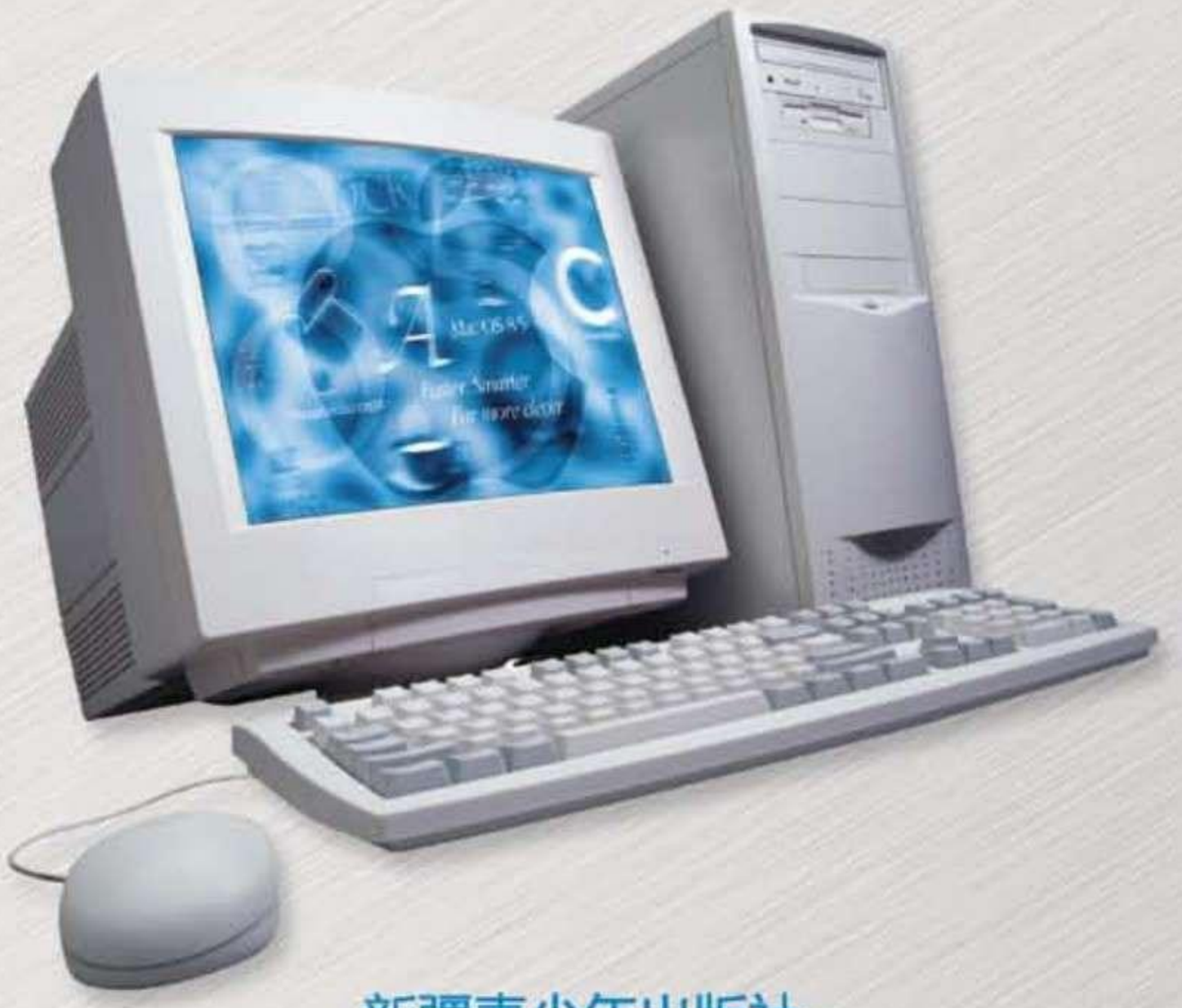
赵明远 任利◉编

信息技术教育大全

XINXI JISHU JIAOYU DAQUAN

03

病毒与预防



新疆青少年出版社

病毒与预防

赵明远　任利　　编

新疆青少年出版社

图书在版编目(CIP)数据

病毒与预防/赵明远,任利编.—修订本.—乌鲁木齐:新疆青少年出版社,2007.3

(信息技术教育大全丛书)

ISBN 978-7-5371-4029-4

Ⅰ.病… Ⅱ.①赵…②任… Ⅲ.计算机病毒—防治—基本知识

Ⅳ.TP309.5

中国版本图书馆 CIP 数据核字(2005)第 115337 号

信息技术教育大全

病毒与预防

赵明远 任利 编

新疆青少年出版社 出版

(地址:乌鲁木齐市胜利路二巷 1 号 邮编:830049)

北京市朝教印刷厂印刷

850×1168 毫米 32 开 100 印张 1200 千字

2007 年 4 月修订版 2007 年 4 月第 1 次印刷

印数:1—3000 册

ISBN 978-7-5371-4029-4

总定价:340.00 元(共 20 册)

前　言

二十一世纪是信息爆炸的时代，也是知识经济飞速发展的时代。这就要求我们要不断地更新观念，掌握现代信息技术，以适应时代发展的需要。

二十世纪六十年代开始萌芽发展的新兴电子计算机信息科技，与二十世纪九十年代初期开始普及的国际互联网通讯科技，构成了信息技术的基本框架，它改变了人类获取信息的途径，提高了人们的工作的效率。

电子计算机信息科技的优势在于能够较容易地实现信息处理的高速度性、高准确性、高标准化；更加合理地配置企业物力和人力资源；增加个人的生产力、支援高层决策力、降低生产成本。国际互联网通讯科技的作用则体现在缩短人与人、人与世界之间的距离；打破国界、疆界的阻隔，让不同种族、不同语言的人们通过网络来互相了解、互相学习、共同提高；将人类的生产力与价值带到一个更高的境界。电子计算

机信息科技与国际互联网通讯科技的联姻可以算得上是科技革命史上最具里程碑式的结合。两者的相互作用，影响了整个世界的信息技术格局。

本套丛书具有知识性、趣味性和实践性的特征。它从人们的日常需要的角度出发，对日常生活、学习、工作中遇到的各种问题进行了有益的探讨，并给出了精辟的讲解，注重知识体系的关联性、整体性和开放性，帮助大家获得信息技术前沿的各种知识。本书不仅注重书本知识的学习，更加注重实践动手能力的培养。让大家在学习中提高，在学习中获得足够的实践。我们的目标是把最优秀最可靠的信息技术知识介绍给广大的读者朋友，让大家在读书中有所获益。

本套丛书在编写过程中，经有关部门批准对部分作品进行了节选，以取适合本套丛书的部分，望未及时取得联系的作者见书后与我们取得联系，以便支付稿酬。另因编辑水平有限，加之时间仓促，文中难免存有谬误之处，望广大读者朋友批评指正，我们不胜感激。

编　者

目 录

第一章　计算机病毒的来源

第一节　病毒的基本常识

提起计算机病毒，相信绝大多数用户都不会陌生（即使那些没有接触过计算机的人大多也听说过），计算机病毒甚至还对有些用户有着切肤之痛，不过要问起计算机病毒是如何产生的、病毒到底有些什么特征，能够回答上来的用户可能并不多。为此，特将有关计算机病毒的定义、起源、历史、特征、传播途径、分类、最新动态、错误认识、防毒原则、解决病毒的办法等内容汇集成文，希望能对广大用户日常反防病毒操作有所帮助：

一、病毒定义

计算机病毒是指那些具有自我复制能力的计算机程序，它能影响计算机软件、硬件的正常运行，导致数据的正确性与完整性受到破坏。

计算机病毒是一个程序，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。计算机病毒可以很快地蔓延，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它一些共同特性：一个被污染的程序是一个能够传送病毒的载体。当你看到病毒载体似乎仅仅表现在文字和图象上时，它们可能也已毁坏了文件、再格式化了你的硬盘驱动或引发了其它类型的灾害。若是病毒并不寄生于一个污染程序，它仍然能通过占据存贮空间给你带来麻烦，并降低你的计算机的全部性能。

可以从不同角度给出计算机病毒的定义。一种定义是通过磁盘、移动硬盘和网络等作为媒介传播扩散，能“传染”其他程序的程序。另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。还有的定义是一种人为制造的程序，它通过不同的途径潜伏或寄生

在存储媒体(如磁盘、内存)或程序里。当某种条件或时机成熟时,它会自生复制并传播,使计算机的资源受到不同程序的破坏等等。这些说法在某种意义上借用了生物学病毒的概念,计算机病毒同生物病毒所相似之处是能够侵入计算机系统和网络,危害正常工作的“病原体”。它能够对计算机系统进行各种破坏,同时能够自我复制,具有传染性。

所以,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。

二、病毒来源

计算机病毒的来源多种多样,有的是计算机工作人员或业余爱好者为了纯粹寻开心而制造出来的,有的则是软件公司为保护自己的产品被非法拷贝而制造的报复性惩罚,因为他们发现病毒比加密对付非法拷贝更有效且更有威胁,这种情况助长了病毒的传播。还有一种情况就是蓄意破坏,它分为个人行为和政府行为两种。个人行为多为雇员对雇主的报复行为,而政府行为则是有组织的战略战术手段(据说在海湾战争中,美国防部一秘密机构曾对伊拉克的通讯系统进行了有计划的病毒攻击,一度使伊拉克的国防通讯陷于瘫痪)。另外有的病毒还是用于研究或实验而设计的“有用”程

序，由于某种原因失去控制扩散出实验室或研究所，从而成为危害四方的计算机病毒。

三、病毒历史

病毒是如何一步步的从无到有、从小到大的发展到今天的地步的呢？下面的介绍可以解除你的这一疑问：

概念的提出：“计算机病毒”这一概念是 1977 年由美国著名科普作家“雷恩”在一部科幻小说《P1 的青春》中提出 。1983 年美国计算机安全专家“考因”首次通过实验证明了病毒的可实现性。

1987 年世界各地的计算机用户几乎同时发现了形形色色的计算机病毒，如大麻、IBM 圣诞树、黑色星期五等等，面对计算机病毒的突然袭击，众多计算机用户甚至专业人员都惊慌失措。1989 年全世界的计算机病毒对用户的攻击十分猖獗，我国也未幸免。其中“米开朗基罗”病毒给许多计算机用户造成极大损失。

1991 年在“海湾战争”中，美军第一次将计算机病毒用于实战，在空袭巴格达的战斗中，成功地破坏了对方的指挥系统，使之瘫痪，保证了战斗的顺利进行，直至最后胜利。

1992 年出现针对杀毒软件的“幽灵”病毒，如One－half。

1996 年首次出现针对微软公司 Office 的“宏病毒”。

1997 年 1997 年被公认为计算机反病毒界的“宏病毒”年。“宏病毒”主要感染 Word、Excel 等文件。如 Word 宏病毒，早期是用一种专门的 Basic 语言即 WordBasic 所编写的程序，后来使用 Visual Basic。与其它计算机病毒一样，它能对用户系统中的可执行文件和数据文本类文件造成破坏。常见的如：Tw no 1(台湾一号)、Setmd、Consept、Mdma 等。1998 年出现针对 Windows95/98 系统的病毒，如 CIH(1998 年被公认为计算机反病毒界的 CIH 病毒年)。CIH 病毒是继 DOS 病毒、Windows 病毒、宏病毒后的第四类新型病毒。这种病毒与 DOS 下的传统病毒有很大不同，它使用面向 Windows 的 VXD 技术编制。1998 年 8 月份从台湾传入国内，共有三个版本：1.2 版/1.3 版/1.4 版，发作时间分别是 4 月 26 日/6 月 26 日/每月 26 日。该病毒是第一个直接攻击、破坏硬件的计算机病毒，是迄今为止破坏最为严重的病毒。它主要感染 Windows95/98 的可执行程序，发作时破坏计算机 Flash BIOS 芯片中的系统程序，导致主板损坏，同时破坏硬盘中的数据。病毒发作时，硬盘驱动器不停旋转转，硬盘上所有数据(包括分区表)被破坏，必须重新 FDISK 方才有可能挽救硬盘；同时，对于部分厂家的主板(如技嘉和微星等)，会将 Flash BIOS 中的系统程序破坏，造成开机后系统无反应。

1999 年 Happy99 等完全通过 Internet 传播的病毒的出现标志着 Internet 病毒将成为病毒新的增长点。其特点就

是利用 Internet 的优势，快速进行大规模的传播，从而使病毒在极短的时间内遍布全球。而 2006 年末至 2007 年初，中国湖北一青年编写的“熊猫烧香”，更是连挪威银行也中招。

四、病毒的特征

提起病毒，大家都很熟悉，可说到病毒到底有哪些特征，能有说出个所以然的用户却不多，这就严重影响了对病毒的防治工作。有鉴于此，特将常见病毒的特征简要介绍如下，希望广大用户能借以对病毒有一个较完善的灵性认识。

1. 传染性

传染性是病毒的基本特征。在生物界，通过传染病毒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。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。只要一台计算机染毒，如不及时处理，那么病毒会在这台机子上迅速扩散，其中的大量文件（一般是可执行文件）会

被感染。而被感染的文件又成了新的传染源，再与其他机器进行数据交换或通过网络接触，病毒会继续进行传染。正常的计算机程序一般是不会将自身的代码强行连接到其它程序之上的。而病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。计算机病毒可通过各种可能的渠道，如 U 盘、计算机网络去传染其它的计算机。当你在一台机器上发现了病毒时，往往曾在这台计算机上用过的 U 盘已感染上了病毒，而与这台机器相联网的其它计算机也许也被该病毒侵染上了。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。

2. 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、目的对用户时未知的，是未经用户允许的。

3. 隐蔽性

病毒一般是具有很高编程技巧、短小精悍的程序。通常附在正常程序中或磁盘较隐蔽的地方，也有个别的以隐含文件形式出现。目的是不让用户发现它的存在。如果不经过代码分析，病毒程序与正常程序是不容易区别开来的。一般在没有防护措施的情况下，计算机病毒程序取得系统控制权

后，可以在很短的时间里传染大量程序。而且受到传染后，计算机系统通常仍能正常运行，使用户不会感到任何异常。试想，如果病毒在传染到计算机上之后，机器马上无法正常运行，那么它本身便无法继续进行传染了。正是由于隐蔽性，计算机病毒得以在用户没有察觉的情况下扩散到上百万台计算机中。

大部分的病毒的代码之所以设计得非常短小，也是为了隐藏。病毒一般只有几百字节或 1k 字节，而 PC 机对 DOS 文件的存取速度可达每秒几百 KB 以上，所以病毒转瞬之间便可将这短短的几百字节附着到正常程序之中，使人非常不易被察觉。

4.潜伏性

大部分的病毒感染系统之后一般不会马上发作，它可长期隐藏在系统中，只有在满足其特定条件时才启动其表现（破坏）模块。只有这样它才可进行广泛地传播。如“PETER—2”在每年 2 月 27 日会提三个问题，答错后会将硬盘加密。著名的“黑色星期五”在逢 13 号的星期五发作。国内的“上海一号”会在每年三、六、九月的 13 日发作。当然，最令人难忘的便是 26 日发作的 CIH。这些病毒在平时会隐藏得很好，只有在发作日才会露出本来面目。

5.破坏性

任何病毒只要侵入系统，都会对系统及应用程序产生程

度不同的影响。轻者会降低计算机工作效率，占用系统资源，重者可导致系统崩溃。由此特性可将病毒分为良性病毒与恶性病毒。良性病度可能只显示些画面或出点音乐、无聊的语句，或者根本没有任何破坏动作，但会占用系统资源。这类病毒较多，如：GENP、小球、W－BOOT 等。恶性病毒则有明确得目的，或破坏数据、删除文件或加密磁盘、格式化磁盘，有的对数据造成不可挽回的破坏。这也反映出病毒编制者的险恶用心（最著名的恐怕就是 CIH、“熊猫烧香”之类的病毒了）。

6.不可预见性

从对病毒的检测方面来看，病毒还有不可预见性。不同种类的病毒，它们的代码千差万别，但有些操作是共有的（如驻内存，改中断）。有些人利用病毒的这种共性，制作了声称可查所有病毒的程序。这种程序的确可查出一些新病毒，但由于目前的软件种类极其丰富，且某些正常程序也使用了类似病毒的操作甚至借鉴了某些病毒的技术。使用这种方法对病毒进行检测势必会造成较多的误报情况。而且病毒的制作技术也在不断的提高，病毒对反病毒软件永远是超前的。

看了上面的介绍，你是不是对计算机病毒有了一个初步的了解？

五、病毒的传播途径

1.通过不可移动的计算机硬件设备进行传播(即利用专用 ASIC 芯片和硬盘进行传播)。这种病毒虽然极少,但破坏力却极强,目前尚没有较好的检测手段对付。

2.通过移动存储设备来传播(包括 U 盘、移动硬盘等)。其中 U 盘是使用最广泛移动最频繁的存储介质,因此也成了计算机病毒寄生的“温床”。

3.通过计算机网络进行传播。随着 Internet 的高速发展,计算机病毒也走上了高速传播之路,现在通过网络传播已经成为计算机病毒的第一传播途径。

4.通过点对点通信系统和无线通道传播。

六、病毒的分类

各种不同种类的病毒有着各自不同的特征,它们有的以感染文件为主、有的以感染系统引导区为主、大多数病毒只是开个小小的玩笑、但少数病毒则危害极大(如臭名昭著 CIH 病毒),这就要求我们采用适当的方法对病毒进行分类,以进一步满足日常操作的需要: