计算机病毒的特征 危害 检测与防治

主编　汪永全

四川科学技术出版社

计算机病毒的特征危害检测与防治

计算机病毒的

特征、危害、检测与防治

主编：汪永全
编委：汪永全 汪岩焯 樊志强 马 腾
陈 静 周冰冰

四川科学技术出版社

图书在版编目(CIP)数据

计算机病毒的特征、危害、检测与防治/汪永全编著．
成都:四川科学技术出版社,2001.1
ISBN 7-5364-4621-7

Ⅰ.计… Ⅱ.汪… Ⅲ.计算机毒病-基本知识
Ⅳ.TP309.5

中国版本图书馆 CIP 数据核字(2001)第 04001 号

计算机病毒的特征、危害、检测与防治

编 著 者　汪永全
责任编辑　康利华　罗小燕
封面设计　韩健勇
版面设计　康永光
责任校对　王　勤　楼　军　刘生碧
责任出版　何明理
出版发行　四川科学技术出版社
　　成都盐道街 3 号　邮政编码 610012
开　　本　787mm×1092mm　1/16
　　印张 16　字数 380 千　插页 1
印　　刷　成都前进印刷厂
版　　次　2001 年 2 月成都第一版
印　　次　2001 年 2 月成都第一次印刷
印　　数　1-3 000 册
定　　价　19.50 元
ISBN 7-5364-4621-7/TP·118

内容简介

1987年全世界发现的计算机病毒不到10种，目前已达20000余种。近年来变形病毒激增，仅宏病毒的变形体就有3650多种，某些病毒则具有无限变形能力。病毒技术和Internet的发展，使病毒危害力度强化，传播速度加快，危害范围急剧扩大。计算机病毒已经成为当代社会的一大公害。

我国计算机的社会拥有量和上网人数越来越多。许多用户迫切需要掌握更多的病毒知识，以防患未然或将病毒造成的危害和损失降低到最小。本书就计算机病毒知识作了全面、系统的介绍，包括病毒的产生、发展、演变、危害、预防、故障分析与检测、杀毒以及杀毒工具的选择、应用、注意事项等内容。全书共分三个部分。一至五章，着重介绍病毒的产生、病毒特征、病毒一般知识。六至十三章，着重介绍病毒的支撑条件、运行环境、传播途径、传播原因及社会危害。十四至十八章，着重介绍计算机系统感染病毒后的异常表现、故障分析、病毒的预防、检测、杀除方法及杀毒工具的选择。力求做到实用、适用和深入浅出，使具有中等以上文化水平的读者都看得懂、学得会、用得上。

引 论

计算机与现代通讯技术、多媒体技术的完美结合，国际互联网络的开通，极大地改变着我们的工作方式、生活方式乃至思维模式，将现代科技、经济和社会发展推向一个从未有过的文明高度。1999年全球上网人数超过1.5亿人，网络通讯量每100天翻一番，使信息资源共享正在成为现实，地球变成了一个“村落”。不仅如此，国家和地域的概念，不同文化和信仰的差异及意识形态领域里的冲突也有所淡化或变得模糊。知识经济正在到来，知识和信息成为新的最富于希望的经济增长点。所有这一切，都与计算机科学的发展，计算机的巨大社会拥有量和网络化联系在一起，将我们强力推进到了更加富于希望的21世纪。

但是，灿烂的阳光下依然存在阴影。高科技的脆弱性和负面效应，常常给我们带来意想不到的有时甚至是巨大的灾难。正如康德200多年前所说：“随着文明的发达，社会邪恶的总量也在增长。”关于技术反噬人类的“墨菲法则”虽然只是一种警告、忠告，但它也并非危言耸听。

现代高科技设备中技术的集成度越高，系统越是复杂，“臭虫”（技术隐含的缺陷或系统安全隐患、漏洞）越是难免。60年代，美国空军的F-111飞机中的计算机程序有近10万条指令；70年代，海军的P-3C飞机中的计算机需要50万条指令；80年代，B—1B轰炸机中的计算机拥有100万条指令；90年代，新型空间站发射需要多台计算机联合工作，指令总数超过8000万条。软件越来越成为计算机系统的关键因素。因此，人们已经越来越难以对技术的安全性作出绝对的保证。正反两方面的技术都在发展，犯罪分子和居心叵测者对系统安全的攻击与挑战从未停止过。

1986年1月28日，是全世界为之震惊和悲伤的日子。这一天，美国“挑战者”号航天飞机升空后不久，突然一声巨响，飞机爆炸了。5名男宇航员和2名女宇航员尸骨未存。许多人通过电视目睹了这一惨剧。事故缘于计算机。在进行生死攸关的程序检查时，计算机却失职了，未能及时发现问题的存在。

继1990年1月15日美国通讯系统大瘫痪之后，1991年9月17日，国际电话电报公司一次规模更大的通讯系统故障发生。事故是由一处备用的蓄电池未能起到应有的作用，引起计算机控制的自动转换与报警系统失聪。诱发计算机故障的是一个计算机软件中隐含的“臭虫”。由于通讯中断，美国最大的3个国际机场：肯尼迪国际机场、拉佳迪亚国际机场和瓦利克国际机场的声讯和数据通讯全部中断。纽约地区的空中交通也全部陷于停顿。500多个国际航班被迫取消，8.5万名乘客滞留空港并与外界失去联系。此外，还造成至少450万部国内电话和50万部国际电话死机。

1996年8月7日，世界上最大的联机服务公司因为一个路由器发生故障，使600万部网络计算机被迫关机长达19个小时，用户所有需要通过网络联系的工作全部中断。公司总裁史蒂夫·凯斯在致用户的道歉信中写道："我希望能告诉你们，这种事情绝不会再次发生，但是坦白地讲，我无法作出这种保证。"

1998年4月，黑客进入美国五角大楼计算机中心，窃走美国全球军事定位系统等敏感情报资料，威胁将把该技术和情报卖给国际恐怖组织。由于该技术用于美国导弹瞄准系统，如果落入敌对势力或国际恐怖组织手中，由此而引起的后果将不堪设想。近年来，世界各地的黑客对五角大楼计算机系统的攻击，每天多达近百次，1998年受到非法攻击多达25万次之多。为避免或减少重大不测事件发生，1998年9月，五角大楼忍痛摘除了因特网上的部分敏感信息库。

1999年2月，一伙手段高明的黑客侵入英国军事卫星通讯系统，操纵了其中一颗卫星的程序。黑客扬言，作为交换条件，除非得到一笔巨款，否则他们将操纵这颗卫星，包括该卫星生成和传输的信息。英国安全机关称该事件为"只有恶梦中才会出现的场面"。

对于高度依赖现代通讯技术和自动化技术的西方国家来说，这些灾难几乎是空前的和无与伦比的。以至于有人夸大高科技的负效应，对它美好的未来充满忧虑和猜疑。1996年3月11日，美国《商业周报》就曾宣布：互联网络已经没有生命力了。前3COM公司创始人，国际数据公司副总裁罗伯特·梅特卡夫曾撰文道："一年前我曾写过信息中断的文章，现在果然发生了，而且越来越频繁，每次中断的时间越来越长，危害程度越来越大。"他指出："许多人把环球网称作'环球堵'的信道堵塞现象，只是导致环球网崩溃的诸多原因之一。"几次影响重大的通讯中断都是看似无关紧要的小事引起的。一只啮齿类动物咬断了电缆线，或者操作者在互联网中心设备的软件上，把字符的位置弄错了。1996年在美国的一次互联网工作会议上，有人甚至哀叹"互联网的寿命像狗的寿命一样短。"一位发言者嘲讽道："如果说洛杉矶让失业的明星到饭店端盘子的话，那么我们也可以说，现在你在纽约用餐，每次碰到的招待员都有可能是水平很高的网址设计员。"公众对互联网的评价像下落的巨大钟摆一样下降。

如果说上述事件的发生具有偶然性，因此造成的恶劣影响和损失仍然有限的话，那么计算机病毒对计算机和网络系统的危害乃至对社会政治、经济发展的干扰和影响则是多方面的、经常发生的、持续的和难以控制的。

1987年10月，"巴基斯坦病毒"在美国泛滥，由于人们对病毒毫无防范意识和准备，使大部分计算机被其感染。1987年每逢13日又恰好是星期五，"黑色星期五病毒"爆发。此时，被感染的机器每运行一个文件便被病毒删除，造成系统内大量文件丢失。全世界数10万台计算机被置于其淫威之下，加之传媒煽情，人们几乎到了风声鹤泪谈毒色变的地步。

1988年11月"蠕虫病毒"发难，在几个小时中，使美国8500多台计算机陷于瘫痪。其余端机和局域网络因采取紧急脱网措施幸免于难。因特网因此而几乎全线崩溃。是年，仅美国就有9万多台计算机受到病毒危害，在人们心目中留下了浓重的阴影。各国科学家将1988年定为"世界计算机病毒年"，以警示世人并激励人们开展反病毒研究。

当黑色星期五病毒和蠕虫病毒袭来时，我国传媒作了适时报导，大多数人对计算机病

毒的理解停留在陌生的字符上。1989 年“小球”、“巴基斯坦”、“大麻”、“雨点”、“杨基”、“黑色星期五”等多种病毒便大举入侵国内,使国人措手不及。一些病毒至今屡见形踪,影响很坏。据公安部调查,是年,全国 PC 机近 80% 横遭病毒飞祸。北京一些高校的计算机系统的染毒率几乎 100%,有的软件中寄宿的病毒多达十多种。

1990 年“全美学自联”和国外一些反华势力,还一再公开扬言要利用病毒破坏我国的重要计算机系统。正如《计算机安全与保密》一书中指出:“尤其值得注意的是计算机病毒也成了境内外敌对分子制造政治影响,实施黄色淫秽宣传和毒害青少年的工具。”

我国科技界将 1989 年定为“中国计算机病毒年”。

1983 年 11 月在美国召开的国际学术会议上,美国计算机安全专家弗雷德·科恩博士首次提供了计算机病毒样本,供与会专家、学者在运行 UNIX 操作系统的 VA11/750 机器上实验,成功地验证了计算机病毒的存在及其危害。1984 年 9 月,国际信息处理联合会计算机安全委员会在加拿大多伦多举行的年会上,弗雷德博士发表了论文《计算机病毒:原理和实验》,将计算机病毒正式定义为:“计算机病毒是一种有害的可运行程序。病毒程序通过修改(操作)系统而传染其他程序,即修改其他程序,使之含有病毒自身精确版本、变种或其他病毒繁衍体。病毒可看作是攻击者愿意使用的任何代码的携带者。病毒中的代码,可经由系统和网络进行扩散,从而强行修改程序和数据。”

同一般有害程序不同的是计算机病毒具有很强的传染性。为了确保计算机资源和计算机信息的安全,必须消除它并禁止它的存在。

一个不幸的事实是,自弗雷德博士的上述实验以来,病毒的数量猛增,病毒的编程技术水平获得了惊人的发展,病毒危害遍及世界,以至于上升成为当今社会的一大公害。

1985 年全世界发现的计算机病毒不到 10 种。1995 年达 10000 种,1999 年末约 20000 种。冠群金辰公司 1999 年 9 月在广告中称,“KILL98 杀毒软件”可“全面查杀 20000 余种世界流行病毒。”目前,全世界每天都有 5~7 种新的病毒出现;具有相同“遗传基因”的变形病毒的数量增加更是惊人。病毒编程技术经历了从低级到高级,从简单到复杂的发展过程。全世界病毒专家和广大计算机用户同仇敌忾,一路围追堵杀,病毒的泛滥肆虐受到抑制,但不是根本上的遏止。

病毒技术的发展已历经数代,突出进展表现在自我保护功能、传播功能、危害功能、变形功能的不断强化。

病毒自我保护功能的强化。“巴基斯坦”病毒是早期发现的病毒之一,只有引导模块和传染模块,没有表现/破坏模块。它只感染软盘,把被感染软盘的卷标全部改为(C) Brain。病毒一旦获得系统的控制权,立即对其占据的 BOOT 区的引导部分进行读写保护,并在 BOOT 区位移量 04 - 05H 处,打上病毒感染的标志 1234H。如果此时检查被其取代的 DOS 引导区,会发现所有引导记录一切正常。若用干净的系统盘启动机器后查看病毒盘引导扇区,则会看到一段有趣的文字,其中包括该病毒的产地、公司名称、病毒版本及所谓的“病毒宣言”。“巴基斯坦病毒”的以上特点,在当时使人们很感惊讶,认为其具有非同寻常的智商,于是又有了一个响亮的名字“巴基斯坦智囊病毒”。

“巴基斯坦病毒”的高明之处是对自己的藏身处所进行保护处理,以掩盖其存在。但是,若与今日病毒的自我保护手段相比,可谓十分的初级了。保护自我,也就是保护生命

力和破坏力。这是病毒与反病毒斗争双方都要首先考虑的。今日病毒的自我保护技术之高明表现在多方面，如采取先进的程序压缩算法，使病毒程序变得更加短小精悍；采取自我加密技术使人难以发现；寻找宿主程序的空洞巧妙栖身；将病毒程序化整为零，分别寄存于宿主程序的不同位置或磁盘碎片中，时机到来时再化零为整，一朝发难；在藏身的磁盘扇区打上“坏簇”标志，逃避系统的读写和检查；破坏系统的错误中断向量，使系统的报警功能失聪；修改系统审计报告，使用户难觅其踪；频繁变化形态、形貌、形迹，以逃避杀毒工具的检测；对杀毒工具的检测进行反跟踪，发现被检测时即恢复被破坏的文件或磁盘的原貌，检测过后再次进入破坏状态；修改病毒检测报告，粉饰天下太平；建立杀毒工具信息库，将杀毒工具作为直接攻击对象，瘫痪其功能，等等。上述自我保护措施或单独使用或组合使用，导致杀毒工具的漏检漏杀、误检误杀。这也是病毒来无踪，去无影，久杀不绝的原因。1996 年美国的一项调查显示：80%的网民承认在事前没有觉察的情况下，遭遇过病毒的袭击。

病毒的传播能力更强。病毒的传染是指病毒从一个程序体进入另一个程序体的过程。它是在操作系统的支持下，由病毒自身的传染功能完成的。是病毒程序区别于其他有害程序最重要的特征。病毒本身是一种应用程序，因此，正常的计算机程序和信息运行的方法和途径，就是病毒运行、传染的方法和途径。病毒传播是指病毒从一个计算机系统进入另一个计算机系统的过程。计算机信息传播的载体、途径和信息通道，也就是病毒传播的载体、途径和信息通道。

病从口入是病毒的主要传染方法，软件则是其主要载体之一。软件是程序或指令的集合。没有软件，计算机便是一堆“废铜烂铁”。就安全性讲，软件有可信软件、不可信软件之分。就来源讲，软件有商品性软件、自由软件、用户自行开发软件之分。从功用上讲又有系统软件、应用软件、工具软件、学习软件、娱乐软件之分。软件的最大特点是流动性、方便性。用户通过交换软件达到信息资源开发与共享的目的。软件来自于世界各地，病毒借助软件传播也来自于世界各个角落。病毒没有国界。

随着信息高速公路的强力开通和 Internet 的迅猛发展，来自于 E-mail 上的病毒和 BBS 上的病毒激增。其危害之大，有时超过一般的软件病毒，成为仅次于软件的第二大病毒载体和传播渠道。

1999 年春节期间出现的“Happy 99 病毒”，传播速度之快，危害之大，在很短的时间内便对许多国家的社会和经济活动产生了不利影响。该病毒最初出现时潜伏在制作精美的电子贺卡中，在网络中被广为下载。计算机一旦被其感染，每当用户向外发送电子邮件时，它就会将自己的复制体发出，用户的电子邮件则发不出去。春节过后，商务邮件大量出现，病毒开始在经济运行部门和政府机构中快速蔓延，造成大面积感染和破坏。

使电子邮件发不出去的另一种病毒“Melissa”出现在 1999 年 3 月 26 日。据因特网报道，一天之内，全世界传染上此病毒的计算机就多达数百万台。微软公司、英特尔公司、摩托罗拉公司计算机中心功能强大的病毒防火墙也被攻破。许多网上公司被迫关闭。该病毒以“来自 X 人的重要信息”为诱饵，附带一个使用微软公司文字处理软件编辑的一个文档，用户一旦下载并打开这个文档，“Melissa”病毒即被激活，自动选择用户电子邮件地址薄中前 50 个通讯地址，将病毒文档发出。以后用户每次用微软公司的处理软件打开一个

文档或创建一个文档时，病毒都会潜藏其中，自动通过电子邮件把这个文档连同病毒一起发送给 50 个用户。其危害是：病毒传播以几何级数增加；用户敏感信息泄密；邮件服务系统负荷过载直至系统瘫痪。病毒发难的这一过程，用户全被蒙在鼓中。

ICSA 公司对 300 家共拥有 5.81 万台 PC 机的大公司调查显示：1997 年，每 1000 台计算机中，感染病毒为 62.5 次，1998 年该数字上升为 86.5 次。病毒传播渠道：1996 年来自于 E-mail 的病毒占病毒比重的 9%，来自于各种软件的病毒占 91%。1997 年来自于 E-mail 的病毒上升为 27%，1998 年上升为 32%。

“病毒发射枪”的出现使病毒陡然长长变粗，也结束了“病从口入”的单一传播方式。方法是运用一定能量的电磁波作为病毒载体和传输能量，将病毒遥控发射到特定感染对象上。特定对象可以是敌对一方的计算机系统，如作战指挥中心、空中交通管制中心、银行和证券交易所的计算机系统；局域网中的服务器；也可以是由计算机控制的其他设备、装置，如机床、精密仪器、通讯卫星、飞行器、尖端武器等。病毒入侵系统后自动传播和实施破坏，或者在需要的时候，遥控激活发难。

将病毒固化在计算机芯片中，通过一定途径和方法使其进入特定的计算机系统中，也是病毒传播的重要方法。1991 年 1 月海湾战争前夕，伊拉克空军从法国购进一台激光打印机，途径约旦首都安曼时，美国中央情报局特工将一枚含有病毒的芯片植入了该打印机，战争打响后，致使伊拉克空军作战指挥系统的计算机网络陷于瘫痪。海湾战争前夕，三名荷兰黑客曾向萨达姆晋言，他们有能力帮助伊拉克抵御多国部队进攻，办法就是用计算机病毒瘫痪多国部队的计算机作战指挥系统。作为代价，要求伊拉克支付他们 100 万美元作为报偿。萨达姆对 3 名黑客的建议视为骗局而嗤之以鼻，从而失去了这场战争的胜利，也失去了与克林顿分享将计算机病毒作为特种非杀伤性武器用于高科技战争的发明权。冷战期间，美国中央情报局也曾以病毒对前苏联通过非常途径从西方国家偷运出境的计算机进行破坏。

计算机病毒全方位传播渠道的存在，使计算机系统安全周界的概念变得模糊。传统的安全周界以计算机与附属设备之间的接口为界，接口以内称系统的内部安全周界，接口以外，称系统外部安全周界。如今这一概念已不确切。计算机病毒可以从多维空间中轻而易举地进入计算机系统潜伏下来，在需要的时候一朝激活发难，从而使用户不胜防备，造成巨大的心理影响和狐疑，甚至对计算机系统和计算机信息产生怀疑。从这个意义上讲，计算机系统无论是单机系统抑或网络系统的安全，并非完全取决于系统本身固若金汤的安全措施，也取决于系统的每一个器件、部件、节点和环节。这是一个令人沮丧的事实。

病毒的传播速度极快，范围扩大。一是病毒从点到点的传播是以光电速度传播。假若有人将染毒的 E-mail 从纽约发往北京，仅需一二秒钟时间。二是病毒从点到面的传播速度加快。几年前国外计算机病毒传播到我国沿海城市需要几个月时间。1999 年 3 月 26 日“Melissa 病毒”，通过国际互联网络，一天之内便在世界各地出现。计算机社会拥有量的大幅度增加，Internet 的建立和上网人数的急剧增加，都为病毒传播提供了社会物质基础和技术基础。由此也使一些原本只有局域性、地方性的病毒一下子变成了广域性病毒，使许多用户蒙难。三是病毒在计算机系统内的传播速度加快。1983 年，弗雷德博士为证实病毒的存在及其危害性所作的 5 次实验中，病毒平均使系统瘫痪的速度是 30 分

钟，其中最快一次仅用了5分钟时间。随着计算机运行速度功能和病毒技术的提高，一些病毒进入计算机系统后，几乎是在开机的瞬间即可完成对系统的感染。继“CIH病毒”之后，专门攻击NT系统的Remote Exploren的病毒又在网上泛滥。该病毒在计算机及网络中的扩散可以不经任何引导，可以在用户不执行任何操作的情况下侵入系统，加密用户的文件，使用户无法调用系统程序或对文件进行读写操作。不同类型病毒在同一系统内或同一文件内并行感染、重复感染、链接感染、交叉感染，往往造成极为复杂的局面。系统资源倍受破坏，病毒的检测和清除也变得十分困难，许多漏检漏杀、误检误杀就是在这种情况下造成的。

病毒的危害功能强化。早期病毒的危害主要表现为截取系统中断向量，破坏系统可执行程序等。病毒技术的发展使病毒危害的范围扩大，力度增加。它强行挤占系统资源；利用字符串穷尽法破译用户的口令，进行非法访问和越权访问；盗用系统密码，破译数据库加密信息；利用高级密码技术对数据库信息加密，使用户无法解读自己的信息；删除系统文件，篡改系统指令，毁坏数据信息；在夜深人静或系统关机时，调用多台计算机运算功能，分散作业一个大的运算题目或检索某一专题的敏感情报信息；在用户全然不知道的情况下对系统进行远程控制，篡改或窃取信息；将敏感信息、罪证，如大量色情图像信息，通过程序压缩技术、加密技术及其他数据转换处理技术，储存在远方用户的计算机中，造成计算机罪案发现难、侦破难、取证难。

1998年出现的两大超级恶性病毒至今使人心存余悸。一是直接以某些型号的计算机CPU为破坏对象的“CIH病毒”的出现，结束了病毒只破坏计算机软件的历史。被破坏的CPU很难修理，有的则几近报废。二是以网络浏览器为破坏对象和窃密对象的浏览器病毒，又称“Java病毒”，对用户的网页资源造成重大危害。浏览器染毒后正常功能无法调用，有时表现为浏览器不停地工作，画面和声音重复出现，键盘和鼠标不听指挥，严重的使系统拒绝工作或锁死。更可恶的是它能窃取系统资源为病毒作者编程服务；将窃取的口令和保密信息等用电子邮件自动发往指定的地址。改进后的该病毒能够溢出浏览器，在网上到处传播。专家预言，该病毒有可能盗用用户名义购物，或者制造逻辑炸弹进行敲诈活动，将恶名记在用户名下。

病毒的这些内容广泛的罪恶活动听起来像是天方夜谭或黑客行为，实际上都是已经发生或正在发生的事情。尤其是利用病毒窃取各类情报信息，近年来有明显增多的趋势，若不被遏止，有可能在经济、政治、科技、军事等领域中被滥用。《羊城晚报》1999年7月11日报道说，电脑病毒肆虐工商界，全球今年已损失76亿美元。1998年的该数字是15亿美元。美国加州调查机构“电脑经济公司”调查负责人迈克尔.厄布斯克鲁尔说道：“个人用户大都不会统计损失结果，一些公司则出于对公司形象的维护，可能缩小损失数额。所以，76亿美元的损失是相当保守的。”他还警告说：“电脑病毒侵袭是一种经济恐怖行为，在现今尚不能以有力手段控制的情况下，未来由此造成的财产和时间损失，都将进一步恶化。而且每一次新的病毒侵袭都将对生产力造成更大的破坏。”

在对大量病毒程序的解剖中发现，许多病毒表现形态不一，病毒的隐藏方式、潜伏地址、激活条件、破坏手法、危害力度也各不相同，但却有着相同的“遗传基因”，即特征值。于是专家认定，这些看似不同的病毒其实都是某一种病毒的变形体，称为变形病毒。

改变一种病毒使其具有某种新的特质、特征，要比重新编写一种病毒容易得多。变形病毒的生成方法，可以由人为地改变病毒程序的某些代码来实现。将病毒代码简单地重新排列组合有时也可生成许多新的变形病毒。病毒在传播过程中为自我保护或产生新的危害，依靠自身的指令也可实现自我变形。

使人震惊的是，一种被称为病毒自动生成机的软件已出现，使病毒生成的模块化、集成化的预言成为现实。它意味着病毒制造者只需成功地设计出一种病毒，便可借助计算机的功能，在此基础上变幻出许许多多形态各异的变形病毒。有的变形病毒每感染一次，就会变一次形；有的变形病毒甚至具有亿万次变形能力。许多杀毒工具所以漏检漏杀，就是因为不能较好地模拟变形病毒的变化技巧和变化趋势而败北。在我国广为流传的“Doctor 病毒”、“New Flip 病毒”、“Casper 病毒”、“1784/HXH 病毒”等都属于这种有极强变化能力的自变形病毒。“G_2 病毒”、“IVP 病毒”、“VCL 病毒”则属于病毒生产机生成的病毒。行天公司宣称其杀毒软件可杀除 18436 个病毒家族、3645 种宏病毒、372 种病毒生成机病毒。可见对付变形病毒形势之严峻。

近年来病毒技术的发展集中体现在变形上，其表现是变形病毒数量猛增，变形技术越来越复杂，病毒危害越来越大。变形病毒可分为 4 种类型。第一种类型的特点是，病毒每感染一个对象后，其代码与前一个染毒文件中的病毒代码几乎没有 3 个相同的连续字节，但这些代码相对的空间排列位置没有变化，称之为一维变形病毒。第二种类型的特点是，除具有一维变形病毒的特征外，病毒代码之间相对的空间排列位置也发生变化，称之为二维变形病毒。二维变形病毒在运行中能用特殊方式加载于正常的系统命令中，修改系统关键内核，与之融为一体，或干脆另外创建一个中断调用功能。第三种类型的特点是，除具备二维变形病毒的特征外，还具有分身术，化整为零，将病毒代码分存于不同地址，只要任何一段病毒程序被激活，都能迅速地化零为整，恢复整个病毒程序原状，实施危害。第四种类型的特点是，具备三维变形特征，这些特征还可以随时间变化而变化，有的则每感染一次就变形一次。四维变形病毒还具有网络功能，隐藏在网络的各个角落，条件成熟时即被激活。也可以通过遥控方式激活，窃取用户保密信息，悄悄发往指定的地址。

变形病毒目前已经发展到三维水平，四维病毒也将开始出现。在一定程度上，变形病毒代表了病毒技术的发展趋势。

有病毒就有反病毒。怎样估价当前的反病毒形势？有几个问题必须正视。一是病毒技术的提高，很大程度上是反病毒技术围剿的结果。这是一场正义与邪恶的较量，罪与罚的较量，生与死的较量。在十多年的较量中病毒与反病毒技术同时得到考验与发展。二是在现阶段，总的来说反病毒技术仍然处于疲于应付的被动局面，但是能够很快控制住病毒肆虐的局面，使病毒危害及其损失大为减少。目前，病毒发展的势头仍然很强，反病毒形势不容乐观，也可以说任重道远。三是计算机科学的发展和计算机应用并未因为病毒猖獗而受到严重影响，计算机与网络已经进入或正在进入人们生活、工作、学习、娱乐的各个方面；因特网作为第四大传媒正在崛起；计算机科学和文化对社会变革的影响正在从各个方面迅速而有力的表现出来。

这使我们想起了千百万年来人类同生物病毒斗争的历程。对某些生物病毒的斗争取得了辉煌的胜利，如“天花病毒”、“狂犬病毒”，人类都找到了获得免疫功能的办法，使这些

病毒丧失了在人类面前为非作歹的能力。对有些生物病毒，如“流感病毒”、“乙肝病毒”、“结核病毒”，人类虽然未能获得免疫功能，但是完全有能力将它们的危害控制在最低水平。对有些生物病毒则至今未能找到有效的抵御办法，如“艾滋病病毒”等。但是，即便是我们已经获得免疫功能的那些病毒，也并未彻底消灭它们，我们找到的仅仅是保护自我的方法。

计算机病毒不是生物病毒胜似生物病毒，因为它是人为的一种有害程序。人同计算机病毒斗争的实质是人与人的斗争，形式和手段变化无穷。计算机病毒因计算机而存在，只要现存的计算机存在，计算机病毒就存在。原因在于现存的计算机，主要是指 PC 机；具有技术上的开放性和不设防性的特点，使病毒得以方便地入侵其中作威作福。或者反过来说，假若计算机病毒不是作为一种可使计算机接受并运行的程序出现和存在，哪有病毒危害之说！

现存的计算机理论和计算机生成技术，远非技术的极限或理想的化身。计算机理论和技术都在发展，第二代 Internet 和新的计算机雏形都已依稀可见。专家预言，现存的计算机理论和技术终将被更理想、更完美的计算机理论和技术所取代。届时计算机病毒将很可能和它依存的现有计算机硬、软件一起，纸船明蜡照天烧。但是计算机犯罪仍然存在，矛盾和斗争仍然存在，不同的是内容和形式都将是崭新的了。

把病毒肆虐全部归咎于技术原因是不对的，人为的原因还很多，包括管理的、社会的和商业运作方面的及计算机安全等级低等原因。

我们研究病毒，了解病毒，目的是为了防治病毒，消灭病毒，还我一个干净的、健康的计算机系统，确保计算机资源不受破坏，确保计算机信息的完整性、保密性和可用性。

早期的杀毒软件是由计算机厂商和软件开发商免费向用户提供的。出于对病毒的同仇敌忾，IBM 公司、英特尔公司、CA 公司、NAI 公司、我国的金辰公司都曾举过义旗。这是一场持久战，一大批反病毒专家走在一起从事反病毒产品的开发，很快形成一种新的产业。目前，反病毒产品分为三大类：杀毒软件、病毒卡和用于网络病毒防治的病毒防火墙。各类产品品牌繁多、门类齐全，杀毒理论和方法也各有所长，共同筑起了一道病毒防线。

1998 年 8 月 30 日，我国公安部计算机安全管理委员会发出超级恶性“CIH 病毒”警报后，中央电视台和各大传媒纷纷报道。瑞星、冠群金辰、江民、趋势、行天许多公司迅速行动，在很短的时间内就研制开发出针对“CIH 病毒”的杀毒软件。到 1998 年 10 月 26 日该病毒再次爆发之日，记者跟踪调查发现，“CIH 病毒”已在国内受到有效遏止。1999 年 3 月 26 日“Melissa 病毒”出现后，数种变形体接踵而至。冠群金辰公司的“KILL98”杀毒软件针对上述病毒，28 日、29 日、30 日、31 日 4 天之内连续升级 4 次，对遏制病毒的蔓延作出了积极的贡献。这有力说明：我国已经拥有了一支高水准的能打硬仗的快速反应的专家队伍，我国反病毒产品的技术水平许多方面不在人下。更重要的是它向世人证明了：计算机病毒是可以预防和遏止的。预防为主，防治并举，是人类与生物病毒和疾病长期斗争积累的宝贵经验，对于计算机病毒这一方针同样适用。

需要强调指出的是，对计算机病毒的防治，必须常备不懈，持之以恒，若有懈怠，就可能给病毒以可乘之机。1999 年 4 月 26 日，“CIH 病毒”在世界各地的大爆发，就是一个深刻的教训。韩国和土耳其受到破坏的计算机各在 30 万台以上。俄罗斯 10 多万台计算机

受损。中东地区的阿联酋10%以上的计算机受损。我国也未能幸免。1999年4月26日，记者采访发现，从上午9时到下午4时，北京各家反病毒技术公司门前，手持被“CIH病毒”损坏的CPU的用户排起了长队，寻求公司的帮助。有些用户来自于国家机关的重要部门，有些来自于重要科研部门，对重要数据、文件的丢失十分沮丧和懊恼。广州市10%的计算机受损。有的用户将计算机内的时钟提前拨到4月24日，26日这天竟然未能幸免。据不完全统计，1999年4月26日这一天，我国受损的计算超过38万台。

1999年4月26日，计算机社会拥有量巨大的美国，仅有2328台计算机受到“CIH病毒”破坏。原因在于，一是用户普遍使用了较高质量的杀毒软件，二是传媒的事前提醒，用户早有防备。在我国，1998年10月26日“CIH病毒”被有效遏制后，传媒过分渲染取得的成就，助长了一些用户的侥幸心理；加之传媒事前未作任何提醒，致使损失酿就。

病毒防治包括单机防治和网络防治。技术上采取的措施：一是建立计算机系统的安全内核，二是使系统具有病毒免疫功能。现阶段完全实现上述措施尚有困难，已经取得的成绩也不尽人意，但无论如何这是解决病毒的根本途径。鉴于现阶段运行的计算机具有系统的开放性和不设防的特点，从管理入手，严防病从口入，显得尤其重要。在继“CIH病毒”之后出现的32位操作系统超级变形病毒“Margery”、“电子邮件病毒Melissa”、“Happy99”等病毒的有效遏止，都得益于以上两个方面的努力。

我国反病毒技术研究和产品开发与国外几乎同时起步。1990年8月我国大亚湾核电站进入施工的关键时刻，储存有从国外引进全套技术资料的计算机系统遭到病毒的突然袭击，陷于瘫痪。若不及时消除病毒，工程进度将受影响，引进资料也有毁于一旦的危险。法国专家用国外杀毒软件杀毒无效，心急如焚。华星公司闻讯后携微机病毒免疫卡赶到现场，手到病除。1990年11月华星公司携该产品参加美国拉斯维加斯世界计算机博览会，挑战西方列强，亮相洞喝：“拿你们的病毒来试！”用于测试的病毒无一生还。美国、英国、澳大利亚、新加坡、加拿大、瑞士等国的订单像雪片般飞来。4年后的1994年瑞星公司的病毒卡再次挑战拉斯维加斯计算机世博会，大获全胜。

在杀毒软件方面，我国也同样取得了可喜的成就。《人民日报》由计算机控制的电子排版系统，曾因病毒入侵而全面罢工，它意味着第二天《人民日报》的停版，这必将在国内外引起重大影响。金辰公司接报后，用KILL杀毒软件抢救成功。1996年“宏病毒”肆虐美国，在染毒的计算机中，“宏病毒”一度高达90%，计算机用户一片惊慌。一些软件开发商高价悬赏“宏病毒”治理技术。瑞星公司从美国考察后，在国际上首次提出了“MPS宏定位跟踪查杀病毒技术”。该技术能够准确判定文件中“宏”的种类和位置，区分正常“宏”和病毒“宏”，做到快速检测、定位、杀毒，而不破坏文件结构。它赢得各国反病毒专家的高度赞扬，使“宏病毒”的传播和危害受到有效遏止。当全世界的网络公司和广大用户尚未从“Melissa病毒”的袭击中清醒过来之时，第6天，瑞星公司又率先拿出了该病毒的解决方案，实现了杀毒软件几乎与病毒同步的目标，再次令世人瞩目。

1999年10月10日，国际信息安全会议在上海召开，来自世界各地的反病毒专家和网络安全专家共济一堂，献计献策。上海网络发展有限公司为展示本公司开发的“华堂网络安全系统”的神技，设下攻防擂台，布告天下：任何人勿需报名登记，在一周时间内，只要能够通过本公司的网络安全防御系统，进入公司网站(http://www.netway.net.cn)，获得主机

上名为 secu.txt 的文件，就算是一次成功的攻击。使用不同方法获得成功者，都可获奖5000元。可是一周时间过去了，5000元大奖终无得主。期间，“华堂网络安全系统”累计遭受来自世界各地的1800多名黑客6万多次攻击，仍安然无恙。参加国际信息安全会议的卿汉斯教授指出，密码、协议、防火墙构成网络安全的三道防线。目前，我国研制的超级防火墙像铜墙铁壁般很难绕过，密码和协议这两大反攻击工具尚无重大突破。

由于缺乏强有力的风险资金的支持和规模效益及其他人所共知的原因，我国反病毒产品起步较晚，总的来说在技术开发与市场开发方面，与发达国家的差距在逐步拉大。竞争是无情的，不进则退。正如英特尔公司总裁所言：“我们必须不断地淘汰自己的产品，否则便会被人淘汰出局。”

1998年6月国外反病毒产品获准进入我国市场，国人又一次面临“狼”来了的尴尬局面。商家面临洋货竞争，从此结束“躲进小楼成一统”的“桃园”生活。对广大用户来说则是一大好事。舶来品价廉物美，可救急，可开眼界。当我们还在DOS环境下操作计算机时，Scam杀毒软件就已为国人知晓。10年后的今天，该公司跻入全球独立经营的十大软件公司行列，公司更名 Network Assoc. ate Id 简称 NAI。NAI不仅有杀毒产品，还能提供全方位网络安全管理方案。包括对客户机、服务器和国际互联网网关在内的防病毒多级处理方案；将桌面加密软件和密钥管理工具与安全产品结合在一起的解决方案；网络管理和桌面服务解决方案；网络故障分析和性能管理的综合解决方案；将强大的桌面救助应用系统与数据库管理系统集成管理的完整方案等。上述产品都已形成了各自独立的软件系列产品，对国内软件市场是一个值得称赞的补充。

美国趋势科技公司的杀手锏是网络监控，即集中网域安全管理技术产品。从单一界面就可以完成产品的安装、配置、病毒码更新及提供统一病毒活性追踪报告等，从而减少了管理流程，节约了费用支出。新近推出的TVCS系列产品，可使系统管理员通过网络集中配置来更新运行于多平台上的反病毒产品，接收警讯及监控整个病毒防御环境，同时生成报告。

20年改革开放的实践，使我国企业已逐步走向成熟。它们不再盲目排外，崇洋媚外，而是找差距并抓住国外公司入市的机会，虚心学习他人的长处和经验，乘长风而升腾，借大船以出海。金辰公司和美国CA公司合作成立冠群金辰公司，堪称优势互补的典范。冠群金辰公司副总裁王铁肩先生以学者兼企业家的风度坦言心迹：“KILL问世以来一直在不断发展、不断前进，但到了1997年时，它的发展出现了困难。首先是全球病毒搜集网很难建立，要进行反病毒，必须首先搜集到病毒。过去在解决病毒方面，我们一直认为没有问题，我们的病毒搜集网是在过去十几年中建立起来的，国内出现病毒我们根本不怕。自 Internet 出现以后，情况发生了变化。从网上‘荡’出一个东西来非常容易，这也导致了病毒无国界，但要建立一个全球病毒搜集网，我们还没有能力。第二个困难是，计算机操作系统发展得太快，我们拿不到系统的底层资料。反病毒软件不是一个普通的应用软件，有时需要把软件写进操作系统的底层，使它变成操作系统的一部分，对系统进行实时的病毒监控。但要做到这一点，必须要对操作系统和网络系统的底层技术、接口都有非常清楚的了解，而现在厂商对这些全都保密。因此，在这种情况下，开发出好的适应于网络的反病毒软件就非常困难。要想开发网络版的反病毒软件在技术上并不太难，难点在于系统

底层资料。我一直认为我们在技术上是领先的,现在我们遇到了阻力,若不能迅速跟上,就有被国外高技术湮没的危险。在这种情况下,为了 KILL 的长久发展,为了 10 年后 KILL 还能存在,我们想出了一条捷径:合资。与国际上技术最先进的软件公司合资,成立"冠群金辰公司"。

冠群金辰公司推出的第一件合作开发产品是 KILL for DESKTOP 98 认证版杀毒软件,立即被美国计算机协会认证。它能够快速检测、杀除世界上所有已知病毒和一些未知病毒,包括时下仍很活跃的"宏病毒"。CA 公司的世界领先的反毒技术、先进的系统底层无缝链接技术与金辰公司国内一流的反病毒技术相结合,可实现实时复制及治愈、实时软盘检测、智能陷阱检测、"宏病毒"检测、灾难检测等。自动病毒特征码更新功能,则可借助国际互联网络实现自动拨号、下载和更新病毒特征文件。用户只需跟随提示进行操作,即可完成自动更新。该软件的多种平台防御体系,支持 DOS、WIN3.X、WIN95 和 WIN98 等多种操作系统,为用户提供了极大的方便。

金辰公司与 CA 公司技术对接,优势互补的下一个目标是开发能够覆盖所有平台和网络的全面的病毒解决方案。这正是目前国内所有反病毒产品生产厂家共同关注的热点、难点问题和技术发展方向。预计在不长的时间内,国内外广大用户将从这种中西合璧的优化组合中进一步大受其益。国内反病毒产品大踏步地进入国际市场的序幕已拉开。

计算机病毒是计算机科学发展阶段的产物,必将随着计算机科学的发展和病毒防治技术的提高,最终被彻底埋葬。但现阶段必须高度警惕,采用正确的病毒防治方法并长备不懈。我们热爱计算机,热爱网络,它是科学赐予当代人类的最大福祉。保护计算机网络的圣洁与健康,我们每个人都有一份责任。

本书的 4 至 6 章是由南阳市公安干部学校汪岩焯同志撰写;7 至 9 章由解放军总参通信部通信装备维修中心樊志强同志撰写;10 至 12 章由河南省检查学校马腾同志撰写;13 至 15 章由北京工业大学陈静(女)同志撰写;16 至 18 章由南阳市卧龙区人民法院周冰冰(女)同志撰写。由于作者水平有限,不当之处请批评指正。

周 刚

2000 年 2 月 10 日

目 录