青少年电脑实用知识普及丛书

电脑病毒防治

吴 越 编著

北京图书馆出版社

图书在版编目(CIP)数据

电脑病毒防治/吴越编著. - 北京:北京图书馆出版社,1998.6
(青少年电脑实用知识普及丛书/吴越主编)
ISBN 7-5013-1509-4

中国版本图书馆 CIP 数据核字(98)第 14240 号

书名 青少年电脑实用知识普及丛书
著者 吴 越 编著

出版 北京图书馆出版社(原书目文献出版社)
发行 (100034 北京西城区文津街 7 号)

经销 新华书店
印刷 湖南广播电视报印刷厂

开本 850×1168(毫米) 1/32
印张 45
字数 1150(千字)
版次 1998 年 7 月第 1 版 1998 年 7 月第 1 次印刷
印数 1-4000 套

书号 ISBN 7-5013-1509-4/G·407
定价 62.00 元(全 10 册)

总 序

电脑是二十世纪最伟大的发明之一。电脑，不但促使科学技术飞速向前发展，而且从科研机构飞进了“寻常百姓家”，成为当代人民生活中不可缺少的家用电器之一，从而彻底改变了人们的生活方式。

电脑从发明到今天，不过半个世纪，但在欧美先进国家早就已经相当普及了。在电脑的发源地美国，几乎家家户户都拥有“个人机”，上至耄耋老人，下至幼稚孩童，都能够在电脑上敲敲打打。有许多“电脑小神童”，后来发展成为硅谷的主人，为电脑事业的发展，做出了不朽的贡献。几十年来，美国在电脑事业方面始终遥遥领先，跟电脑的普及和众多的“电脑小神童”有绝对的关系。

当人家正在潜心研究电脑的时代，也正是我们无情地向“文化”开刀、向科学大闹革命的年代。直到拨乱反正以后，电脑方才开始在大陆“登陆”，但那也只是科研机关中的“稀罕物儿”，被当作“宠儿”娇生惯养地“供”了起来，闲杂人等，是连摸一下的可能都没有的。

电脑在中国大陆逐渐普及，终于走进了普通家庭，还是近年来特别是 1995 年以后的事情。这主要归功于两个方面。

第一是电脑价格的一降再降。一般的说法，电脑发明于 1939 年，1946 年正式建成并投入使用。从 1946 年到 1975 年的 30 年，电脑主要服务于科研、军事和大型企事业，与个人的工作、学习关系不大，与家庭生活更是风马牛不相及。从 1976 年到 1995 年，是电脑飞速发展与普及的 20 年。根据统计，1975 年全世界只有几万台电脑，到了 1995 年，就增加到 1.4 亿台，而其价格，则只有 20 年前的一万分之一；如果与 50 年前的第一台电脑比，则只有几千万分之一了。而从 1996 年到 1998 年的三年时间中，电脑的价格几乎又下降了二分之一。现在中国大陆一般有正常收入的工薪阶

层，不用节衣缩食，就能够购买一台中等档次的家用电脑。

第二，是软件产品的不断丰富，特别是汉字输入电脑的技术逐渐成熟。可以想象：如果电脑这个“洋玩意儿”根本就不认识中国字，所有在机器上运行的软件都不是为中国人开发的，除了高级科技人员之外，普通人很难学会操作，那么，电脑在中国大陆的普及，也是根本不可能的。

正因为如此，电脑才与中国人民结下了不解之缘。从1993年开始，中国的家用电脑销售量不断上升，到了1997年，终于达到了新的高潮。根据有关机构的统计数据，1997年底大陆共有电脑500万台，家用电脑的销售量比1996年足足增加了50％以上；预计1998年还有持续上涨的趋势。

电脑在中国的普及，加上“电脑要从娃娃抓起”的号召，中国的“电脑小神童”，也应该产生或已经开始产生了吧？电脑世界的博大精深，是没有“顶峰”的，还有许多未被开发的领域，正等待着无数的电脑小神童去开发呢！

现在，“家用电脑”已经逐渐普及，走进书店，电脑书刊琳琅满目，令人眼花缭乱。但是内容深奥的居多，青少年或电脑盲根本看不懂。买回一本书来，能够看明白的、真正有用的，不过十分之一而已。

我是中国大陆最早使用电脑从事文学创作的作家，十几年来，根据自己使用、教学电脑的经验，已经出版有10本共400万字的电脑通俗教材。这一套书，就是专门写给中学程度的青少年以及初学电脑的成人看的，内容力求深入浅出，通俗易懂，由浅入深，循序渐进，不讲高深的理论，而以应用为主。只要结合实际认真学完这一套书，就能从入门到精通，成为“电脑小神童”或者熟练用户。

希望这套书对您进入电脑天地起一个“领路人”的作用。如果需要在软件方面得到帮助，请来信。地址：100086 北京市 海淀区 大钟寺南村甲81号 中国戏剧出版社。

吴　越

1998年6月1日于北京

目 录

导 言

电脑发明到今天，已经有半个多世纪了；电脑病毒的出现，还只有十来年的历史。

电脑的出现，使人类文明向前迈进了一大步，给人们带来了无法计算的利益。电脑病毒的出现，只能破坏、阻碍人类文明的发展，使人们蒙受到无法估算的经济损失。所以有人把电脑病毒称之为“无形的杀手”和“万恶的魔鬼”，是一点儿也不过份的。

好在“魔高一尺，道高一丈”，现代科学的发展，不管怎么隐秘、怎么厉害的电脑病毒，都有相应的杀毒软件来对付它。因此对于电脑病毒，我们的态度是：第一反对，第二不怕。从另一个角度说，也希望电脑软件高手们从人类的共同利益出发，把自己的聪明才智用在对人类文明发展有贡献的地方，不要再去继续制造有百害而无一利的新病毒，而成为人人咒骂的“杀手”和“魔鬼”

时至今日，凡是学电脑的人，即便是“全封闭”式的、从来不与外界“交流软件”的人，也难免会沾上病毒。因为我们确实从买来的正版软件甚至正版的光盘中发现过电脑病毒。如果不懂得电脑病毒的防治，就难免被电脑病毒这个恶魔趁虚而入。尽管电脑感染上了病毒有杀毒软件可以把它杀死，但是也不排斥病毒杀死了，机内的文件也被破坏了的“两败俱伤”的局面。对电脑用户来说，最好的办法是“防患于未然”，千方百计不让电脑病毒侵犯机器；一旦发现有电脑病毒入侵，立即干净、彻底地加以消灭，绝不让它造成破坏和损失。

下面，就从电脑病毒发生、发展的历史说起，详细介绍电脑病毒的防治方法。

第一章

电脑病毒常识

一、什么叫做电脑病毒

什么叫做“电脑病毒”？简单地说，“电脑病毒”，是一组具有复制功能的破坏性电脑程序。

“电脑病毒”这一名词引自于生物学中的病毒概念，因为它是一种像生物病毒那样能够生存、繁殖、传播并危害电脑系统的特殊程序。从实质上分析，它跟生物学上所讲的“病毒”当然毫无共同之处，也没有一点儿连带关系。

有趣的是，“电脑病毒”这个术语，并不是出于科学家的有意“剽窃”，而是出于文学家的偶然“移植”。

1977 年夏天，在美国出版了一本相当畅销的科幻小说，名叫《P－1 的青春》，作者托马斯·捷·瑞安，是个极富想象力的科幻天才。他在小说中描写了一种可以在电脑之间传染的东西，而且首次从生物学界和医学界移植了“病毒”这个名词，把这种可以在电脑之间传染的东西叫做“电脑病毒”。更其令人拍案叫绝的是：他在这部小说中还描写了一场电脑病毒袭击控制了七千台电脑、造成一次破坏性极大的灾难——这简直是十一年后“莫里斯事件”的奇妙的预言！

尽管电脑病毒和生物病毒分属两个风马牛不相及的学科，但是两者之间确实有十分相似之处。人们把传播疾病、危害生命安全的一大类微生物称为“生物病毒”，因此，把传播电脑疾病(发生故障)、危害电脑系统安全的有害程序称之为“电脑病

毒”，倒也形象贴谱，何况电脑病毒往往是一些小巧玲珑的短程序，不妨把它们看成是电脑程序中的“微生物”；而生物病毒所具有的传染、潜伏、隐藏、危害等等特性，电脑病毒也无不具备。所以说，“电脑病毒”这个术语，不管它是怎样来的，倒是非常合适，如果打算再造一个，恐怕还没有这样贴切传神呢！

电脑病毒可以在电脑运行中自我复制(繁殖)并不断感染其他程序，在电脑系统内扩散；如果是在电脑网络中，传染的速度和面积就更快、更大了。

电脑病毒可以依附、寄生在某些程序上潜伏下来，在电脑中合法地运行，一旦条件成熟（例如一定的时间），就可以被激活。

所以，美国国家电脑安全中心为电脑病毒下的定义是：“电脑病毒是一种自我繁殖的特洛依木马，这匹‘马’由三条腿支撑：任务部分(干坏事的主要部分)、激活部分和自我繁殖部分。”

既然电脑病毒跟生物学无关，当然就都是人为的。所以现在大多数国家的法律都明文规定：凡故意制造病毒并已经对他人造成损害的，属于犯罪行为。

为什么要强调“故意制造”四个字呢？因为电脑病毒的形成，确实可以分为“故意制造”和“无意中造成”两大类。

故意制造的病毒，有的是恶作剧性质，例如曾经广泛流传过的“大麻病毒”，凡是感染了这种病毒的电脑，在运行过程中或每次启动的时候，屏幕的左上角都会出现一行字：“你的电脑现在变成石头了！”如果不是故意，怎么会有这样一行字呢？

在电脑病毒中，有许多是属于恶作剧性质的，例如在荷兰发现的“荷兰女孩病毒”，在其1332字节的病毒程序中，提供了一个名叫Sylvia的荷兰女孩的征婚广告，用不着说，那是骗人的，没有人会去应征；在葡萄牙发现的阿姆斯特拉德病毒，感染了.COM文件以后，在增加的847个字节的病毒程序中，夹

进了一份 Amstrad 电脑的假广告。这一类恶作剧形式各异，花样翻新，层出不穷，简直令人啼笑皆非。

另外有一些电脑病毒，则属于“社会报复”性质。例如“六四病毒”，每次发作的时候，屏幕上都会出现“不要忘记六四”这样的字行。

可见这一类病毒，确实是有人在故意制造的；动机更是千奇百怪，老板解雇、情人分手等等，都可以成为制造电脑病毒的原因。

值得注意的是：玩儿这类“电脑游戏”的人，本来只是一些被称为“电脑狂人”的西方青少年。近来发现，这种恶作剧也有“国产”的了。例如有一种因为发作的时候在硬盘分区表中有 New Century of Computer Now 字样而被称为“新世纪病毒”的，只在每年的 5 月 4 日发作，屏幕上会显示出一封给 XqR 的信：

X q R：

Wherever, I love you for ever and ever!
The beautiful memory for ours in that summer time has been recorded in he computer history.
Bon Voyage, My dear XqR!

YOURS 05 12 1991 in our home

意思是：XqR：无论到什么时候，我永远永远地爱你。在那个夏天里，咱们的美好记忆都记录在电脑的历史中。旅途平安，我亲爱的 XqR！你的××，1991 年 5 月 12 日于咱们家。

毫无疑问，这是一对中国情人分手后的“永恒的纪念”。

与日期有关的电脑病毒，当然都是故意制造的。1989 年 10 月 13 日星期五，一种取名于古老的圣经故事、从以色列希伯莱大学产生的名叫“黑色星期五”的神秘病毒，经过长期潜伏、广泛传播以后，终于有了一个大爆发的机会，袭击了全世界数

以百万计的运行着 DOS 的微机，结果是：每运行一个文件，就被删除一个文件，用户们只好被迫停机，为此而造成的损失，难以估计。

黑色星期五病毒又叫“犹太人病毒”、“长方块病毒”、“滚雪球病毒”、“希伯莱病毒”、“耶路撒冷病毒”、“疯狂拷贝病毒”、“十三号星期五病毒”等等，属于世界级恶性病毒。由于它传播速度极快，行踪又很诡秘，隐藏得比较深，具有极强的繁殖力和生命力。自从这个恶魔出世以后，很短的一段时间就在全世界范围内广泛扩散，所以影响面及危害性都很大。它攻击所有的 .COM 文件和 .EXE 文件，使 .COM 文件增加 1808 字节， .EXE 文件则以每运行一次增加 1808 字节的速度增长，直到占满整个磁盘空间为止。病毒进入内存以后大约三十分钟，屏幕左下方出现长方形亮块或作有规律闪动，有时候还伴随着条形花纹，系统速度明显减慢，甚至达到无法忍受的地步。到了机内系统日期是 13 日又恰逢星期五，病毒就开始大发作，给用户造成极大的损失。

1989 年 10 月黑色星期五病毒大发作的时候，当时中国的电脑一者为数还不甚多(共计 50 万台)，二者国内发现小球病毒才半年时间，许多人都还不知道什么叫做“电脑病毒”，所以对电脑病毒的新闻报导也比较淡漠。到了 1990 年 4 月 13 日又逢星期五，这位黑色杀手再次光临，引起了世界范围的一片恐慌。这时候电脑病毒已经在我国迅速蔓延，新闻媒介不得不作出了忧心忡忡的报导。到了 1992 年 3 月初，几乎全世界所有的新闻媒介都报导了这样一条消息：一种名叫“米开朗琪罗”的烈性电脑病毒，将在 3 月 6 日也就是意大利文艺复兴时期最伟大的雕塑家米开朗琪罗诞生 517 周年那一天流行，袭击全世界的电脑。这一回，中国的新闻界几乎是一涌而上，电视、广播、日报、晚报全体出动，一时间电脑病毒居然成了新闻明星。尽管大多数人对这种高科技领域内的鬼怪一无所知或知之甚少，却也在街头巷尾议论纷纷，津津乐道。

还有一种与日期有关的电脑病毒，叫做“美国佬病毒”，又叫做“扬基病毒”、“涂鸦病毒”，有报道说也已经进入我国。这一病毒1989年9月发现于维也纳，它对执行文件的威胁并不太严重，属于“执行文件寄生型”病毒，一旦进入内存，就在下午正五点钟奏出《扬基歌》（美国独立战争时期一首有名的歌曲）的主旋律，对电脑的破坏似乎不大；但若用户从贴有写保护口标签的磁盘上调用文件，磁头就会在磁盘上来回走动，发出很大的摩擦声，如果不及时关闭，就有可能划伤磁盘而丢失文件。

与时间有关的病毒中，还有一个叫“星期日病毒”的也很著名。这一病毒每逢星期日就发作，先在屏幕上显示一行文字：“今天是星期日，何必这样辛苦呢？”接着就捣毁FAT表，把磁盘里的数据全部破坏。在荷兰发现一种叫做“发薪日(Payday)病毒”的，是黑色星期五病毒的变种，它不管日期，专门在星期五捣毁运行中的电脑文件。

无意中造成的病毒，编制者的初衷并不是故意制造恶作剧，也不是出于某种报复，而是另有其他目的。例如有名的“巴基斯坦病毒”,就是巴基斯坦的两兄弟编制出来的。他们开了一家电脑商店，开发出一种软件，为了防止别人拷贝复制，他们在软件里编进了一种程序，使得这种软件只许使用，不许复制。谁要是非法复制，谁的电脑就会被这种特制的破坏程序所感染，造成损失。结果，由于软件的“放射性”复制，这种破坏性程序也广泛扩散开来，一发而不可收拾，终于形成了一种“恶性电脑病毒”。

电脑病毒的破坏性有大有小，因病毒品种而异。有一些病毒专门对数据进行破坏或修改。例如在墨西哥城发现的“魔鬼的舞蹈病毒”(Devil's Dance)，感染 .COM 文件，使其长度增加941个字节，并篡改输送到并行口和串行口去的数据；在里斯本发现的“里斯本病毒”，感染 .COM 文件，长度增加648个字节，被感染的文件有八分之一的程序头被修改为“爱滋病”

的名称：@AIDS；在纽约发现的“DBASE 病毒”，感染 .COM 文件，专门捣毁 .DSF 文件中的数据；在希伯莱大学发现的“阿拉巴马(Alabama)病毒”，感染 .EXE 文件，使其增加 1560 个字节，进入内存后操纵 FAT 表，使文件名互相调换，造成文件逐渐遗失；在英国布莱顿发现的“打印错(TYPO)病毒”，感染 .COM 文件以后，增加 867 个字节，并修改并行口上的数据，使打印出错。有一些病毒，则破坏系统区，从而造成系统瘫痪。

例如“爱滋病木马(AIDS Information Trojan)病毒”，寄生在 DOS 引导区，用被它感染的系统盘启动 90 次以后，硬盘就被锁死；在美国宾州伯利恒勒海大学发现的“勒恒(Lehigh)病毒”，攻击 COMMAND.COM 文件，使其增加 20 个字节，改变文件生成的日期和时间，并在四次感染后摧毁所有的系统数据；在美国加州奥克兰梅利特学院发现的“林荫散步道病毒”，侵犯系统引导区，将原引导区程序存放到磁盘的第一空闲簇，导致系统不能启动；“秘密复仇者(Dark Avenger)病毒”攻击的对象很多，包括 .COM 文件，感染后增加 1800 个字节，获得控制权后，具有反监控和跟踪能力，对文件和 FAT 表定时破坏。

二、是谁第一个制造病毒

最早“发明”电脑病毒的究竟是谁，至今并无定论，一般人都认为是世界驰名的微型软件公司(Microsoft)的创办人——“电脑奇才”比尔·盖茨(Bill Gates)。

七十年代初，比尔刚刚进入中学，还只有十三岁的时候，就已经是一位赫赫有名的破坏电脑系统安全的“专家”。他在破译电脑密码方面确实具有特殊的天才，而且还一心一意把非法入侵电脑系统作为自己具有非凡天才的最高体现。他曾经在一台电脑终端仅仅敲进 14 个字符，就侵入了 DEC 公司一套层层设防的多用户电脑系统。他到处炫耀自己曾经使某某公司的

电脑系统失灵，或者使某某公司的程序崩溃，以此作为自己的“资历的证明”。

当时美国最大的电脑公司 C^3 公司曾经宣称：它的全国性电脑网络——赛伯网络在任何时候都是安全的。小盖茨决心以自己的天才向这家大公司挑战。他用一台外围处理机去控制主机，侵入了赛伯网络，然后和赛伯网络的操作员斗智，终于摆脱了他们的监视而打入了主机。为了表示自己的胜利，小盖茨最后向主机输入了一组“特别程序”，结果使得全部电脑都出了毛病，导致全国性网络的瘫痪，赛伯网络不得不宣布停止工作。

盖茨向赛伯网络中心输入的“特别程序”，也许就是人类最早制造的电脑病毒。

这事情如果发生在今天，如此严重的电脑犯罪肯定会把盖茨送进牢房的。但在当时，像“电脑病毒”、“电脑犯罪”这一类术语还没有出现，所以小盖茨最后被抓住的时候，法律也不知道对这个尚未成年的、纯粹出于兴趣而搞恶作剧的电脑小天才应该如何惩办是好了。C^3 公司也只是狠狠地把他批评了一顿，就此作罢。

但是，电脑病毒却从此谬种流传，而且花样翻新，层出不穷，其危害范围之广大、性质之恶劣，恐怕连盖茨也没有料到吧？

另一种说法，认为盖茨编制的“特别程序”只能使电脑瘫痪，停止工作，程序本身不能复制，还不能算是真正的电脑病毒；而莫里斯编制的具有复制、传播功能的“特别程序”，才是真正的电脑病毒。

莫里斯 1965 年 11 月 8 日出生在美国新泽西州的莫里斯敦。他的父亲老莫里斯是美国电话电报公司贝尔实验室里负责政府电脑安全工作的专家。早在 1961-1962 年，老莫里斯就经常在下班以后留在实验室里和同事们玩儿一种自创的叫做“达尔文”的高级电子游戏，玩儿法是：各人编制一组程序，去毁灭

对方的程序。——实际上，这就已经是一种电脑病毒的雏形了。

小莫里斯得之家传，十二岁的时候，就能够编制一定质量的电脑程序。上中学以后，对电脑的兴趣越来越高。十七岁那年，他到人才济济的贝尔实验室，负责编写一些电脑安全程序，开始展现他的电脑智慧。后来他到哈佛大学心理学电脑中心当程序员，并最后在这里取得学位。

八十年代末，莫里斯在科尔内大学攻读博士，他的研究课题之一，就是把一种“无害”的病毒名叫“蠕虫”的，慢慢地传播到其他电脑系统中去。1989 年 11 月初，他的研究出了程序方面的差错，“无害”的病毒程序形成了具有复制功能的恶性病毒，并且把它送进了美国最大的电脑网络——Internet 网络。这以后的一系列事态变化，可就连莫里斯自己也没有料到了。

1989 年 11 月 2 日下午 5 点钟，Internet 网络的管理人员发现有一种神秘的病毒程序在网络中运行，并不断地截取用户口令等机密文件，用以欺骗网络中的“哨兵”，长驱直入网络中心；一旦入侵得手，立即反客为主，并闪电般地自我复制，抢占地盘。

网络的用户们目瞪口呆地看着这些神秘的入侵者迅速占领了电脑内存，使得许多台电脑在莫名其妙的状况下僵死，一方面无计可施，一方面急如星火地打电话向网络中心的工作人员求援。这时候，网络中心已经是四面楚歌，眼睁睁地看着网络中的电脑一批接着一批地因感染病毒而相继“死亡”，除了宣布网络暂时关闭并向电脑专家们求救之外，也是束手无策，无可奈何。

到了 11 月 3 日清晨 5 点，加州大学伯克利分校的电脑专家们方才找出了阻止病毒蔓延的方法。可是短短的 12 个小时内，这个“蠕虫”已经通过网络系统迅速地传染给了美国各地的大学和军事系统中的电脑，使得 6200 多台电脑瘫痪或半瘫痪，不计其数的资料和数据在这一夜之间遭到破坏，直接和间接造成的经济损失，高达一亿美元以上！