

计算机万个为什么丛书

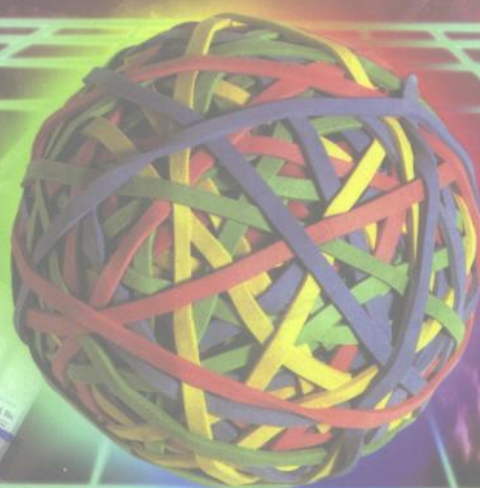
计算机万个为什么丛书

JISUAN JI WAN GE WEI

DI CONG SHU

计算机病毒

庾光蓉 李卫 张光祥 主编



电子科技大学出版社

声 明

本书无四川省版权防盗标识，不得销售；版权所有，违者必究，举报有奖，举报电话：
(028) 6636481 6241146 3201496

JS202/26

计算机万个为什么丛书

计 算 机 病 毒

庾光蓉 李 卫 张光祥 主编

出 版：电子科技大学出版社 (成都建设北路二段四号：邮编,610054)

责任编辑：汤云辉

发 行：电子科技大学出版社发行

印 刷：四川建筑印刷厂

开 本：787×1092 1/16 印张 13.25 字数 319 千字

版 次：1999 年 6 月第 1 版

印 次：1999 年 6 月第 1 次印刷

书 号：ISBN 7—81065—045—9/TP·23

印 数：1—3000 册

定 价：15.00 元

前 言

在科学技术飞跃发展的今天，电子计算机、电脑越来越引人注目，目前它在科研、工业、自动化、通讯、工程设计、办公自动化、教育、信息处理等多方面都得到广泛的应用，正逐步普及到家庭。

在我们学习计算机的时候，常会听到一些行家们大谈计算机病毒，仿佛每一天都会有各种各样的电脑病毒从我们身边冒出来一样。然而不知你是否冷静想过：“电脑病毒”到底是个什么东西呢？

计算机病毒是一种最为奇特的人类智慧的结晶，但它给信息处理造成广泛、深刻的负效应。

西方国家把病毒作者、网络非法入侵者称做“hacker”。在病毒出现之前 hacker 就存在。只有那些对计算机内部细节了如指掌，无所不知的人才能获此称谓。Robert T. Morris 是著名的 hacker。1988 年 11 月 2 日，年仅 23 岁的 Morris 编写的蠕虫，打入美国的 Internet 网络，致使网络崩溃，震惊全世界，闯下大祸。IBM 公司的密码专家曾花费 18 个月时间，研究 DES 密码的破译方法，未获成功。Morris 单枪匹马破解了用 DES 加密的口令字，成功地非法侵入了网络。专家们评论：hacker 们有双重性，是难得的人才又是可以造成巨大灾难的人。

全世界发现病毒种类超过 10 000 种，在反病毒斗争中，人们将面临如此庞大而且还在不断增殖的病毒群体，要和数以千计的 hacker 做知识较量。

病毒像一个幽灵在计算机世界游荡。

多态性病毒是病毒中的“千面人”，所有用常规病毒特征代码法的 SCAN 类工具都不能识别它。

破坏性感染病毒，在依附到宿主程序上的同时，吞食掉宿主程序的某些肢体，成为杀毒工具不可逾越的障碍。

中间插入型病毒，伴侣型病毒，病毒相生现象，给反病毒提出了一个又一个难题。

病毒自动生成技术的出现和传播，使病毒的生成由手工转向自动，如果说手工生成的病毒是一股涓涓细流，自动生成的病毒将使之变成波涛汹涌的病毒海洋。

本书采用问答式科普说明、讲解的方法，为你介绍有关病毒的基础知识和一些专业理论。既能为初涉及电脑的人揭开“病毒”的神秘面纱，又能满足较高层次人士提高的需求。

我们还编入了一些有关电脑的其他基础理论知识，希望对你了解掌握电脑能起到一臂之力。

最后，我们真诚希望读者都能通过阅读与实践来学习我们的经验，提高电脑用户的知识水平。

编 者

1999 年 3 月

目 录

第 一 篇

1. 病毒的起源是什么?	(1)
2. 病毒有哪些大事记?	(2)
3. 病毒发展的年表是怎样的?	(5)
4. 计算机系统的安全可能受到哪些方面的威胁?	(6)
5. 由于计算机系统较脆弱,在设计系统时,应重要考虑哪些因素?	(6)
6. MS-DOS 在计算机安全方面的不足是什么?	(7)
7. 计算机病毒的起源是什么?	(7)
8. 冯·诺依曼体系与计算机病毒之间有什么关系?	(9)
9. 信息共享与计算机病毒有什么关系?	(9)
10. 病毒的定义是什么?	(10)
11. 什么是 Fred·Cohen 定义?	(10)
12. 什么是 Dean Dennis Longly 和 Michael Shein 定义?	(10)
13. 对病毒的定义,还有什么其他论点?	(11)
14. 怎样理解 Fred·Cohen 定义?	(11)
15. 病毒的基本特性有哪些?	(12)
16. 病毒有哪些一般特性?	(14)
17. 计算机病毒由哪几部分构成?	(15)
18. 为说明病毒程序的结构,能否给出一种病毒程序例?	(16)
19. 能否再给出一具体病毒程序例?	(17)
20. 计算机病毒按感染方式分类是怎样的?	(18)
21. 病毒按功能是怎样分类的?	(19)
22. 病毒按感染能力是怎样分类的?	(20)
23. 病毒按感染目标分类是怎样的?	(20)
24. 病毒按链接方式是怎样分类的?	(21)
25. 什么是链式病毒?	(22)
26. 什么是计算机细菌?	(22)
27. 病毒感染目标有哪些?	(23)
28. 病毒感染的一般过程是怎样的?	(23)
29. 病毒宿主程序分为几类及其控制权是什么?	(24)
30. 病毒常驻内存的特点有哪些?	(25)

31. 什么是病毒修改中断?	(25)
32. 病毒感染后长度变化是怎样的?	(26)
33. 病毒感染分为哪两种?	(27)
34. 什么是寄生感染和滋生感染?	(29)
35. 什么是综合感染?	(30)
36. 什么是交叉感染?	(30)
37. 什么是插入感染?	(31)
38. 什么是逆插入感染?	(32)
39. 什么是替代感染?	(32)
40. 什么是携带感染?	(32)
41. 什么是链式感染?	(33)
42. 什么是零长度感染?	(34)
43. 什么是破坏性感染?	(35)
44. 什么是系统隐含文件的感染?	(35)
45. 病毒的基本特性是什么?	(36)
46. 病毒按知名度分类法分是怎样的?	(36)
47. 病毒触发条件是什么?	(36)
48. 病毒采用日期做触发条件的情况有哪些?	(37)
49. 时间触发有哪些方式?	(38)
50. 键盘触发有哪些类型?	(38)
51. 病毒的感染触发方式有哪些?	(39)
52. 什么是病毒的启动触发?	(40)
53. 什么是访问磁盘次数触发?	(40)
54. 什么是调用中断功能触发?	(40)
55. 什么是CPU 型号触发?	(41)
56. 如何分析FLIP 病毒激活条件?	(41)
57. 计算机病毒的破坏行为有哪些?	(42)
58. 攻击系统数据区是怎么回事?	(42)
59. 攻击文件是怎么回事?	(44)
60. 如何删除文件?	(44)
61. 如何更改文件名?	(44)
62. 如何替换内容?	(45)
63. 如何丢失部分代码?	(45)
64. 如何致内容颠倒?	(45)
65. 如何将写入时间变空白?	(45)
66. 如何变碎片?	(46)
67. 如何假冒文件?	(46)
68. 如何丢失文件簇?	(46)
69. 如何攻击数据文件?	(46)

70. 攻击内存是怎么回事?	(47)
71. 如何占用大量内存?	(47)
72. 如何改变内存总量?	(47)
73. 如何禁止分配内存?	(47)
74. 如何蚕食内存?	(48)
75. 干扰系统的运行是怎么回事?	(48)
76. 如何不执行命令?	(48)
77. 如何干扰内部命令的执行?	(49)
78. 如何虚假报警?	(49)
79. 如何致打不开文件?	(49)
80. 如何致内部栈溢出?	(49)
81. 如何占用特殊数据区?	(50)
82. 如何换现行盘?	(50)
83. 如何致时钟倒转?	(50)
84. 如何致重新启动?	(50)
85. 如何致死机?	(51)
86. 如何强制游戏?	(51)
87. 如何扰乱串、并行口?	(51)
88. 速度下降是怎么回事?	(51)
89. 攻击磁盘有哪些方式?	(52)
90. 扰乱屏幕显示有哪些方式?	(52)
91. 什么是字符跌落?	(52)
92. 什么是环绕方式?	(53)
93. 什么是倒置方式?	(53)
94. 什么是显示前一屏?	(53)
95. 什么是光标下跌?	(53)
96. 什么是滚屏呢?	(53)
97. 抖动又是什么呢?	(54)
98. 病毒乱写屏幕又是怎么回事?	(54)
99. 病毒吃字符是怎么回事?	(54)
100. 病毒干扰键盘操作方式有哪些?	(54)
101. 什么是响铃方式?	(55)
102. 病毒如何封锁键盘?	(55)
103. 病毒如何换字?	(55)
104. 如何抹掉缓存区字符?	(55)
105. 病毒如何重复呢?	(55)
106. 病毒如何使输入紊乱?	(56)
107. 喇叭有几多?	(56)
108. 病毒怎样“演奏曲子”?	(56)

109. 病毒如何放警笛声?	(56)
110. 为何电脑中传出“炸弹噪声”?	(57)
111. 还有什么病毒怪声呢?	(57)
112. 病毒如何攻击 CMOS?	(57)
113. 病毒怎样干扰打印机?	(57)
114. 病毒演化是怎么回事?	(58)
115. 病毒演化的后果是什么呢?	(58)
116. 为何谨慎处理病毒样本?	(59)
117. 病毒变种的缘由是什么?	(59)
118. 病毒变种类型有哪些?	(59)
119. 病毒家族知多少?	(60)
120. Vienna 病毒家族是怎样的?	(60)
121. Jerusalem 家族是怎样的?	(61)
122. Jerusalem 病毒触发条件有哪些?	(62)
123. Jerusalem 病毒的杀伤作用如何?	(62)
124. Jerusalem 病毒为什么对 COM 文件是单次感染而对 EXE 文件则是重复 感染呢?	(62)
125. 该病毒有哪些变种特征?	(62)
126. 如何识别病毒家族?	(63)
127. 什么是病毒相克——互相攻击?	(63)
128. 什么是病毒相生——互相救助?	(64)
129. 病毒采用密码技术有哪些作用?	(65)
130. 你知道密码概念吗?	(65)
131. 密码系统的种类有哪些?	(66)
132. 对称型密码系统的使用方法是怎样的?	(67)
133. 什么是 DES 密码系统?	(67)
134. 公开密钥系统有哪些优点?	(67)
135. 什么是“蠕虫”?	(67)
136. 什么是 Arpanet 网络?	(68)
137. 蠕虫工作原理是怎样的?	(69)
138. 想知道蠕虫入侵一瞬是怎样的吗?	(70)
139. 蠕虫的蔓延过程是怎样的?	(70)
140. 如何消除莫里斯蠕虫?	(71)
141. 莫里斯蠕虫的经济损失知多少?	(71)
142. 审判中的新问题是什么?	(72)
143. 莫里斯事件的反响有哪些?	(72)
144. 病毒的隐蔽技术和欺骗行为是怎样的?	(72)
145. 何为变化隐蔽?	(73)
146. 何为脱皮技术?	(73)

147. 何为病毒自杀?	(74)
148. 何为病毒密码?	(74)
149. 隐蔽型病毒病例——4096 病毒是怎样的?	(74)
150. 隐蔽技术有什么危害呢?	(75)
151. 病毒技术有哪些新动向?	(75)
152. 什么是隐蔽型病毒?	(76)
153. 什么是多态性病毒?	(76)
154. 什么是病毒自动生成技术?	(77)
155. 什么是超级病毒?	(78)
156. 什么是破坏性感染病毒?	(78)
157. 什么是反病毒技术?	(79)
158. 什么是一般预防对策?	(79)
159. 病毒征兆有哪些?	(80)
160. 怎样进行反病毒处理?	(82)
161. 病毒诊断的原理是什么?	(82)
162. 什么是长度检测法?	(83)
163. 什么是病毒签名检测法?	(83)
164. 什么是特征代码段检测法?	(84)
165. 病毒的消除是怎么回事?	(84)
166. 如果受到病毒感染, 如何治疗呢?	(84)
167. 为什么要剖析病毒样本?	(85)
168. 怎样研制病毒试验样本?	(86)
169. COM 型文件的治疗是怎样的?	(87)
170. EXE 型文件的治疗?	(87)
171. 免疫处理是怎么回事?	(88)
172. 病毒的预防是怎么回事?	(88)
173. 简单的预防方法是怎样的?	(89)
174. 如何对软件的试验生产过程控制?	(90)
175. 软件备份是什么样子的?	(90)
176. 控制输入输出是怎么回事?	(90)
177. 为何要谨慎选择工作人员?	(91)
178. 反病毒工具是怎么回事?	(91)
179. 反病毒工具自身安全是怎样的?	(91)
180. 使用检测病毒工具的要点是什么?	(92)
181. 为什么使用消除病毒工具要谨慎?	(92)
182. 理想的反病毒工具是什么?	(93)
183. 病毒检测方法有哪些?	(93)
184. 什么是特征代码法?	(93)
185. 什么是校验和法?	(94)

186. 什么是行为监测法?	(95)
187. 对多态性病毒的检测方法是什么?	(96)
188. 什么是感染实验法?	(96)
189. 病毒检测实验应注意什么?	(97)
190. 怎样使用 DEBUG 检测病毒?	(97)
191. 怎样检测 BOOT 扇区病毒?	(98)
192. 怎样检测 COM 文件病毒?	(98)
193. 怎样检测 EXE 文件病毒?	(99)
194. 什么是病毒的消除?	(100)
195. 什么是引导型病毒的消毒?	(100)
196. 什么是文件型病毒的消毒?	(100)
197. 什么是交叉感染时的消毒?	(101)
198. 怎样给 EXE 型文件交叉感染消毒?	(101)
199. 怎样给 COM 型文件交叉感染消毒?	(101)
200. 病毒治疗软件研制的情况如何?	(102)
201. 什么治疗工具 Clean-up?	(102)
202. 病毒治疗实验的方法有哪些?	(103)
203. Jerusalem-B 病毒的特征有哪些?	(106)
204. Jerusalem-B 病毒的工作原理是什么?	(106)
205. Jerusalem-B 病毒的诊断方法是什么?	(107)
206. Jerusalem-B 病毒的治疗方法?	(108)
207. 什么是 Vienna 病毒?	(108)
208. Vienna 病毒 A 型和 B 型版本的差异是什么?	(108)
209. Vienna 病毒的诊断方法有哪些?	(109)
210. 对维也纳病毒的治疗方法有哪些?	(109)
211. 什么是 1701/1704-B 病毒 (雨点)?	(110)
212. 1701/1704-B 病毒的特征是什么?	(110)
213. 1701/1704-B 病毒的诊断方法有哪些?	(110)
214. 怎样治疗 1701/1704-B 病毒?	(110)
215. 什么是 YanRee Doodle (扬基歌) 病毒?	(111)
216. 4096 病毒 (100 年) 是什么?	(111)
217. Ping Pong (小球) 是什么?	(113)
218. Ping Pong 诊断方法是什么?	(113)
219. Ping Pong 的治疗方法是什么?	(114)
220. Mari juana (大麻) 病毒的有关知识是什么?	(116)
221. 如何进行病毒预防?	(117)
222. 硬件引导的数据病毒有哪些?	(117)
223. 怎样使用 DEBUG 保存硬盘主引导扇区?	(118)
224. 怎样使用 DEBUG 保存硬盘的 FAT 表、文件目录?	(121)

225. 如何使用 Mirror 命令?	(122)
226. 如何进行硬盘系统数据修复?	(123)
227. 如何回写硬盘主引导扇区?	(123)
228. 怎样回写硬盘 Boot 扇区?	(124)
229. 怎样回写硬盘 FAT 表、根目录?	(124)
230. 如何使用 Unformat?	(125)
231. 什么是磁盘读写监视?	(125)
232. 什么是行为准则监视技术?	(125)
233. 什么是病毒行为和误报警?	(126)
234. 什么是 CD-ROM 光盘——病毒新载体?	(126)
235. 什么是 hacker?	(127)
236. 病毒检查技术有哪些局限?	(128)
237. 什么是隐蔽性病毒技术?	(128)
238. 什么是多态性病毒技术?	(129)
239. 什么是插入型病毒技术?	(129)
240. 什么是超级病毒?	(130)
241. 什么是病毒检测工具的杀手——病毒自动生产技术?	(130)
242. 什么是杀毒工具的困惑——破坏性感染病毒?	(131)
243. 对反病毒技术有哪些期望?	(131)
244. 入侵 Boot 扇区的病毒 Disk killer 是怎么样的?	(132)
245. Disk Killer 的内容是什么?	(132)
246. Disk Killer 身首接合阶段是怎么样的?	(132)
247. Disk Killer 拦截中断阶段情况如何?	(135)
248. Disk Killer 读入与运行 DOS Boot 阶段是怎么一回事?	(136)
249. Disk Killer 的核心 ISRS 的内容是什么?	(136)
250. KINT-8H/9H 子程序是怎么回事?	(136)
251. KINT-13H 子程序的内容是什么?	(138)
252. 什么是 LOAD-PT-BT 子程序?	(142)
253. 病毒执行感染的部分是怎样的?	(144)
254. HD-MAKER 感染硬盘是怎么回事?	(145)
255. FLP-MAKER 感染软盘是怎么回事?	(147)
256. GET-CLUS 是怎样的?	(150)
257. 什么是 Disk Killer 的破坏行为?	(155)
258. Disk killer 的遗传指什么?	(155)
259. Disk killer 头部里的基因有哪些?	(155)
260. 决定潜伏期的基因有哪些?	(155)
261. Disk killer 类病毒的通性是什么?	(156)
262. Disk killer 为什么不掩护同族?	(156)
263. 为什么 Disk killer 具有侵略性?	(157)

264. 如何提防 Disk killer 的进化、变体?	(158)
265. 什么是计算机病毒的自然淘汰?	(158)
266. 关于 Int 9h? 的探讨?	(158)
267. 热启动具有怎样的潜在危险?	(159)
268. 入侵 Pre-Load 扇区的病毒 Stone 是怎样的?	(160)
269. Stone 是怎样启动的?	(160)
270. Stone 病毒的启动流程是怎样的?	(160)
271. Stone 的启动信息是什么?	(161)
272. Stone 如何感染硬盘?	(161)
273. Stone 如何感染软盘?	(162)
274. Stone 对磁盘有什么影响?	(163)
275. Stone 的传染力怎样?	(165)
276. 为何要提防 Stone 的变种?	(165)
277. CIH 是一种什么样的病毒?	(165)
278. CIH 病毒何时被发现的?	(166)
279. CIH 病毒发现时是如何处理的?	(166)
280. CIH 病毒真的能对硬件进行破坏吗?	(166)
281. 用户能自己修复吗?	(166)
282. 用户能自己修复数据吗?	(167)
283. 目前有好的防犯该病毒的方法吗?	(167)
284. 目前有好的查杀 CIH 病毒的方法吗?	(167)
285. CIH 病毒为什么能破坏计算机硬件?	(167)
286. 早期采用 EPROM 的计算机可以避免 CIH 病毒攻击吗?	(168)
287. 目前对于用户来说, 对 CIH 病毒有什么预防的办法吗?	(168)
288. 为什么说 CIH 病毒是硬件升级软件化的一枚苦果?	(168)
289. 2000 问题到底是什么?	(169)
290. 2000 问题涉及哪些方面?	(170)
291. 各国解决 2000 年问题的行动有哪些?	(171)
292. 对于 Y2K 还应注意些什么问题?	(172)
293. Y2K 有哪些免费软件?	(173)
294. 怎样发现网络服务器的千年问题?	(173)

第 二 篇

295. PC 机常见软故障分析及解决对策是什么?	(174)
296. 为何 DOS 版本不兼容?	(174)
297. 系统配置错误有哪些?	(175)
298. 使用操作不当表现在哪里?	(175)
299. 硬盘建立不当是怎么回事?	(175)

300. 硬盘因感染病毒而不能引导系统是怎么回事?	(176)
301. 如何对硬盘数据进行日常维护?	(176)

第 三 篇

302. 如何使用微机及其一些维护常识?	(178)
303. 数据保护的的经验有哪些?	(178)
304. WPS 的一些特殊使用技巧是什么样子的?	(181)
305. WPS 加密文件的解密方法是什么?	(182)
306. 目录管理有什么技巧?	(183)
307. 怎样使用与维护软盘?	(183)
308. 如何恢复 0 磁道损坏软盘中的信息?	(185)
309. 如何使用新到手的软件?	(185)
310. 什么是操作系统, 汉字输入类软件?	(186)
311. 应用工具类软件有哪些?	(187)
312. 磁盘拷贝、加密类软件有哪些?	(187)
313. 测试验机类软件有哪些?	(188)
314. 计算机辅助设计绘图类软件有哪些?	(188)
315. 查消病毒类软件有哪些?	(188)
316. 压缩扩容工具类软件有哪些?	(188)
317. 翻译、英语学习类软件有哪些?	(188)
318. 打字、键盘类软件有哪些?	(189)
319. 发声类软件有哪些?	(189)
320. 程序语言类软件有哪些?	(189)
321. 数据库及管理类软件有哪些?	(189)
322. 编辑类、排版类软件有哪些?	(189)
323. 视窗类软件有哪些?	(190)
324. 网络通讯类软件有哪些?	(190)
325. 资料信息库类软件有哪些?	(190)
326. 打印、仿真类软件有哪些?	(190)
327. 转化类软件有哪些?	(190)
328. 教育、CAI 类软件有哪些?	(190)
329. 其他类的软件还有哪些?	(191)

参 考 篇	(192)
-------------	-------

第一篇

1. 病毒的起源是什么?

1988年11月2日下午5时1分59秒,美国康奈尔大学的计算机科学系研究生,23岁的莫里斯(Morris)将其编写的蠕虫程序输入计算机网络。在几小时内导致Internet网络堵塞。这个网络连接着大学、研究机关的155 000台计算机,这些计算机用于与美国军方交换和搜集非保密数据。

莫里斯的蠕虫程序感染了约6000台计算机,使网络堵塞,运行迟缓。莫里斯因计算机欺诈和滥用罪,成为依据1986年制定的计算机安全法被地方法院起诉的第一个计算机犯罪者。如果起诉有效,他将被判处五年监禁和250000美元罚款。

美国当局对莫里斯的起诉果断而迅速,是有原因的。首先这一事件导致了国家的大计算机网络堵塞,成为报纸的头版新闻,轰动了美国社会。其次,受到美国一些国会议员的政治压力,他们自信在两年前刚刚通过了一个有效的计算机安全法。最后是来自某些计算机专家的歇斯底里的义愤。

而最主要的原因可能是莫里斯的父亲是美国高级情报和安全机关——国家安全局(NSA)的高级计算机专家,他有能力为儿子求情使之逃避起诉。

莫里斯的蠕虫就像是计算机世界的一次大地震,引起巨大反响,震惊了全世界,引起了人们对计算机病毒的恐慌,也使更多的计算机专家重视和致力于病毒研究。

美国的一些计算机专家在事件发生后,仔细剖析了莫里斯的蠕虫程序,对其性质和行为做了深入研究。对蠕虫事件的后果做了比较全面公正的评价。在指出其危害的同时,认为蠕虫程序揭露了国家计算机网络存在的漏洞,并引起了计算机界对病毒构成的潜在威胁的普遍重视。

莫里斯的蠕虫程序在全世界刮起了一场旋风,激起舆论界和科技界对计算机病毒的普遍关注。

莫里斯不是计算机病毒的始创者,美国的计算机专家B. Meeks指出:计算机病毒可能已有二十多年的历史了。美国军方研究计算机病毒已经十多年了。只是莫里斯事件发生后,病毒才被公开,成为受人关注的问题。

美国著名的计算机安全专家Frederick B. Cohen在加利福尼亚大学作博士论文时,就研究了计算机病毒,以求寻找一种方法防御那些能自身繁殖的程序。Cohen发现防御它们几乎不可能。Cohen使用了DECVAX计算机和Univac 1108计算机,他发现在关键的几分钟里病毒就可在计算机内传播。

Cohen关于病毒的研究成果于1984年首次在国际计算机安全会议上发表。

1986年Rudiger Dierstein等人在法国巴黎召开的计算机安全会议上发表了论文“计算

机病:潜在的威胁”。

2. 病毒有哪些大事记?

如果从1946算起,电子计算机问世已经近50年了。计算机病毒的有据可查的历史已经二十多年。1972年在ARPAnet网络上发现了世界上第一例病毒。1986年1月发现IBM PC机上的第一例病毒、计算机病毒多数是运行在微型机上,随着IBM PC机的普及不断蔓延,以后波及APPLE公司的Macintosh机种,继而又入侵了日本NEC公司的PC系列机种。1989年1月时,病毒不足100种,1990年1月超过150种,1990年12月时,已超过260种。1994年夏,据资料介绍,已发现文件型病毒4500种,引导型病毒350种,病毒总数已近5000种。

对病毒的发展历史,作精确描述是很困难的。根据笔者掌握的资料,将病毒发展中的重大事件叙述如下,从中可以看出病毒发展的梗概。

(1) Creeper 病毒事件

80年代初发现的最早的一例病毒。在ARPAnet网络上扩散。在终端上显示:I'm the creeper, catch me if you can!

早期版本只有繁殖功能,而后变成边繁殖边传播。人们开发了Reaper反病毒工具,抑制了该病毒。

(2)1984年9月Frederick B. Cohen在加利福尼亚大学读博士学位时,将所做的自我繁殖程序称为计算机病毒,首次在美国安全学术会议上发表其研究成果,并警告此种技术可以简单地突破当时的安全技术。

(3)1986年1月在巴基斯坦的拉合尔,Basit和Amjacl兄弟二人为防止非法拷贝编制了世界第一例IBM PC机病毒“巴基斯坦病毒”,也是世界上罕见的写有病毒作者的姓名、住址的病毒。初期版本只感染软盘,后来的变种也感染硬盘了。

病毒含有如下信息:

WELLCOME TO THE DUNGEON.

BEWARE OF THIS VIRUS.

CONTACT US FOR VACCINATION.

在扩散过程中,几经改动变成具有破坏性的病毒。

(4)1987年2月加拿大出现首例Macintosh机病毒“Peace”,又名“MacMag”。该病毒是由加拿大的Mac Mag杂志的主编Richard Brandow主持,由其雇员Drew Davidson编制。在1988年3月之前,病毒感染扩散,1988年3月2日显示:

“a Peace on Earth message”.

病毒将自身删除。

(5)1987年7月在汉堡发现“n VIR”病毒。这是有多个变种的Macintosh病毒。当系统程序一被感染,就在病毒内设置初始值为1000的计数器,每次机器启动或执行染毒程序时,计数器分别减1或2。当计数器为0时,偶而蜂鸣器响。

(6)1987年9月在美国的达拉斯发现Macintosh机上的“SCORE”病毒,是某编程人员为了攻击他在以前工作的公司中所编写的两个程序而开发的。该病毒在系统中生成了两个

隐蔽文件“SCORE”和“Desktop”。病毒可以导致速度下降、打印障碍和系统崩溃。

(7)1987年11月在美国宾夕法尼亚州的勒海大学发现MS-DOS系统的“勒海”病毒。它采用特殊手法感染,染毒后的文件长度不变。变种内部有计数器,感染一定次数后,破坏BOOT和FAT区。

(8)1987年11月发现Amiga病毒“SCA”

它是为数不多的Amiga病毒的一种。英国、澳大利亚、美国发现感染事件,在Amiga系统的Boot区感染后,显示下述信息:

Something wonderful has happened.

Your Amiga is alive and even better!!!

Some of your disks are infected by VIRUS.

Another masterpiece of the Maga-Mighty SCA.

显示信息后,程序或数据被破坏。该病毒的变种有Byte Bandito。

(9)1987年11月在以色列的希伯来大学发现“Jerusalem”病毒(又名PLO)

它是13日星期五发病的MS-DOS病毒的原型。病毒设计者将病毒设计成1988年5月13日发作,这一天恰好是以色列占领巴勒斯坦的40周年纪念日,致使希伯来大学数千台微机染毒,速度变慢。1988年5月13日世界各地许多该病毒变种发作,这些变种不管年份,只要是13日星期五便会发作。由于该病毒选择的发病日期及把以色列计算机作为攻击目标,所以又名PLO病毒。似乎病毒的设计者有明显的政治目的。

(10)1987年12月西德的BIT net网络发现“Christmas Tree”病毒,即圣诞树病毒。实质是攻击IBM国际通信网络BIT net中的IBM终端的蠕虫。它乱用电子邮件网络中传送一颗圣诞树图案及下述信息:

A Very Happy Christmas and Many Best Wishes for the new Year.

Let this run and enjoy yourself.

Browsing this file is no fun at all.

Dust type "CHRISTMAS"

上述信息在通信网络中各处传送,使网络速度下降,受害达72小时之久。

(11)1988年2月“Peace”病毒感染磁盘事件

“Peace”病毒侵入美国的阿鲁达斯公司的生产线,该公司发现已出售的图形软件“Free Hard”被“Peace”病毒感染,公司被迫将5000套染毒软盘回收。

(12)1988年3月“SCORES”病毒侵入NASA事件

1987年3月发现的“SCORES”病毒侵入美国宇宙航空局(NASA)的计算机网,感染了200台Macintosh微机。

(13)1988年3月“Flu-Shot4”病毒假冒“Flu-Shot”反病毒工具事件

有人用“Flu-Shot4”病毒在计算机通信网络中冒充的反病毒工具“Flu-Shot”的新版本。实质是IBM PC机的MS-DOS病毒。

(14)1988年4月美国阿拉梅达大学“Alameda”病毒事件

美国加利福尼亚州阿拉梅达的梅立特学院首次发现“Alameda”病毒。是采用欺骗技术的引导型病毒,它可以截获CTRL-ALT-DEL组合键,在热启动的场合下,能使病毒仍能驻留在内存中,同时能感染系统盘和非系统盘。病毒可以使运行速度下降,使系统崩溃,是一

种较高技术层次的引导型病毒。

(15)1988 年 5 月美国通讯社“巴基斯坦”病毒发作事件

1986 年 1 月在巴基斯坦发现的“巴基斯坦”病毒,入侵美国康涅狄格州罗德兰岛的 The Providence Journal Britten 新闻通讯社。记者的原稿数据全部被破坏,不能读出。

(16)1988 年 6 月日本 NEC 公司的 PC-VAN 事件

日本的微机通信网络 PC-VAN 发生盗窃识别口令事件。在多个成员收到的以电子信件方式送来的程序中混入了病毒。染毒程序一运行便感染 COMMAND.COM,每当工作站进行读写时,被加密的识别口令便会自动写入电子告示板的某个插板中。而后病毒作者对密码化的识别口令进行解密并乱用。该病毒迫使日本 NEC 公司开始执行微机安全对策计划,并激发了微机用户对病毒的保护意识。

日本 NEC 公司的 PC 系列微机,虽然也使用 MS-DOS,但与 IBM PC 机及其兼容机的 MS-DOS 不同,IBM PC 机的软件不能在日本 NEC 公司的 PC 系列机上运行。病毒入侵日本 NEC 公司的 PC 系列微机标志着病毒又步入了一个新机种。

(17)1988 年 11 月 ARPAnet 网络 Internet 事件

美国康奈尔大学 23 岁的研究生罗伯特·莫里斯编写的蠕虫程序入侵美国的大规模 Internet 网络,连接该网的美国各地的研究所、大学的 6000 台计算机被击中,它是攻击 SUN 和 VAX 的 UNIX 蠕虫。

(18)1989 年 10 月 WANK 袭击 DECnet 网络

“WANK”是袭击 DECnet 网络中 VAX 机的蠕虫。美国的 NASA、日本的 HEPnet 网都发现它入侵一些研究所、大学。

(19)1989 年 12 月混有病毒的艾滋病信息软盘邮送敲诈事件

美国的人类学博士鲍伯编制了有关医学艾滋病信息磁盘,其中暗含病毒,将磁盘由巴拿马的西布格公司免费邮送世界各地,数量逾万片。在说明书中要挟用户使用前必须向西布格公司预付 378 美元,否则将损害用户的其他程序。肯尼亚的一些大机关机器染毒,英国、南非、津巴布韦也发现了该种病毒。它是波及全世界多个国家的用病毒做恐怖活动的恶性事件。

(20)1990 年 1 月“4096”隐蔽型病毒问世

1990 年 1 月在以色列发现首例隐蔽型病毒“4096”。该病毒在感染文件的目录年值上增加 100,故又名“100 年病毒”,采用了高超的欺骗技术。对系统用户讲,它几乎是不可见的。病毒程序被访问时,病毒自身可以将病毒代码从文件脱出难于发现。不仅攻击程序而且攻击数据文件,狡猾而凶狠。

(21)1991 年发现“GPI”首例病毒

该病毒是对付 NOVELL 公司 Netware 的病毒,是以色列(Jerusalem)病毒的变种,冲破了网络 OS 的安全机制,进行了感染。

(22)1992 年 3 月米开朗基罗病毒冲击世界

瑞典、荷兰于 1991 年 4 月发现米氏病毒之后一年间,该病毒在全世界广泛蔓延。由于美国著名的反病毒公司 McAfee Association 的经理 Mr. John McAfee 预先对全世界发出警告,1993 年 3 月 6 日该病毒发作时,被害程度比预想轻。

(23)1992 年多态性病毒的突起

从1990年起,病毒每次感染时突然改变形态的新型病毒逐渐增加。1992年此类病毒的增加特别明显。在保加利亚开发出多态性发生器是编制病毒时使用的程序模块。最著名的最早的多态性病毒是“黑夜复仇者——Dark Avenger”。

(24)1992年病毒生产工具“VCL”在美国的传播

VCL是Vincs Creation Laboratory的缩写。是生成病毒用的软件工具,有人通过美国的计算机通信网络散布了此工具。它可以按照用户的要求选择感染、潜伏、发病方式生成用户所想要的病毒。使病毒的生成摆脱了完全依赖于手工,进入了计算机辅助的阶段。

(25)1992年9月发现首例Windows病毒

在芬兰发现只感染Windows应用程序的病毒。发现后,由于各反病毒厂家迅速采取应对措施,该病毒未能大范围扩散。

(26)1993年4月美国的Microsoft公司与反病毒厂家联手合作

美国Microsoft公司在MS-DOS6.0版本中纳入了反病毒厂家Central Point公司的反病毒工具,包括静态检测工具,常驻程序。在MS-DOS6.0的非常驻命令Format中也采取了特殊策略,在格式化后可以不丢失原有文件,这些都反应了病毒危害的深刻程度已影响到操作系统的设计。

3. 病毒发展的年表是怎样的?

(1)1972年:“Creaper”事件

(2)1984年:F. B. Cohen博士发表病毒研究论文

(3)1986年:发现首例IBM PC病毒“Pakistani”

(4)1987年:

- 发现首例Macintosh机病毒“Peace”
- 发现感染后长度不变的“Leihigh”病毒
- 发现Amiga病毒“SCA”
- 以色列发现“PLO”病毒
- 西德BIT网络“Christmas”病毒事件

(5)1988年:

- “Peace”病毒混入美国阿鲁达斯公司售出的大量磁盘
- “SCORE”病毒入侵美国宇航局NASA
- “Flu-Shot4”病毒假冒反病毒工具“Flu-Shot”事件
- 发现隐蔽型引导病毒“Alameda”
- 巴基斯坦病毒在美国新闻通讯社发病
- 美国首次判决病毒作者有罪
- 病毒入侵苏联政府的80台机器
- 莫里斯蠕虫入侵Internet网

(6)1989年:

- “Jerusalem”病毒使英国数百用户受损
- “Datacrime1、2、3”在荷兰感染10万台计算机