北京科海培训中心

计算机病毒与反病毒技术

张汉亭 编著

清华大学出版社

计算机病毒与反病毒技术

清华大学

北京科海培训中心

计算机病毒与反病毒技术

张汉亭　编著

清华大学出版社

(京)新登字 158 号

内 容 提 要

本书作者积多年反病毒技术研究的经验，从数千种病毒中概括了病毒的感染、触发及破坏行为；通过跟踪、剖析病毒的新技术，如隐蔽性病毒、链式病毒、伴侣病毒、多态形病毒、超级病毒、病毒自动生成技术等；进一步阐述病毒家族关系，病毒相生、病毒相克现象。

针对病毒技术的新动向，介绍了各种反病毒技术，其中包括使用 CD-ROM 光盘所应注意事项。通过本书使读者对病毒有较深刻的认识，以便及早发现和防范病毒。

本书供工程技术人员以及大专院校师生作为全面了解与处理计算机病毒的技术参考书。

书　名：计算机病毒与反病毒技术
编　者：张汉亭
出版者：清华大学出版社(北京清华大学校内，邮编 100084)
印刷者：北京朝阳科普印刷厂印刷
发　行：新华书店总店北京科技发行所
开　本：16　印张：16　字数：386 千字
版　次：1996 年 5 月第 1 版　1996 年 12 月第 2 次印刷
印　数：5001～8000
书　号：ISBN 7-302-01603-8/TP・1088
定　价：22.00 元

前　言

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，打入了美国的 Internet 网络，致使网络崩溃，震惊了全世界，闯下了大祸。IBM 公司的密码专家曾花费 18 个人-年，研究 DES 密码的破译方法，未获成功。Morris 单枪匹马破译了用 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。

据资料介绍，1994 年夏，全世界已发现 4500 种文件型病毒，350 种引导型病毒，病毒种类已近 5000 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。

如果用户不了解病毒，常使正常工作难以维持。为普及病毒知识，谨将此书献给读者。如果能对读者有所帮助，笔者将感到欣慰。欢迎读者对书中错误之处，不吝指正。

成书过程中，曾得到郭剑昆、白淑英同志的鼓励与支持，谨向他们致以深切谢意。

笔　者

1996 年 1 月

目 录

第1章 引 论

1.1 莫里斯事件

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250 000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以使之逃避起诉。

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。只是最近，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DEC VAX计算机和Univac1108计算机，他发现在关键的几分钟内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“计算机病毒：潜在的威胁”。

1.2 病毒大事记

如果从1946年算起，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了。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，作精确描叙是很困难的。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。

- 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,cath 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。

- 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。
- 1986年1月在巴基斯坦的拉合尔，Basit和Amjad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。
- 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MacMag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。
- 1987年7月在汉堡发现"nVIR"病毒。这是有多个变种的Macintosh机病毒。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。

- 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。
- 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。
- 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 happend.
  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 Bandit。
- 1987年11月在以色列的希伯莱大学发现"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，致使希伯莱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。似乎病毒的设计有明显的政治目的。
- 1987年12月西德的BIT net网络发现"Christmas Tree"病毒(圣诞树病毒)。实质是攻击IBM国际通信网络BITnet中的IBM终端的蠕虫。它乱用电子邮件系统在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 youseif.
  Browsing this file is no fun at all
  Just 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。

- 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 Hand'被"Peace"病毒感染，公司被迫将5000套染毒软盘回收。
- 1988年3月"SCORES"病毒侵入NASA事件

  1987年发现的"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。

- 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 PDS 的反病毒工具 ‘Flu-Shot’ 的新版本。实质是 IBM PC 机的 MS-DOS 病毒。
- 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 CTL-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。
- 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。
- 1986 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自我保护意识。
  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。
- 1988 年 11 月 ARPAnet 网络 Internet 蠕虫事件
  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。
- 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。受害单位对蠕虫显示的信息、症状做出报告。
- 1989 年 12 月混有病毒的爱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爱滋病信息磁盘，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。
- 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。
- 1991 年发现“GPI”首例网络病毒

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。

- 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 Assosiation 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，被害程度比预想得轻。

- 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”。

- 1992 年病毒生产工具“VCL”在美国的传播

  VCL 是 Virus 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一工具。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。

- 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对应措施，该病毒未能大范围扩散。

- 1993 年 4 月美国 Microsoft 公司与反病毒厂家联手合作

  美国 Microsoft 公司在 MS-DOS 6.0 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-DOS 6.0 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。

病毒发展的年表如下：

1972 年：

- “Creeper”事件

1984 年：

- F. B. Chon 博士发表病毒研究论文

1986 年：

- 发现首例 IBM PC 病毒“Pakistani”

1987 年：

- 发现首例 Macintosh 机病毒“Peace”
- 发现感染后长度不变的“Lehigh”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

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-Shot 4”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
- 病毒侵入苏联政府的 80 台机器
- 莫里斯蠕虫入侵 Internet 网

1989 年：

- “Jerusalem”病毒使英国数百用户受损
- “Datacrime 1.2.3”在荷兰感染 10 万台计算机
- 1989 年 4 月中国首次发现 Ping Pong 病毒
- “WANK”蠕虫攻击 DECnet 网络
- “AIDS”病毒磁盘邮送敲诈事件

1990 年：

- 发现首例隐蔽型病毒“4096”

1991 年：

- 发现首例攻击网络的病毒“GPI”

1992 年：

- 米开朗基罗病毒在世界各地发病
- 美国在伊拉克防空系统中成功地施放病毒
- 多态性发生器使突然变异的多态性病毒剧增
- 美国网络中病毒生成工具“VCL”传播散布
- 芬兰发现首例 Windows 病毒

1.3 计算机脆弱性和病毒起因

国际标准化委员会对计算机安全的定义提出如下建议：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭破坏、更改、显露”。

计算机系统的安全可能受到三方面的威胁：

- 自然灾害
- 意外事故
- 人为破坏

本书不准备讨论广义上的计算机安全问题，仅限于与计算机病毒有关的因素。

1.3.1 脆弱的计算机系统

设计计算机系统时，主要考虑下述因素：