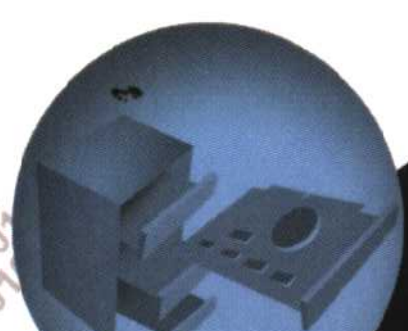
电脑应用技巧系列手册

电脑防黑及隐私保护技巧手册

卢国俊　韩建光　编著

完全实例
完全技巧
完全步骤
完全引导



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

电脑应用技巧系列手册

电脑防黑及隐私保护技巧手册

卢国俊　韩建光　编著

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

内 容 简 介

本书针对电脑应用中病毒防护和清除的问题提供了各种防病毒知识、软件安装、使用和防护、清除方法。对各种病毒的表现形式、特征和消除，做了较详细叙述，同时给出大量实用的防护及清除技巧，为保证电脑正常运用，提供了宝贵经验。

本书详实、新颖、方法简单实用，是广大电脑用户的必备工具书。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

电脑防黑及隐私保护技巧手册 / 卢国梭，韩建光编著. —北京：电子工业出版社，2006.2
（电脑应用技巧系列手册）
ISBN 7-121-02217-6

Ⅰ. 电… Ⅱ. ①卢… ②韩… Ⅲ. 电子计算机—安全技术—技术手册 Ⅳ. TP309-62

中国版本图书馆 CIP 数据核字（2006）第 002524 号

责任编辑：焦桐顺
印　　刷：北京天竺颖华印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
经　　销：各地新华书店
开　　本：787×1 092　1/48　印张：5.875　字数：174 千字
印　　次：2006 年 2 月第 1 次印刷
印　　数：5 000 册　　定价：10.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第1章 电脑防护基础

近年来，利用网络安全的脆弱性，黑客在网上的攻击活动每年以几何级数的速度在增长。他们把网络的各种漏洞和缺陷作为靶子，无孔不入，或者修改网页进行恶作剧，或者非法进入主机破坏程序，或者企图利用银行网络进行诈骗犯罪，或者窃取网上信息兴风作浪，或者进行电子邮件骚扰，或者施放病毒使网络陷于瘫痪等。

与此同时，我国网络受黑客侵犯的事件也屡屡发生，呈明显上升趋势。有人说过一句话："因为因特网无国界，所以因特网上的安全就是国界。"

1.1 防毒基础

1.1.1 什么是计算机病毒

计算机病毒（Computer Virus）在《中华人民共和国计算机信息系统安全保护条例》中被明确定义：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，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

计算机病毒究竟是从何而起的？

1983年，美国贝尔实验室的研究人员经常设计各种会吃掉对方程序的程序，作为闲暇之余的的消遣。1987年，一对巴基斯坦兄弟为防止他人盗拷他们编写的电脑程序，编写了第一个电脑病毒——大脑病毒（C-Brain）。

1988年11月2日下午5时1分59秒，美国康奈

尔大学计算机科学系23岁的研究生莫里斯（Morris），将其编写的蠕虫程序输入计算机网络，在几小时内导致因特网堵塞，运行迟缓。这件事就像计算机界的一次大地震，震惊全世界，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对防止计算机病毒的研究。

1988年下半年，最初引起人们注意的病毒是20世纪80年代末出现的“黑色星期五”、“米氏病毒”、“小球病毒”等。此后，由计算机病毒发作而引起的“病毒事件”接连不断。1998年第一个通过E-mail传递的名为Happy 99的病毒出现，加上尾随其后的梅丽莎病毒、爱虫、红色代码、冲击波等病毒，更是给社会造成了很大损失。

1.1.2 病毒的特征有哪些

1. 传染性

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，那么病毒会在该计算机上迅速扩散，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连接时，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

此为试读，需要完整PDF请访问：www.ertongbook.com

行连接到其他程序之上的。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，如软盘、计算机网络去传染其他的计算机。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软盘就已感染上了病毒，而与这台机器相连的其他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。

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、目的对用户是未知的，是未经用户允许的。

2. 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。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。正是由于其隐蔽性，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。

3. 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传播。如“PETER-2”病毒在每年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3, 6, 9月的13日发作。当然，最令人难忘的便是26日发作的CIH病毒。这些病毒在平时会隐藏得很好，只有在发作日才会露出其本来面目。

4. 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不同程度的影响。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，可将病毒分为良性病毒与恶性病毒。良性病毒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，例如，GENP、小球、W-BOOT等。恶性病毒则有明确的目的，或破坏数据、删除文件或加密磁盘、格式化磁盘，或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。

5. 不可预见性

从对病毒的检测方面来看，病毒还有其不可预见性。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，因此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。由于病毒的制作技术也在不断提高，因此病毒对反病毒软件永远是超前的。

1.1.3　病毒的破坏目标和攻击部位有哪些

计算机病毒的破坏行为体现了病毒的杀伤能力。其破坏行为千奇百怪，不可能说全，而且难以做详尽的描述。根据现有的病毒资料可以把病毒的破坏目标和攻击部位归纳如下。

1. 攻击系统数据区

攻击部位包括：硬盘主引导扇区、Boot 扇区、FAT 表、文件目录等。

一般来说，攻击系统数据区的病毒是恶性病毒，受损的数据不易恢复。

2. 攻击文件

病毒对文件的攻击方式很多，可列举如下：

删除、改名、替换内容、丢失部分程序代码、内容颠倒、写入时间空白、假冒文件、丢失文件簇、丢失数据文件等。

3. 攻击内存

内存是计算机的重要资源，也是病毒攻击的主要目标之一。病毒额外地占用和消耗系统的内存资源，可以导致一些较大的程序难以运行。

病毒攻击内存的方式如下：占用大量内存、改变内存总量、禁止分配内存、蚕食内存等。

4. 干扰系统运行

病毒会干扰系统的正常运行，以此作为自己的破坏行为。此类行为也是花样繁多，例如：不执行命令、干扰内部命令的执行、虚假报警、使文件打不开、使内部栈溢出、占用特殊数据区、时钟倒转、重启动、死机、强制游戏、扰乱串行口、并行口等。

5. 速度下降

病毒激活时，其内部的时间延迟程序启动，在时钟中纳入了时间的循环计数，迫使计算机空转，计算机速度明显下降。

6. 攻击磁盘

攻击磁盘的行为包括攻击磁盘数据、不写盘、写操作变成读操作、写盘时丢失字节等。

7. 扰乱屏幕显示

病毒扰乱屏幕显示的方式很多，可列举如下：字符跌落、环绕、倒置、显示前一屏、光标下跌、滚屏、抖动、乱写、吃字符等。

8. 键盘

病毒干扰键盘操作，已发现有下述方式：响铃、封锁键盘、换字、抹掉缓存区字符、重复、输入紊乱等。

9. 喇叭

许多病毒运行时，会使计算机的喇叭发出响声。有的病毒作者通过喇叭发出种种声音，有的病毒作者让病毒演奏旋律优美的世界名曲，在高雅的曲调中去杀戮人们的信息财富。已发现的喇叭发声有以下方式：演奏曲子、警笛声、炸弹噪声、鸣叫、咔咔声、嘀嗒声等。

10. 攻击 BIOS

在机器的 BIOS 区中，保存着系统的重要数据，例如，系统时钟、磁盘类型、内存容量等，并具有校验和。有的病毒激活时，能够对 BIOS 区进行写入动作，破坏系统 BIOS 中的数据。

11. 干扰打印机

典型现象为：假报警、间断性打印、更换字符等。

1.1.4　常见病毒有哪几类

按照计算机病毒属性的区分进行分类，可以有下面的几类：

1. 按照计算机病毒存在的媒体进行分类

根据病毒存在的媒体，可以划分为网络病毒、文件病毒、引导型病毒。

网络病毒通过计算机网络传播感染网络中的可执行文件，文件病毒感染计算机中的文件（如，COM, EXE, DOC 等），引导型病毒感染启动扇区（Boot）和硬盘的系统引导扇区（MBR）。

还有这三种情况的混合型，例如，多型病毒（文件和引导型）感染文件和引导扇区两种目标。这样的病毒通常都具有复杂的算法，它们使用非常规的办法侵入系统，同时使用了加密和变形算法。

2. 按照计算机病毒传染的方法进行分类

根据病毒传染的方法可分为驻留型病毒和非驻留型病毒。

驻留型病毒感染计算机后，把自身的内存驻留部分放在内存（RAM）中。这一部分程序挂接系统调用并合并到操作系统中去，并处于激活状态，一直到关机或重新启动。

非驻留型病毒在得到机会激活时并不感染计算机内存。一些病毒在内存中留有小部分，但是并不通过这一部分进行传染，这类病毒也被划分为非驻留型病毒。

3. 按照计算机病毒破坏的能力进行分类

根据病毒破坏的能力可划分为以下几种。

良性病毒：仅仅显示信息、奏乐、发出声响，自我复制等。它除了传染时减少磁盘的可用空间外，对系统没有其他影响。

恶性病毒：封锁、干扰、中断输入输出、使用户无法打印等正常工作，甚至电脑终止运行。这类病毒在计算机系统操作中造成严重的错误。

极恶性病毒：死机、系统崩溃、删除普通程序或系统文件，破坏系统配置导致系统死机、崩溃、无法重启。这些病毒对系统造成的危害，并不是本身的算法中存在危险的调用，而是当它们传染时会引起无法预料的和灾难性的破坏。

灾难性病毒：破坏分区表信息、主引导信息、FAT，删除数据文件，甚至格式化硬盘等。

4. 按照计算机病毒特有的算法进行分类

根据病毒特有的算法，病毒可以作如下划分。

伴随型病毒

这一类病毒并不改变文件本身，它们根据算法产生 EXE 文件的伴随体，具有同样的名字和不同的扩展名（COM）。例如，XCOPY.EXE 的伴随体是 XCOPY.com。病毒把自身写入 COM 文件并不改变 EXE 文件，当 DOS 加载文件时，伴随体优先被执行，再由伴随体加载执行原来的 EXE 文件。

蠕虫型病毒

此种病毒通过计算机网络传播，不改变文件和资料信息，利用网络从一台机器的内存传播到其他机器的内存、计算网络地址，将自身的病毒通过网络发送。有时它们存在于系统内，一般除了内存不占用其他资源。

此为试读，需要完整PDF请访问：www.ertongbook.com