软件工程师丛书

防毒杀毒

——防杀计算机病毒自学教程

张 健 编著

電子工業出版社
Publishing House of Electronics Industry
URL:http://www.phei.com.cn

软件工程师丛书

防毒杀毒

——防杀计算机病毒自学教程

张 健 编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

图书在版编目(CIP)数据

防毒杀毒——防杀计算机病毒自学教程/张健著. —北京：电子工业出版社，1999.9

ISBN 7-5053-5450-7

Ⅰ.防… Ⅱ.张… Ⅲ.计算机病毒—防治—软件工具 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(1999)第 62480 号

内 容 提 要

本书从剖析计算机病毒特性出发，全面细致地介绍了预防和杀除计算机病毒的基本方法，内容涉及当前流行的多种计算机病毒以及应用最多的几种防杀病毒工具软件，书中还特别说明了 Windows 病毒和网络病毒的特性及防杀方法。

本书通俗易懂，内容全面，既适用于一般计算机用户认识病毒的本质和了解病毒现象，也适用于软件工程师深入了解病毒原理和技术发展，有助于在开发工作中或开发的产品上采取防范措施。

丛 书 名： 软件工程师丛书

书　　名： **防毒杀毒——防杀计算机病毒自学教程**

编 著 者： 张　健

责任编辑： 卢　山

印 刷 者： 北京市天竺颖华印刷厂

出版发行： 电子工业出版社出版、发行　URL:http://www.phei.com.cn

北京市海淀区万寿路 173 信箱　邮编　100036　发行部电话(68214070)

经　　销： 各地新华书店经销

开　　本： 787×1092 1/16　印张：12　字数：261 千字

版　　次： 1999 年 9 月第 1 版　1999 年 9 月第 1 次印刷

印　　数： 5000 册

书　　号： ISBN 7-5053-5450-7 / TP・2746

定　　价： 20.00 元

出版说明

近年来，随着计算机技术，特别是 Internet 网络的高速发展，计算机应用已经深入到人类社会的各个行业，各个领域，甚至千家万户。信息化社会、网络时代已经离我们不远了。

然而，计算机技术的发展，计算机应用的普及和深入，引发了对计算机软件的要求更广、更精、更加简便，以解决层出不穷的实际应用的问题。这样一来，非但没有解决十余年前专家们曾经预见的软件危机，反而使这一危机愈演愈烈。在世界范围内，软件开发人员的匮乏，高水平的操作系统、开发语言及应用软件的不足，各种补丁程序满天飞，已经成为计算机应用继续发展的一大障碍。

在我国，软件危机也同样存在，解决这一问题是目前刻不容缓的大事。

更值得引起我们重视的是，中国软件业要走自主创新之路。国际几大软件公司雄厚的技术和资金优势，已经垄断了重要的软件领域，并不断地推出新版本。后来者既要学习借鉴他人的技术，又绝不能永远跟着他人走下去。只是热衷于在他人的新版本上做一些表层开发工作是短视的，长此下去会逐渐丧失自主开发软件的能力。因此，在软件的学习和应用上，要学会掌握核心技术，即软件开发的思路和基本方法，并根据实际工作中提出的问题开发有自主知识产权的创新软件。

正是基于这种形势和认识，为发展我国的计算机软件开发事业尽一份出版工作者的责任，我们推出了这套《软件工程师丛书》。

这套丛书是为所有软件工程师和学习软件开发的计算机用户编写的，内容涵盖计算机软件开发的方方面面，其中既有国内作者编著的书籍，也有从国外精选引进的外版书。

为保证丛书的质量，我们选择的作者都是工作在计算机应用第一线，具有丰富软件开发和应用经验的学者、专家和高级工程师，外版书的译者都有多年计算机图书的翻译经验。

我们出版这套丛书的是想帮助软件开发人员提高技术水平，解决他们在软件开发和应用过程中遇到的各种问题。

这套丛书大致可分为四种类型：

一是实例型，如《Visual Basic 6.0 中文版实例详解》，通过大量有用的实例说明如何使用某种流行语言开发自己的应用系统。

二是实用型，如《Windows 2000/NT 疑难问题详解》，回答在应用某种操作系统中遇到的各种疑难问题。

三是技术型，如《软件测试自动化技术和实例详解》，介绍有关软件测试技术及其在实

践中的应用。

四是手册型，如《Visual C++6.0 类库大全》，是软件工程师的必备手册，可从中随时查阅所需的内容。

我们相信这套丛书对软件工程师和学习软件开发、应用的读者会有所帮助，我们希望听到读者宝贵的建议和意见。同时，希望更多的作者和我们联系，出版更多更好的书籍，来充实这套软件工程师丛书。

我们曾经努力，我们正在努力，我们仍将努力。

電子工業出版社
URL:http://www.phei.com.cn

前　言

今天，计算机已日益普及，并已深入到社会的各个阶层。计算机进入家庭已经成为现实，这给人们的工作和生活带来了前所未有的便利和效率。尤其是因特网的迅速发展，使人们的信息交流突破了地域的限制。与此同时，越来越多的人遭遇到计算机病毒，有些人深受其害，蒙受巨大损失。特别是使用计算机从事软件开发和文书写作的人们，不经意间，计算机病毒就会把人们数月、甚至多年积累在计算机中的知识财富抹得一干二净。面对残酷的现实，为使广大计算机使用者能更多地认识计算机病毒、了解病毒原理，尤其是为了在病毒尚未发作和破坏之前及时地发现并彻底杀除它们，特将此书献给读者。

本书针对典型病毒的介绍十分详细和具体，其内容包括病毒的危害性、传播与“生存”方式和发现及杀除方法等，对从事开发工作的软件工程师来说，既有自我保护作用，也有助于从预防病毒和安全运行方面改进自己的软件的性能。

全书共七章。第 1 章介绍计算机病毒基本概念。第 2 章通过病毒侵入后引起的种种异常现象，介绍判断病毒的方法。第 3 章介绍几种流行的杀毒软件及其使用方法。第 4 章介绍 Windows 环境下防杀宏病毒的方法。第 5 章介绍如何防杀网络病毒。第 6 章介绍病毒与反病毒技术。第 7 章提供计算机病毒“黑名单”，较详细地介绍了 57 种常见病毒和列表给出 1000 种病毒的基本特点。

由于水平有限，书中疏漏与不妥之处敬请读者批评指正。

参加本书编写工作的还有王艳秋、唐毅谦、张少中、王俊生、岳大鹏及郑风翼等。

编　者

1999 年 9 月

目　录

第1章

了解计算机病毒

近几年来，有关计算机病毒的报导和消息很多，尤其是1999年4月26日，CIH病毒的大范围发作甚至引起了信息业的震动。究竟是什么原因人们对计算机病毒如此关注呢？原来计算机病毒如同人类机体上的癌，它对计算机系统有着十分强大的破坏力。病毒能够破坏计算机系统内珍贵的信息资料，甚至能够损坏计算机硬件。由此可以看出，了解一些有关计算机病毒的知识，对于使用计算机的人们来说是十分必要的。本章将从CIH病毒入手，介绍什么是计算机病毒、计算机病毒的特点、种类和危害。

1.1 “病毒核弹”CIH“大爆炸”

1999年4月26日上午八时，和往常一样，我习惯地打开计算机，我的计算机曾给我的工作带来极高的效率，也曾在业余时间给我带来许多欢乐。然而它今天似乎有些反常，以往漂亮的画面不见了，取而代之的是一个黑漆漆的屏幕，我的计算机怎么了？

几天后，我终于明白了。我的计算机感染了病毒，而且感染的是被称为“病毒核弹”的CIH病毒。这种有史以来最为恶毒的病毒不仅能破坏保存在硬盘上的珍贵信息资料，而且还能破坏计算机主板，使计算机彻底瘫痪。如此看来，我的计算机真是凶多吉少。

CIH病毒每年的4月26日发作，有些它的变种病毒每月的26日也会发作。病毒发作后，看到的只是一个黑漆漆的屏幕，反复启动，依然如故。面对由CIH病毒强大的破坏力造成的一个个黑漆漆毫无生机的屏幕，病毒制造者有何感想不得而知，但4月26日确实是国内许多计算机使用者最黑暗的日子。据报导，在这一天，全国有数以万计的计算机被CIH病毒击中，大量珍贵的资料被毁、计算机主板被破坏，损失达十亿元。由此可见计算机病毒十分可怕。

1.2 什么是计算机病毒

在使用计算机时，有时会遇到一些奇怪的现象。例如，运行某个软件时出现死机，或计算机无缘无故地重新启动；屏幕上出现奇怪的图形或符号；喇叭里发出奇怪的声音；硬盘中的资料不翼而飞；打印机无法正常工作等。这些现象有可能是计算机硬件故障引起的，也有可能是软件配置不当引起的，但大多数情况下是计算机病毒引起的。

由于计算机病毒的作者相互隔绝，又怀着不同的目的，所以现在发现的计算机病毒千差万别，种类不一。因此，对计算机病毒的定义只能是对其共性的描述。

美国著名的计算机安全专家Fred Cohen，于1983年首次在国际计算机安全会议上发表了关于计算机病毒的研究成果。他说，计算机病毒是一种程序，它用修改其他程序的方法将自己的精确拷贝或者可能演化的形式放入其他程序中，从而感染它们。由于这种感染特性，病毒可以在信息交流的途径中迅速传播，并破坏信息的完整性。

1994 年 2 月 28 日，我国出台《中华人民共和国计算机安全保护条例》，对病毒的定义如下：计算机病毒，是指编制、或者在计算机程序中插入的，破坏计算机功能或者破坏数据、影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

简单地说，计算机病毒是一种特殊的计算机程序。它是由一些怀有不同目的的人编写的。它与生物学病毒有着十分相似的特性，如感染性、寄生性和破坏性。它虽然对人不会造成直接伤害，但对计算机系统却可能造成致命的伤害。

计算机病毒程序比较小，一般不会超过 5KB。与计算机其他合法程序一样，可以存储，可以执行，但是它没有文件名，不能在磁盘中以文件的形式独立存在。表 1-1 是病毒程序与正常程序的比较：

表 1-1　病毒程序与正常程序的比较

病毒程序	其他正常可执行程序
一般比较小，在几百到几千字节之间	一般比较大
并非完整的程序，必须依附在其他程序上	是完整的程序，独立地存在于磁盘上
没有文件名	有自己的文件名和扩展名，如 COM、EXE
有感染性，能将自身复制到其他程序上	不能自我复制
在用户完全不知道的情况下执行	根据用户的命令执行
在一定条件下有破坏作用	无破坏作用

计算机病毒寄生于磁盘、光盘等存储介质当中。这时它是静态的，不会感染，也不会起破坏作用。当用寄生了病毒的磁盘启动计算机时，或者执行染毒程序时，病毒就会随着合法运行的程序进入计算机内存，这时病毒进入活跃状态，随时可以进行感染和破坏，这个过程被称为激活病毒。

病毒被激活后，随时可以进行感染和破坏。不同的病毒有不同的感染目标，病毒的破坏行为也是不同的。

虽然现在对计算机病毒的定义存在着差异性，但都肯定这样一个事实，即：计算机病毒是一种特殊的程序。

1.3　病毒的起源

“计算机病毒”一词首次出现是在科幻小说中。1977 年，美国的 Thomas J.Ryan 出版了他的一本科幻小说，名叫《The Adolescence of P-1》，在这部小说中作者幻想出世界上第一个计算机病毒，它可以从一台计算机传播到另一台计算机，最终控制了 7000 多台计算机的操作系统，造成一场大灾难。

10 年后，计算机病毒由幻想变成了现实，并广泛传播。

1987 年 10 月，在美国发现第一例计算机病毒(Brain)。

1988 年，各种计算机病毒相继出现并广泛传播。11 月 2 日，美国康奈尔大学的学生，23 岁的莫里斯(Morris) 将自己编制的蠕虫程序输入到计算机网络中，在几小时内造成 Internet 网络的堵塞，6000 多台计算机被感染，造成巨大损失。

1989 年 11 月 13 日，这天恰巧是星期五，著名的“黑色星期五”病毒发作，损失巨大。

1991 年，发现首例专门攻击计算机网络的病毒“GPI”。

1994 年后，采用密码技术、编写技巧高超的隐蔽性病毒和多变型病毒相继出现。

1995 年 8 月 9 日，在美国首次发现专门攻击 Windows 操作系统的新型病毒，这就是宏病毒 Concept。

1998 年 6 月，世界上首例能够破坏硬件的病毒 —— CIH 病毒被发现。CIH 病毒产于台湾，它既攻击硬盘中的文件系统，又攻击计算机硬件(主板)，并使其损坏。

从首例计算机病毒被发现起，病毒的发展速度十分惊人。1988 年底，病毒不足 100 种；1994 年夏，病毒的数量已近 5000；到 1998 年夏，据资料介绍，全世界已发现的计算机病毒超过 15000 种，并且以每天 10 种的速度在增加。病毒的攻击目标已由单台计算机，发展到网络计算机；由破坏磁盘中的信息，发展到破坏计算机硬件。

关于计算机病毒的起源众说纷纭，大至有如下几个方面：

1.3.1 起源于计算机爱好者的表现欲

一些人认为：计算机病毒来源于一些计算机爱好者的表现欲。这些人编制计算机病毒的目的不是为了破坏，而是为了显示他们渊博的计算机知识和高超的编程技巧。

美国康奈尔大学的莫里斯在编制蠕虫程序时，单枪匹马地破译了采用 DES 对称密码加密的口令，使蠕虫无孔不入。而对 DES 密码，IBM 公司曾组织了由 18 个密码专家组成的班子，花了近一年的时间也未能找到破译方法，由此可见，莫里斯的技术能力是非常惊人的。

但是，由著名专家组成的委员会在蠕虫事件的调查报告中认为：莫里斯释放蠕虫程序是一种忽视了明显的潜在后果的青少年行为，并客观地指出，当蠕虫程序进入网络，骗取了口令之后，它已经获取了系统用户的特权，可以读取被保护起来的机密数据，可以做种种特权操作，蠕虫已经具备了进行最严重破坏的能力。但是，蠕虫没有做，蠕虫造成的唯一破坏仅仅是使计算机的运行速度变迟缓。

这说明莫里斯已经具备相当高超的技巧，如果他恶意攻击，蠕虫可以造成极为严重的后果。蠕虫事件是计算机病毒起源于计算机爱好者的表现欲的有力证据。

1.3.2 来源于软件加密

还有一些人认为：计算机病毒来源于软件的加密技术。

软件产品是一种知识密集的高科技产品。软件产品的研制耗资巨大，而且生产效率很

低，但复制软件却异常地简单。由于各种原因，社会未能对软件产品提供有力的保护，大量存在非法拷贝和非法使用的情况，严重地损害了软件产业的利益。为了保护软件产品，防止非法复制和非法使用，软件产业发展了软件加密技术，使软件产品只能使用，不能复制。

早期的加密技术是自卫的，它可以使程序锁死，使非法用户无法使用，或使磁盘“自杀”，防止非法用户重复破译。后来随着加密与破译技术的激烈对抗，软件加密由自卫性转化为攻击性，于是产生了计算机病毒。

著名的巴基斯坦病毒 C-Brain，是世界上唯一的给出病毒制造者姓名和地址的病毒，其目的就是跟踪软件的非法用户。

1.3.3 来源于游戏

60 年代初，美国麻省理工学院的一些年青研究人员，在做完工作后，利用业余时间玩一种他们自己创造的计算机游戏。做法是某个人编制一段小程序，然后输入到计算机中运行，并设法消毁对方的游戏程序。这可能就是计算机病毒的雏型。

1.3.4 来源于感情的寄托

一些病毒信息具有明显的感情色彩，表明病毒制造者借用病毒发泄心中郁愤，这种病毒的名称和发作显示信息往往直书心意。

1.4 病毒的感染载体与寄生软件

计算机病毒的感染载体主要有磁盘(软盘和硬盘)、光盘和计算机网络。

1. 硬盘

在计算机系统中，由于硬盘的容量比较大，且读写速度快，所以人们在使用计算机时，读写文件主要是在硬盘上，因此，硬盘就成了病毒寄生的主要载体。

2. 软盘

软盘的特点是携带方便，同时又具有一定的容量。目前，很多单位和个人经常以软盘为载体交流应用软件或交换数据。如果将带有病毒的软盘用在其他系统中，病毒就会感染该系统，因此，软盘就成了病毒传播的主要载体。

3. 光盘

计算机系统中使用的光盘多为 CD-ROM，只能读不能写，因此，光盘中的文件是不会被病毒感染和破坏的。但是，光盘软件如果有病毒则会感染和破坏其他的载体。一些光盘制造者在光盘中集成大量的软件，相当于软盘的数百倍，如果不仔细检查处理，其中的一些软件则可能带有病毒。这种情况出现在盗版软件光盘中较多。

4. 计算机网络

计算机网络实现了资源共享，给人们带来很多方便。但是，只要在网络中传输的数据或文件染有病毒，病毒就会以极快的速度在网络中蔓延，破坏力极大。

计算机病毒总是以寄生方式隐藏在计算机软件之中，尤其下列软件较为危险：

1. 盗版软件

盗版软件因人们随意相互拷贝而流传，在这个过程中，根本无法保证它不会被病毒感染。制造病毒的人会专门利用盗版软件来传播他的病毒。

2. 公共软件

公共软件允许人们随意拷贝，同盗版软件一样，人们无法确定公共软件是否染毒，但是，由于这种拷贝是合法的行为，因此公共软件带有病毒的机率不会像盗版软件那样高。

3. 国际互联网络上的下载软件

国际互联网络上的软件资源极其丰富，许多软件可以下载使用，但是下载的软件中可能含有病毒。

4. 具有报复功能的正版软件

有些正版软件为了防止被非法用户拷贝或使用，采用了防盗惩戒措施，即如果发现有这些非法行为，便释放出计算机病毒予以惩戒。

5. 带宏的数据文件

如 Word 的 doc 和 dot 数据文件。此类文件用 Word 打开时可能会使其中的病毒宏运行，进而感染和破坏用户的数据文件甚至硬件。

1.5 病毒的危害

计算机病毒有感染性，它能广泛传播，但这并不可怕，可怕的是病毒的破坏性。一些良性病毒可能会干扰屏幕的显示，或使计算机的运行速度减慢；但一些恶性病毒会破坏计算机的系统资源和用户信息，造成无法弥补的损失。归纳起来，计算机病毒的危害大致有如下几个方面：

1. 破坏磁盘文件分配表(FAT 表)，使磁盘上的信息丢失，这时使用 DIR 命令查看文件，会发现文件还在，但文件名与文件的主体已失去联系，文件已无法使用了。

2. 删除软盘或硬盘上的可执行文件或数据文件，使文件丢失。

3. 修改或破坏文件中的数据，这时文件的格式是正常的，但内容已发生了变化。这对于军事部门或金融系统的破坏是致命的。

4. 产生垃圾文件，占据磁盘空间，使磁盘空间逐渐减少。

5. 破坏硬盘的主引导扇区，使计算机无法启动。

6. 对整个磁盘或磁盘的特定扇区进行格式化，使磁盘中的全部或部分信息丢失。

7. 破坏计算机主板上 BIOS 内容，使计算机无法工作。