 编



冶金工业出版社

<http://www.cnmp.com.cn>

计算机病毒防治与信息 安全知识 300 问

张 洁 张学志 王 鹏 编

北 京
冶 金 工 业 出 版 社
2006

内 容 提 要

本书从实用的角度出发,分析整理了计算机各种常见病毒和信息安全方面的 300 个问题,从病毒基础知识、病毒档案、病毒防治、杀毒软件、信息安全和防御黑客技术等六个方面介绍了相关的知识,深入分析了计算机病毒的生成机理、感染途径和防治方法,以帮助读者了解计算机病毒,并在日常生活中更好地加以防范,最低限度地降低计算机病毒对用户的伤害。

本书精选的 300 个问题具有很强的代表性,并深入浅出、简单明了地进行了解答,适合广大计算机爱好者以及软件开发人员学习和参考。

图书在版编目(CIP)数据

计算机病毒防治与信息安全知识 300 问/张洁等编.

北京:冶金工业出版社,2006.10

ISBN 7-5024-4085-2

I. 计... II. 张... III. 计算机病毒—防治—问答
IV. TP309.5-44

中国版本图书馆 CIP 数据核字 (2006) 第 096547 号

出 版 人 曹胜利 (北京沙滩嵩祝院北巷 39 号,邮编 100009)

责任编辑 张 卫 (联系电话:010-64027930; 电子信箱:bull2820@sina.com)

王雪涛 (联系电话:010-64062877; 电子信箱:2bs@cnmip.com.cn)

张爱平 (联系电话:010-64027928; 电子信息:zaptju99@163.com)

美术编辑 李 心 责任校对 符燕蓉 李文彦 责任印制 丁小晶

北京兴顺印刷厂印刷;冶金工业出版社发行;各地新华书店经销

2006 年 10 月第 1 版,2006 年 10 月第 1 次印刷

787mm×1092mm 1/16; 15.75 印张; 377 千字; 235 页; 1—3000 册

25.00 元

冶金工业出版社发行部 电话:(010)64044283 传真:(010)64027893

冶金书店 地址:北京东四西大街 46 号(100711) 电话:(010)65289081

(本社图书如有印装质量问题,本社发行部负责退换)

前 言

计算机已经进入社会生活的各个方面，成为人们工作、学习、生活的工具。随着计算机在各行各业的广泛应用，计算机病毒也随之泛滥，已经危害到科学研究、工程实践、经济、军事，甚至危害到国家安全，其危害程度也越来越受到人们的关注。

虽然已出版的关于计算机病毒的书比较多，但其内容只是就杀毒软件的使用谈防治，而计算机病毒的时效性又非常强，更新速度也非常快，因此一些书的内容很快就会随着计算机病毒的更新而变得陈旧过时。本书根据计算机病毒的机理从实用的角度出发，分析整理了计算机病毒基础知识、病毒档案、病毒防治、杀毒软件、信息安全和防御黑客技术等方面的问题，深入浅出地介绍了计算机病毒的生成机理、感染途径和防治方法，通过举一反三，帮助读者了解计算机病毒的相关知识和掌握防治病毒的方法。同时书中也简要地介绍了最新的病毒和杀毒软件，读者也可以了解计算机最新病毒的信息。

本书适用于广大计算机爱好者，也可供广大编程爱好者、软件开发人员参考。

由于时间仓促，书中难免有些不妥之处，恳请读者谅解，并请指正。

编 者

2006年6月

目 录

第1章 病毒基本知识.....	1
1. 什么是计算机病毒?	1
2. 计算机病毒是怎么产生的?	1
3. 计算机病毒有哪些特性?	1
4. 计算机病毒主要有哪些传播途径?	3
5. 计算机病毒是如何感染文件的?	3
6. 如何确定 Boot 区是否被病毒感染?	3
7. 计算机病毒主要存在哪些媒体上?	4
8. 计算机病毒的生命周期有多长?	4
9. 计算机病毒由哪些部分组成?	5
10. 衡量病毒的标准是什么?	5
11. 计算机病毒的破坏类型有哪几种?	6
12. 计算机病毒的表现现象有哪些?	6
13. 计算机病毒的主要破坏行为有哪些?	6
14. 计算机病毒的隐蔽性主要有哪些表现?	7
15. 计算机病毒的触发机制是什么?	7
16. 计算机病毒的传染机制是怎样的?	8
17. 计算机病毒的寄生对象有哪些?	9
18. 计算机病毒有哪些寄生方式?	9
19. 计算机病毒的引导过程是怎样的?	9
20. 计算机病毒与逻辑炸弹有什么区别?	10
21. 对计算机感染病毒的错误认识主要有哪些?	10
22. 计算机感染病毒后主要有哪些症状?	11
23. 病毒工作环节包括哪几个方面?	12
24. 与计算机病毒有关的名词有哪些?	12
25. 目前出现的计算机病毒有哪些新特点?	14
26. 国内外病毒行业的发展状况怎样?	15
27. 什么是计算机病毒对抗?	16
28. 计算机病毒的攻击技术是什么?	17
29. 计算机病毒的防御技术是什么?	17
30. 什么是超级计算机病毒?	18

31. 病毒隐藏技术主要有哪些?	18
32. 什么是中断?	19
33. 中断与计算机病毒有什么关系?	19
34. 什么是病毒自动生产技术?	20
35. 什么是多态性病毒技术?	20
36. 什么是隐藏性病毒技术?	21
37. 在网络上计算机病毒有什么特点?	21
38. 破坏性感染病毒技术有哪些?	22
39. 怎样面对计算机病毒?	22
40. 上网看 Homepages 会中毒吗?	23
41. 计算机病毒是谁制造的?	23
42. 计算机染上病毒是正常现象吗?	24
43. 计算机病毒有哪些本质弱点?	24
44. 微型计算机病毒对系统的影响表现在哪些方面?	24
45. 如果计算机感染了病毒怎么办?	25
46. 如何安装和使用杀毒软件?	25
47. 计算机突然变慢是怎么回事?	27
48. 为什么计算机流量会突然增加?	27
49. 计算机为什么突然丢失文件, 且多了一个未知的账号?	27
50. 计算机安装了操作系统补丁 (Windows update), 安装了防病毒软件, 而且也按时升级病毒定义文件, 为什么还是中了木马程序?	28

第 2 章 病毒档案

51. 计算机病毒最常见的有哪几种类型?	29
52. 国际上对病毒的命名主要有哪些?	30
53. 为什么一种病毒会有多个名称?	31
54. 32 位操作系统下有哪些病毒?	31
55. 什么是 DOS 病毒?	32
56. 什么是 Windows 病毒?	33
57. 什么是入侵型病毒?	35
58. 什么是嵌入式病毒?	35
59. 什么是外壳类病毒?	35
60. 什么是伴随型病毒?	35
61. 什么是“蠕虫”型病毒?	35
62. 什么是“寄生”型病毒?	36
63. 什么是引导型病毒?	37
64. 什么是变形病毒, 分为哪些类型?	37
65. 什么是欺骗病毒?	38

66. 什么是多形型病毒 (幽灵病毒)?	38
67. 什么是计算机宏病毒?	38
68. 宏病毒是如何传播的?	39
69. 宏病毒有哪些危害?	39
70. 计算机宏病毒有哪些?	40
71. 计算机宏病毒的作用机制?	40
72. 计算机宏病毒的原理?	40
73. 计算机宏病毒的主要类型?	41
74. 什么是计算机网络病毒?	41
75. 计算机网络病毒有哪些特点?	41
76. 计算机网络病毒传播的方式及特点?	42
77. 什么是“QQ 尾巴”?	43
78. 什么是“木马”病毒?	44
79. 什么是计算机邮件病毒?	45
80. 什么是恶意网页病毒?	46
81. 恶意网页病毒有哪些特点及种类?	46
82. 宏病毒与传统病毒有哪些差异?	50
83. 引导型病毒主要有哪些特点?	50
84. 网络病毒有什么特点?	51
85. 网络病毒有什么危害性?	51
86. “蠕虫”病毒有什么特点?	52
87. “蠕虫”病毒的基本原理?	53
88. “寄生”型病毒有什么特点?	53
89. 计算机宏病毒有什么特点?	54
90. 计算机邮件病毒有什么特点?	54
91. 什么是 ActiveX 恶意程序码?	55
92. 什么是混合型病毒?	55
93. 混合型病毒有什么特点?	55
94. 恶意网页病毒有些什么症状?	56
95. 不驻留内存的病毒和驻留内存的病毒有什么不同?	57
96. 目前的计算机流行病毒有哪些?	57
97. 2004 年最流行的十大病毒是哪些?	58
98. 最新 MSN 病毒有些什么特点?	60
99. 什么是 CIH 病毒?	62
100. CIH 病毒是怎样发展的?	62
101. 经典的计算机 CIH 病毒有哪些特点?	63
102. 怎么判断是否感染 CIH 病毒?	63

103. 怎样防治 CIH 病毒?	64
104. CIH 是用什么方法进行感染的?	64
105. CIH 病毒怎样破坏 BIOS?	65
106. 受 CIH 病毒攻击后的修复方法是什么?	65
107. 最新“冲击波”病毒的特点有哪些?	66
108. 最新网络蠕虫 I-Worm/Novarg (挪威客) 的可能邮件形式是什么?	66
109. 尼姆达病毒的传播手段及特点有哪些?	66
110. 红色代码病毒的特点是什么?	68
111. Sircam “蠕虫”病毒的特点是什么?	69
112. HappyTime “蠕虫”病毒的特点?	70
113. CodeBlue (蓝色代码) “蠕虫”病毒的特点?	70
114. Funlove 病毒的特点?	71
115. Hybris “蠕虫”病毒的特点?	72
116. 病毒编制的关键技术有哪些?	73
117. 哪些病毒是定时病发的?	73
118. 什么是手机病毒?	78
119. 手机病毒主要有哪些?	79
120. 手机病毒怎么破坏手机的?	79
121. 手机病毒引发的三大疑问是什么?	80

第 3 章 病毒防治

122. 计算机病毒防治的概念是什么?	82
123. 怎样检测计算机病毒?	82
124. 计算机病毒发作前的表现形式是什么?	83
125. 计算机病毒发作时的表现形式是什么?	83
126. 计算机病毒发作后的表现形式是什么?	84
127. 计算机病毒的预防技术有哪些?	84
128. 计算机病毒的消除技术主要有哪些?	85
129. 什么是计算机病毒的免疫原理?	85
130. 计算机病毒的管理办法有哪些?	87
131. 计算机病毒的防治策略有哪些?	87
132. 目前主要的反病毒技术有哪些?	87
133. 主要反病毒的方式有哪些?	88
134. 反病毒技术是怎样判断病毒的?	89
135. 反病毒技术是怎样清除病毒的?	90
136. 反病毒技术的主要特点是什么?	90
137. 如何才能预防病毒破坏?	91
138. 怎么远离计算机病毒?	91

139. 计算机病毒检验的特征代码法的主要步骤和优缺点是什么?	92
140. 计算机病毒检验的校验和法的主要步骤和优缺点是什么?	92
141. 计算机病毒检验的行为监测法的主要步骤和优缺点是什么?	93
142. 计算机病毒检验的软件模拟法的主要步骤和优缺点是什么?	93
143. 对感染病毒的软盘进行 DIR 操作就会导致硬盘被感染吗?	94
144. 将文件改为只读方式可免受病毒的感染吗?	94
145. 病毒能感染处于写保护状态的磁盘吗?	94
146. 反病毒软件能够清除所有已知病毒吗?	94
147. 使用杀毒软件可以免受病毒的侵扰吗?	94
148. 磁盘文件损坏多为病毒所为吗?	95
149. 如果做备份的时候, 备份了病毒, 那么这些备份是无用的吗?	95
150. 反病毒软件可以随时随地防护任何病毒吗?	95
151. 病毒不能从一种类型计算机向另一种类型计算机蔓延吗?	95
152. 病毒不感染数据文件吗?	95
153. 病毒能隐藏在计算机的 CMOS 存储器里吗?	96
154. 去除计算机病毒需要低级格式化吗?	96
155. “蠕虫”病毒的防治?	97
156. “特洛伊木马”病毒如何防治?	97
157. 计算机宏病毒如何防治?	98
158. 宏病毒的传播途径有哪些?	99
159. 怎么清除计算机宏病毒?	99
160. QQ 尾巴如何防治?	100
161. MSN 病毒怎么防治?	103
162. 在中毒环境下如何查杀震荡波?	103
163. 计算机邮件病毒的防治?	104
164. 怎样预防计算机网络病毒?	105
165. 怎样防止计算机病毒对网络的攻击?	107
166. 网络病毒防治服务常见设置有哪些?	108
167. 怎样保持计算机不染病毒?	109
168. 如何对冲击波病毒进行防治?	109
169. 如何对网络天空蠕虫病毒进行防治?	111
170. “网银大盗”及变种病毒如何防治?	112
171. 如何对“Worm. Mydoom”蠕虫病毒进行防治?	113
172. “恶鹰”Worm. Beagle 蠕虫病毒如何防治?	114
173. 如何对 QQ 木马 Win32. Troj. QQNark 进行防治?	114
174. CIH 病毒如何防治?	114
175. 如何对尼姆达病毒进行防治?	116

176. 如何对红色代码Ⅱ病毒进行防治?	117
177. 如何对 Sircam“蠕虫”病毒进行防治?	118
178. 如何对 HappyTime 蠕虫病毒进行防治?	118
179. 如何防治 CodeBlue (蓝色代码) 蠕虫病毒?	119
180. 如何防治 Funlove 病毒?	121
181. 如何防治 Hybris 蠕虫病毒?	121
182. 红色代码Ⅱ变种 (CodeRedⅢ) 的分析解决方案是什么?	122
183. “恶邮差 (Supnot. 127488. h)” 新变种分析及解决方案。	123
184. Format 这个命令可以将病毒完全清除, 这是真的吗?	126
185. 怎样防范电子邮件病毒和“邮件炸弹”?	127
186. 遭受恶意网页病毒破坏, 怎么修复?	127
187. 如何设置 Win2000 的口令?	128
188. 什么是计算机端口?	129
189. 计算机有哪些端口, 作用分别是什么?	129
190. 如何关闭计算机 3389 端口?	130
191. 如何关闭计算机 4899 端口?	130
192. 如何关闭计算机 5800, 5900 端口?	131
193. 如何关闭计算机 6129 端口?	131
194. 如何关闭计算机 45576 端口?	131

第 4 章 杀毒软件..... 132

195. 什么是杀毒软件?	132
196. 杀毒软件的组成?	132
197. 国外主流的杀毒软件有哪几种?	132
198. 国内主流的杀毒软件有哪几种?	133
199. 杀毒软件的杀毒原理是什么?	133
200. 病毒检测软件的作用原理是什么?	133
201. 杀毒软件有些什么功能?	134
202. 什么是杀毒软件的实时功能?	134
203. 杀毒软件杀毒应注意哪些方面?	134
204. 杀毒软件能杀木马吗?	135
205. 在 Windows 下, 为什么用杀毒软件不能杀掉病毒?	135
206. 杀毒软件中, 什么称为病毒隔离?	135
207. 瑞星杀毒软件怎么安装?	135
208. 瑞星杀毒软件怎么操作?	141
209. 江民杀毒软件怎么安装?	142
210. 江民杀毒软件怎么查毒?	148
211. 江民杀毒软件怎么杀毒?	149

212. 金山毒霸怎么安装?	152
213. 金山毒霸怎么查毒?	154
214. 金山毒霸怎么杀毒?	156
215. 怎么用金山毒霸修复 IE 的文件关联?	157
216. 怎么用金山毒霸智能过滤邮件垃圾?	157
217. 怎么用金山毒霸突破磁盘分区的访问限制?	159
218. Norton 杀毒软件怎么安装?	160
219. Norton 杀毒软件怎么查毒?	164
220. Norton 杀毒软件怎么杀毒?	165
221. Kill98 杀毒软件怎么安装?	167
222. Kill98 杀毒软件怎么查毒?	171
223. Kill98 杀毒软件怎么杀毒	173
224. “QQ” 病毒专杀工具有哪些?	173
225. 常见的流行的网络病毒主要有哪些?	174
226. 冲击波病毒专杀工具有哪些?	174
227. 怎么杀灭冲击波病毒?	175
228. 振荡波病毒专杀工具有哪些?	178
229. 振荡波病毒的发作现象是什么?	178
230. 解决振荡波病毒的方法是什么?	180
231. 怎么在线杀毒?	180
232. 在线杀毒的主要网站有哪些?	181
233. 杀毒软件与防火墙有什么不同?	182
234. 杀毒软件进一步发展的瓶颈在哪里?	182
235. 杀毒软件的急救盘怎么用?	182
236. 安装杀毒软件后与其他软件冲突怎么办?	184
237. 杀毒软件不能正常升级怎么办?	184
238. 杀毒软件无法清除病毒怎么办?	185
第 5 章 信息安全	186
239. 什么是计算机信息安全?	186
240. 什么是计算机网络安全?	186
241. 信息安全和网络安全潜在的威胁有哪几方面?	186
242. 目前主要有哪些信息安全隐患?	187
243. Windows 的主要安全隐患有哪些?	187
244. Unix 主要存在哪些安全隐患?	188
245. 什么是网络炸弹?	188
246. 什么是邮件炸弹?	188
247. 什么是逻辑炸弹?	188

248. 什么是后门?	189
249. 什么是伪 IP?	189
250. 什么是 IE 漏洞?	189
251. IE 有哪些安全漏洞?	189
252. IE 安全漏洞怎么修补?	190
253. E-mail 工作原理是什么, 有哪些安全漏洞?	190
254. 什么是 E-mail 欺骗?	191
255. 什么是 E-mail 轰炸和炸弹?	191
256. 什么是防火墙?	192
257. 防火墙的主要功能有哪些?	192
258. 怎么安装防火墙?	193
259. 防火墙如何设置?	197
260. 防火墙如何卸载?	202
261. 国内有哪些主要的防火墙软件?	203
262. 国外有哪些主要的防火墙软件?	203
263. 怎么对计算机系统进行安全设置?	204
264. 设置计算机密码应遵循什么原则?	204
265. 计算机中有些什么加密技术?	205
266. 系统中各种密码文件分别在什么位置?	206
267. 怎样检测系统中的木马?	207
268. 怎样删除系统中的木马?	208
269. Windows 中有哪些信息安全方面的服务?	210
270. 木马主要采用哪些端口?	211
271. 木马程序是如何实现隐藏的?	214
272. 什么是拒绝服务式攻击?	215
273. 什么是缓冲区溢出攻击?	215
274. 什么是补丁?	216
275. 补丁有什么用?	216
276. 怎样为系统程序打补丁?	216
277. 怎么清除 BO2000 木马?	216
278. 怎么清除 NetSky 木马?	217
279. 怎么清除 Happy99 木马?	218
280. 怎么清除冰河木马?	218

第 6 章 防御黑客技术..... 220

281. 什么是黑客?	220
282. 黑客可以分为哪几种类型?	220
283. 黑客有什么样的危害?	221

284. 黑客具备什么技能?	221
285. 黑客攻击手段有哪些?	221
286. 黑客用什么工具破译密码?	223
287. 黑客用什么工具扫描端口?	223
288. 防御黑客的主要措施有哪些?	224
289. 什么是入侵检测系统 (IDS)?	225
290. 有哪些重要的 IDS 系统?	225
291. 入侵者如何进入系统?	225
292. 入侵者进入系统主要有哪几种方式?	226
293. 入侵者为何能闯入系统?	226
294. 入侵者如何获取口令?	227
295. 典型的入侵场景有哪些?	228
296. 入侵有哪些方式?	228
297. NIDS 检测到一个入侵行为后做什么?	229
298. 除了 IDS 外, 还有什么入侵对策?	229
299. IDS 系统应该安放到网络的什么部位?	230
300. 最新病毒有哪些类型?	230
参考文献	235

第1章 病毒基本知识

1. 什么是计算机病毒？

计算机病毒是具有自我复制能力的计算机程序，它能影响计算机软硬件的正常运行、破坏数据的正确与完整，它是一个程序、一段可执行码。就像生物病毒一样，计算机病毒有独特的复制能力，它可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上，当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。

除复制能力外，某些计算机病毒还有其他一些特性：一个被污染的程序能够传送病毒载体。当病毒载体似乎仅仅表现在文字和图像上时，它们可能已经毁坏了文件、再格式化了硬盘驱动或引发了其他类型的灾害。若是病毒并不寄生于一个污染程序，它仍然能通过占据存储空间带来麻烦，并降低计算机的全部性能。

由此，我们可以从不同角度给出计算机病毒的定义：一种是能够实现自身复制且借助一定的载体存在的具有潜伏性、传染性和破坏性的程序；另一种是人为制造的程序，它通过不同的途径潜伏或寄生在存储介质（如磁盘、内存）或程序里，当某种条件或时机成熟时，它会自我复制并传播，使计算机的资源受到不同程度的破坏。

简单地说，计算机病毒就是能够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的、具有对计算机资源进行破坏作用的一组程序或指令集合。

2. 计算机病毒是怎么产生的？

计算机病毒都是人为制造出来的，计算机病毒的主要来源有以下几项：

- (1) 引进的计算机系统和软件中带有病毒；
- (2) 各类出国人员带回的机器和软件染有病毒；
- (3) 购买、使用一些染有病毒的游戏软件；
- (4) 非法拷贝中毒；
- (5) 计算机生产、经营单位销售的机器和软件染有病毒；
- (6) 维修部门交叉感染；
- (7) 有人研制、改造病毒；
- (8) 敌对分子恶意以病毒进行宣传 and 破坏；
- (9) 通过国际计算机网络传入。

3. 计算机病毒有哪些特性？

目前，在世界范围内发现的计算机病毒已超过 1000 种，国内已发现的计算机病毒也

有几十种,例如:“小球”病毒、“大麻”病毒、“黑色星期五”病毒、“雨点”病毒、“磁盘杀手”病毒、“音乐”病毒等。尽管这些病毒各自的传染方式、传染目标不一样,发作条件各异,干扰和破坏程序不同,但是,它们都有如下共同的特性:

(1) 计算机病毒的程序性(可执行性)。计算机病毒与其他合法程序一样,是一段可执行程序,但它不是一个完整的程序,而是寄生在其他可执行程序上,在病毒运行时,与合法程序争夺系统的控制权。计算机病毒只有当它在计算机内得以运行时,才具有传染性和破坏性,甚至会造成系统崩溃,导致计算机瘫痪。

(2) 计算机病毒的传染性。传染性是病毒的基本特征。在生物界,病毒通过传染从一个生物体扩散到另一个生物体,在适当的条件下,它可得到大量繁殖,并使被感染的生物体表现出病症甚至死亡。同样,计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机,在某些情况下造成被感染的计算机工作失常甚至瘫痪。

(3) 计算机病毒的潜伏性。

一个编制精巧的计算机病毒程序,进入系统后可以不马上发作,在几周或者几个月内甚至几年内隐藏在合法文件中,对其他系统进行传染,而不被发现。

潜伏性的第一种表现是不用专用检测程序是检查不出来的,因此病毒可以静静地躲在磁盘或磁带里呆上几天,甚至几年,一旦得到运行机会,就四处繁殖、扩散,继续为害。潜伏性的第二种表现是计算机病毒的内部往往有一种触发机制,不满足触发条件时,计算机病毒除了传染外不做什么破坏。触发条件一旦得到满足,有的在屏幕上显示信息、图形或特殊标识,有的则执行破坏系统的操作,如格式化磁盘、删除磁盘文件、对数据文件做加密、封锁键盘、使系统锁死等。

(4) 病毒的非授权性。

病毒未经授权而执行。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、目的对用户是未知的,是未经用户允许的。

(5) 计算机病毒的破坏性。

所有的计算机病毒都是一种可执行程序,而这一可执行程序又必然要运行,所以对系统来讲,所有的计算机病毒都存在一个共同的危害,即占用系统资源,降低计算机系统的工作效率,其具体情况取决于入侵系统的病毒程序。

同时,计算机病毒的破坏性主要取决于计算机病毒设计者的目的。如果病毒设计者的目的在于彻底破坏系统的正常运行的话,那么这种病毒对于计算机系统进行攻击造成的后果是难以设想的,它可以毁掉系统的部分数据,也可以破坏全部数据并使之无法恢复。但并非所有的病毒都对系统产生极其恶劣的破坏作用。

(6) 病毒的寄生性(依附性)。

病毒程序嵌入到宿主程序中,依赖于宿主程序的执行而生存,这就是计算机病毒的寄生性。病毒程序在侵入到宿主程序中后,一般对宿主程序进行一定的修改,宿主程序一旦执行,病毒程序就被激活,从而可以进行自我复制和繁衍。

(7) 病毒的针对性。

计算机病毒是针对特定的计算机和特定的操作系统的。例如,有针对 IBM PC 机及其

兼容机的，有针对 Apple 公司的 Macintosh 的，还有针对 Unix 操作系统的。例如“小球”病毒是针对 IBM PC 机及其兼容机上的 DOS 操作系统的。

(8) 计算机病毒的可触发性。

病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自己，病毒必须潜伏。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，使病毒继续潜伏。

(9) 病毒的衍生性。

病毒的衍生性为一些有意者提供了一种制造新病毒的捷径。分析计算机病毒的结构可知，传染的破坏部分反映了设计者的设计思想和设计目的。但是，这可以被其他掌握原理的人以其个人的企图进行任意改动，从而又衍生出一种不同于原版本的新的计算机病毒（又称为变种），这就是计算机病毒的衍生性。这种变种病毒造成的后果可能比原版病毒严重得多。

(10) 计算机病毒的持久性。

即使在病毒程序被发现以后，数据和程序以至操作系统的恢复都非常困难。特别是在网络操作情况下，由于病毒程序由一个受感染的拷贝通过网络系统反复传播，使得病毒程序的清除非常复杂。

4. 计算机病毒主要有哪些传播途径？

随着计算机技术的发展，病毒的传播途径也随之多样化起来，但是归纳来讲，主要有以下几种：

第一种途径：通过不可移动的计算机硬件设备进行传播，这些设备通常有计算机的专用 ASIC 芯片和硬盘等；

第二种途径：通过移动存储设备来传播，这些设备包括软盘、磁带等；

第三种途径：通过计算机网络进行传播；

第四种途径：通过点对点通信系统和无线通道传播。

5. 计算机病毒是如何感染文件的？

在系统运行时，病毒通过病毒载体从系统的外存储器进入系统的内存储器，常驻内存。该病毒在系统内存中监视系统的运行，当它发现有攻击的目标存在并满足条件时，便从内存中将自身存入被攻击的目标，从而将病毒进行传播。而病毒利用系统 INT13H 读写磁盘的中断又将其写入系统的外存储器（软盘或硬盘）中，再感染其他系统。

6. 如何确定 Boot 区是否被病毒感染？

正常的 PC DOS 启动过程是：

(1) 开机后进入系统的检测程序并执行该程序对系统基本设备进行检测；

(2) 检测正常后从系统盘 0 面 0 道 1 扇区即逻辑 0 扇区读入 Boot 引导程序到内存的 0000:7C00 处；

(3) 转入 Boot 执行；

(4) Boot 判断是否为系统盘, 如果不是系统盘则提示;

Non-system disk or disk error

Replace and strike any key when ready

否则, 读入 IBM BIO.COM 和 IBM DOS.COM 两个隐含文件;

(5) 执行 IBM BIO.COM 和 IBM DOS.COM 两个隐含文件, 将 Command.com 装入内存;

(6) 系统正常运行, DOS 启动成功。

如果 Boot 区被病毒感染则会出现以下一些现象:

(1) 先用与硬盘上相同版本的干净 DOS 系统软盘启动计算机, 启动过程中, 按 F5 键, 然后用 MEM 或 MI 查看并记下计算机自由内存空间大小; 接着用硬盘引导计算机, 引导过程中, 按 F5 键, 以便跳过 Config.sys 和 Autoexec.bat 中的驱动程序和执行文件, 这时再用 MEM 或 MI 查看计算机的自由内存空间; 如果上述两次自由内存空间大小不一致, 则该计算机的硬盘 Boot 区肯定已被病毒感染。

(2) 用硬盘引导计算机, 运行 DOS 中的 MEM, 可以查看内存分配情况, 尤其要注意基本内存, 一般为 640K, 有的微机为 639K。如果基本内存为 638K、637K 或 636K 等情况, 那么 Boot 区肯定被感染上病毒。

(3) 机器在运行过程中刚设定好的时间、日期, 运行一会儿被修改为缺省的时间、日期, 这种情况下, 系统很可能带有引导型病毒。

(4) 在开机过程中, CMOS 中刚设定好的软盘配置 (即 1.44M 或 1.2M), 用软盘启动时一切正常, 但用硬盘引导后, 再去读软盘则无法读取, 此时 CMOS 中软盘设定情况为 None, 这种情况肯定带有引导型病毒。

(5) 硬盘自引导正常, 但用干净的 DOS 系统软盘引导时, 看不到硬盘如 C\ 盘 (除特殊的需外加驻留内存的大硬盘和 FAT32 位), 这肯定感染上引导型病毒。

(6) Windows 95 经常无法启动, 这很可能带有引导型病毒。

7. 计算机病毒主要存在哪些媒体上?

计算机病毒是一种可直接或间接执行的文件, 是依附于系统特点的文件, 是没有文件名的秘密程序, 但它的存在却不能以独立文件的形式存在, 它必须是以附着在现有的硬、软件资源上的形式而存在的。

微型计算机系统在目前来说永久性存储设备即外存储器主要是磁盘。磁盘包括硬盘和软盘。从存储容量角度来讲, 硬盘容量是一般软盘容量的几百至几千倍, 并且硬盘容量越来越大, 软盘一般为 1.44MB。微型计算机系统所使用的文件存放于磁盘之中, 所以微型计算机的病毒是以磁盘为主要载体的。

8. 计算机病毒的生命周期有多长?

计算机病毒的产生过程可分为: 程序设计-传播-潜伏-触发-运行-实行攻击。计算机病毒拥有一个生命周期, 从生成开始到完全根除结束。

开发期: 在几年前, 制造一个病毒需要计算机编程语言的知识。但是今天有一点计算机编程知识的人都可以制造一个病毒。通常计算机病毒是一些误入歧途的、试图传播计算