电脑应用不求人系列丛书

网络安全与防黑技术

孙 锋 编著

- 病毒知识
  防毒软件
  病毒FAQ
- 黑客知识
  防火墙软件
  黑客FAQ
- 密码知识
  密码破解
  密码FAQ

机械工业出版社
China Machine Press

电脑应用不求人系列丛书

网络安全与防黑技术

孙 锋 编著

机 械 工 业 出 版 社

本书立足于扩展读者的知识面，以增强计算机用户的安全使用为出发点，使用户能有效地抵御病毒、防范黑客的侵袭，能正确地安装杀毒软件、设置防火墙，在特殊问题上可以手动排除故障，处理疑难、防患于未然，安全有效地使用计算机。

本书借鉴了大量的科技文献，内容丰富，针对当前实际问题，并从基础应用开始讲解，适用于广大计算机爱好者。

图书在版编目（CIP）数据

网络安全与防黑技术/孙锋编著.
-北京：机械工业出版社，2004.3
（电脑应用不求人系列丛书）

ISBN 7-111-14131-8

Ⅰ. 网… Ⅱ. 孙… Ⅲ. 计算机网络-安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2004）第 017249 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：夏孟瑾　　版式设计：谭奕丽
北京中加印刷有限公司印刷 • 新华书店北京发行所发行
2004 年 4 月第 1 版第 1 次印刷
787mm×1092mm 1/16 • 21.5 印张 • 488 千字
0001-5000 册
定价：28.00 元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话：（010）68993821、88379646
封面无防伪标均为盗版

前　言

随着信息技术的发展，网络正悄然而迅速地走进我们的日常生活。遍布全球的互联网络使任意一个角落的人都可以与远在万里的陌生人即时进行信息交流，如发送电子邮件、传输各种文件、浏览网页资料、网络软件在线安装、即时信息讨论等。它使各行各业都发生了深刻的变化，如今的网络已成为人们生活中不可缺少的一部分，人类社会对信息网络系统的需求和依赖程度正在日益增加。

在人们从网络中获得巨大收益的同时，网络所带来的负面影响促使着人们不得不面对一个现实：由于网络庞大的覆盖性、繁杂的多样性，使得其与计算机系统的基本安全“最少即是最安全的”原则相违背。网络的脆弱性也随之相对明显，网络的安全隐患比比皆是，各种各样的安全漏洞、安全问题接连不断。

作为普通的网络用户，人们都有着共同的忧虑——病毒、安全、私密。本书正是立足于广大用户的这些普遍问题，将内容划分为病毒、黑客、密码三篇，每篇又分为基础知识、处理方法和常见问题三部分，力求全面拓展用户的防护知识并解决用户的疑难问题。

为了实现广大计算机爱好者的愿望，特推出“电脑应用不求人”系列丛书，帮助全面而快速地掌握各种计算机的应用技能和技巧，包括：

- 《网络安全与防黑技术》
- 《网络操作技术》
- 《电脑系统的维护与优化》
- 《电脑硬件常见问题与故障排除》
- 《电脑软件常见疑难问题详解》

这些丛书的内容都与计算机的日常应用密切相关，是用户日常学习工作的好帮手。

为了让计算机用户能更快地理解和掌握图书的内容，我们采用了“提出问题”、“解决问题”的方式，精心筛选了诸多疑难问题，并给出详细的解决方法，让读者在阅读的时候不仅可以循序渐进，而且可以对号入座，及时解决常见的计算机软件使用问题，轻松提高自己的计算机应用能力和操作能力。

参与本书的编写及校对工作的还有：孙丽娟、贾清新、杨敏、周末、袁江、张卫娜、崔增岗、王小丽、王静、王杰江、魏淑兰、王瑞省、孙泽欣、刘艳芬、刘沛勇、王清维等，在此表示感谢！

由于时间有限，书中疏漏之处在所难免，诚望广大读者予以批评指正。

编　者

目　录

第一篇　病　毒　篇

[不求人！]

附 录

第一篇 病毒篇

随着计算机的普及，几乎所有的用户都知道计算机病毒的概念，而大多数人对计算机病毒还不是很了解，认为其高深莫测。虽然为其计算机安装了杀毒软件、设置了防火墙，但新病毒依然不断问世，防不胜防。据统计，每天都会有新病毒诞生，而且病毒形式和破坏力非同小可。而事实上计算机病毒并不是什么可怕的灾难，对病毒的认识与防范有助于我们处理与解决计算机中遇到的问题，以便更有效地应用计算机。

第1章 病毒知识

1.1 计算机病毒的基本定义

所谓计算机病毒，指的是一段被刻意写成的可执行程序，该程序会自动寻找“宿主”并且依附在它上面，例如计算机的磁盘扇区、可执行文件和内存等。不论寄宿的对象是谁，病毒都会想尽办法延长自己的生命。

正常的程序不会有寻找并依附在宿主上的操作，因此，这种具有传染特性的程序就被称为病毒(Virus)。计算机病毒其实就是一个程序，它和我们平常所使用的 IE、Word、Outlook 软件一样，都是属于计算机软件，只不过这种程序拥有和细菌一样独特的“寄生”、“感染”、“繁殖”、“破坏”等特性，所以称其为病毒。

简单来说，病毒就是一段非常小的程序（通常只有几千字节或者几百字节），它会不断地自我复制、隐藏、感染其他的软件程序或计算机，然后伺机执行一些（破坏）动作。

在计算机领域里，电子邮件、文本文件、可执行文件，甚至网页都是计算机病毒的活动领域。但说到底，计算机病毒如同正常的文本软件和游戏程序一样，不过是计算机中执行的程序。它们之间的差别就在于正常的程序可以帮助用户省时省力地完成许多工作，而计算机病毒则减慢计算机的运行速度，让文件数据或系统毁于一旦。

1.2 计算机病毒的危害

多数病毒并不以破坏为目的，但是病毒程序具有传染性，会间接导致操作系统运行速度变慢、兼容性变差、浪费磁盘空间等许多副作用。而少数恶性病毒会删除磁盘数据、格式化磁盘，甚至清除计算机的 BIOS 设置，但最令人气愤的是，有些病毒会假借计算机用户的名义到处散播有毒邮件，泄漏用户的个人隐私、商业机密，或在计算机里安装“后门”程序，让网络黑客轻易地控制计算机并作为跳板来危害他人，到最后这个黑锅却得由计算机用户来背。

一旦计算机被病毒入侵，不但会对计算机数据的安全构成极大的危害，而且稍有不慎就会伤害到许多无辜的人，使灾情如滚雪球般越滚越大。这些计算机病毒虽然具有在瞬间将数据化为乌有的能力，但是只要处理得当，就技术上来说计算机用户可以控制它的感染范围、有效降低损失，而且多数病毒发作所破坏的数据是可以通过特殊的方法复原的。用户需要做的善后工作是建立全面的防御体制，降低计算机病毒入侵的可能性。

计算机病毒会对计算机系统的软件或者硬件造成破坏。根据目前计算机病毒的破坏程度，大致可分为以下几种情况。

1. 系统速度变慢甚至死机

计算机病毒因为要在后台进行自我复制、感染的工作，所以它必须要驻留在内存中伺机执行，因此，计算机速度会被病毒这些额外的工作占用大量的资源，使得速度变慢，情况严重的话，甚至死机。

2. 硬盘容量减小

计算机病毒既然是计算机程序的一种，所以它一定也需要占用磁盘空间，因此，计算机病毒大量自我复制，感染其他文件，造成硬盘空间的急剧减小，直至网络系统崩溃。

自从“梅丽莎”病毒出现以后，目前许多新的计算机病毒（如 Nimda、求职信病毒等）都开始利用网络系统的漏洞大量地复制和传播，这些病毒大多利用系统漏洞和电子邮件把病毒大量地寄给感染者，一传十、十传百，这样大量的电子邮件就涌入了服务器，造成网络拥塞，甚至崩溃。

计算机病毒最令人发指的就是破坏数据。例如，前几年比较流行的 CIH 病毒，就是破坏用户的硬盘分区表，让用户的计算机无法启动。更有甚者，CIH 病毒还可以利用主板 BIOS 的一个设计缺陷，在 BIOS 中写入空数据，使用户的计算机陷入一片黑屏的状态，不得不送入厂家进行维修。

1.3 计算机病毒的传播途径

计算机病毒实际上是一种程序。而程序必须要执行才能有所动作，计算机会中毒就是因为用户执行了被感染病毒的文件，或者被他人利用系统漏洞非法执行了病毒文件。计算机病毒因为拥有高度传染性，所以使用者常常在莫名其妙的情形下就感染上了病毒。计算机病毒的传播途径也是有章可循的，根据目前计算机的使用情况，可以把中毒的原因简单地归为 5 类：

1. 执行了网络上中毒的文件

网络上下载的文件已经被感染，执行以后，用户的计算机就会中毒。

这里所谓的网络是广义的网络，包括企业内的局域网和大家通常使用的互联网。当用户从网络中获取一个感染病毒的软件，或是收到的电子邮件中含有病毒，或在不经意间浏览网页时，都有可能中病毒。根据统计，目前通过网络感染的病毒已经比通过磁盘和光盘感染的病毒高出 100 倍。可见，网络已经成为最大的病毒传播途径。

2. 执行了磁盘、光盘上中毒的文件

磁盘和光盘中的文件已经被感染病毒，运行以后，用户的计算机就会感染病毒。

3. 使用中毒的磁盘或光盘启动

磁盘或光盘的引导扇区已经中毒，当使用这种磁盘或光盘启动时，用户的计算机就会感染病毒。

当文档文件感染了宏病毒而用 Word、Excel 等打开时，就会执行其中的宏病毒，然后用户的计算机就会感染病毒。

不小心使用了含有病毒的软盘或者光盘启动，计算机就会感染开机型病毒。

不小心执行了感染了磁盘或者光盘中感染病毒的文件，计算机就会感染文件型病毒。

计算机系统已经感染了病毒，在用户访问磁盘或者将已经感染病毒的文件刻录到光盘内时，这些病毒就乘机感染磁盘和光盘，然后再继续传播。

4. 收到的电子邮件含有病毒

电子邮件的附件中含有病毒文件，执行附件以后，用户的计算机就会感染病毒。

5. 利用操作系统的漏洞

Nimda 等病毒，都是利用 Windows 操作系统的一些系统漏洞来修改网站 htm、html、asp 等文件，在用户浏览这些网页时，系统就会中毒。

知道了中毒的原因，下面我们就针对这些原因，介绍如何避免一些操作，以降低中毒的概率：不要随便执行、启动电子邮件中的文件；不要随便下载陌生网站上的文件；不要随便使用来源不明的软件和文件；不要使用不安全的磁盘启动；不要随便启动 Office 的宏功能。

1.4 计算机病毒的分类

研究计算机病毒需要科学系统地对病毒划分种类，并制成一本病毒家族谱，当遇见新病毒时方便索查。

对病毒进行分类的方法有很多种。基于技术的分类方法是计算机病毒的基本分类法，通过技术分类可以更容易理解病毒的概念，以后计算机中毒时能对症下药。某些类型病毒虽然按技术分类法可以被划归到一类，但是因为其技术特点往往会被单独分类，比如宏病毒实际上也可以看成是文件型病毒的一种，这种病毒利用了 Office 软件的宏功能，将病毒加在文本、表格等类型文件上，一旦中毒文件被打开，病毒程序便会立刻执行，这是目前侵害办公室计算机系统的主要凶手。

1.4.1 网络病毒

此类病毒通过网络传播，并且不依附于文件等传统宿主，它直接寄生在内存中。这是目前最新的一类计算机病毒，典型代表是“红色代码”病毒。

网络病毒利用网络不断寻找有安全漏洞的计算机，侵入并寄生在内存中，伺机进行下一步动作。如果将网络上的所有计算机都同时关机，这些病毒自然就会被清除了，但在真实世界是不可能实现的。此类病毒是目前最新发现的病毒，因此它将来会如何演化还不确定。

1.4.2 邮件病毒

邮件病毒主要是利用电子邮件软件的漏洞进行传播的计算机病毒，属于目前最热门的病毒之一。一般而言，此类病毒是利用电子邮件的客户端软件（如 Outlook）的漏洞来传播，感染邮件服务器的情况较为少见。

Internet 将整个世界连在一起，人们都使用电子邮件进行沟通，一旦某个人的邮件软件被感染，那么该受害者通信簿中的其他人很快便会收到病毒邮件，如此循环，使邮件病毒的传播速度按照等比级数增长，它比以往任何一种病毒的感染能力都强而且快。不过，此种类型的病毒往往会因为病毒邮件散播的速度太快，导致邮件服务器负载过大而崩溃，从而间接减小病毒的危害范围。最新的邮件病毒种类众多，较知名的有“梅丽莎”（Melissa）病毒和“妮姆达（Nimda）病毒等。

1.4.3 文件型病毒

文件型病毒也属于目前最常见的计算机病毒，它是附加在 EXE 和 COM 等文件上执行的计算机病毒。

在 MS-DOS 时代，文件型病毒达到一个发展高峰；到了 Windows 操作系统时代，这种病毒数目大大减少。这是因为 MS-DOS 可执行文件的相关技术是公开的，文件型病毒容易编制，因而特别流行。到了 Windows 操作系统时期，微软对 Win32 的可执行的二进制文件的结构数据披露较少，它只被掌握在为数甚少的技术人员手中，所以 Windows 操作系统的文件型病毒比较少见。近期最厉害的文件型病毒就是 CIH，其程序代码真是又漂亮又简洁。

文件型病毒又分为非常驻型病毒与常驻型病毒两大类。

1. 非常驻型文件病毒

是指在宿主程序执行时同步执行的病毒程序，其传染与破坏的动作一并进行；宿主程序执行结束时，病毒程序也结束。

2. 常驻型文件病毒

是指在宿主程序执行时也执行的病毒程序，它同时进行传染与破坏操作，在宿主程序执行结束时，病毒程序仍然驻留在内存，继续进行传染与破坏操作。

1.4.4 宏病毒

办公软件（如 Microsoft Word、Excel 等）是经常使用的应用程序，这类软件一般都支持宏（Macro）（如微软的 Office 产品支持的宏编辑器是 Visual Basic）。这些宏可以方便地完成一些重复繁琐的操作，但是这一项功能往往被变相利用作为计算机病毒的制作工具。宏病毒是利用宏编写的计算机病毒，它附加在各种文档和表格文件上，文件被办公软件打开时，会自动执行病毒程序并将其扩散。宏病毒的出现打破了非 EXE、COM 文件不能携

带病毒的旧观念。由于宏容易制作，所以各式各样的宏病毒不断被创造出来。最近出现了生成宏病毒的软件，它使不懂 Visual Basic 的人制造病毒更加方便了。目前在企业的计算机系统中宏病毒仍然相当泛滥。

其实，防范宏病毒并非难事，目前的杀毒软件都有防范未知宏病毒的功能，微软的新版办公软件已经具备了一定程度的防范能力。

1.4.5 引导型病毒

这种病毒感染系统启动区的 MBR 和系统文件，在操作系统启动之前会将病毒程序植入内存。

此类病毒在 MS-DOS 操作系统时代特别猖獗，主要原因是 MS-DOS 的启动原理及操作系统内核比较简单，而且相关的技术数据比较容易获得，编制此类病毒程序的难度并不高。到了 Windows 95/98 流行的时代，操作系统的体系结构较以往不同，引导型病毒无法对操作系统造成太大的伤害。目前常用的 Windows 2000/XP/NT 操作系统，微软公司对其核心技术并未完全公开，因此编制此类病毒的技术难度大大增加，所以此类病毒已经很少见了。

引导型病毒又分为普通引导型病毒与隐密引导型病毒两大类。

1. 普通引导型病毒

这类引导型病毒直接修改启动区的引导程序，以使病毒程序可以被自动加载到内存。

2. 隐密引导型病毒

这类引导型病毒同样是修改启动区的引导程序，而使病毒程序能被自动加载到内存。但感染此病毒后，即使检查启动区，所得结果仍是正常的扇区数据，就好像没有中毒一样，此类型病毒不易被觉察。

1.4.6 变体病毒/千面人病毒

这是高级的文件型病毒，其特点是每次进行传染时都会改变程序代码的特征，以防杀毒软件的追杀。

此类病毒的算法比一般病毒复杂，其制作者编写程序的水平较高。病毒制作者之所以会开发变体病毒，是因为早期的杀毒程序比较依赖于用固定的病毒特征码来检测计算机病毒，因此一些聪明的病毒制作者就使用数学算法为病毒程序加密，使病毒程序每次都呈现不同的型态，让杀毒软件检测不到。正因为如此，变形病毒的制作难度较高，自然较为少见。

1.4.7 其他类型的病毒

除了以上病毒类型之外，还有一些其他类型的病毒及有害程序，如 Java 病毒、PDF 病毒、图文件病毒和目录型病毒等，但都很罕见。

1.4.8 混合型病毒

混合型病毒指兼具两个以上病毒类型特征的计算机病毒，例如有些文件型病毒同时也是开机型病毒。

目前最猖撅的邮件病毒中有很多都是文件型病毒和宏病毒的混合体，以前流行的“文件-开机混合型”病毒随着开机型病毒的消亡，已渐渐退出病毒制作领域。单一传播渠道的病毒在许多病毒制作者眼里越来越不够水准，因此混合型病毒必会不断演化下去并整合进更多的新技术。虽然此类病毒看起来厉害，但实际上因整合不同病毒技术于一体是件高难度的工作，所以此类病毒的经典作品甚少。再者，因为此类病毒必须具备不同的功能而容易造成程序代码过长、不灵活等缺点，而且经常得冒着容易被杀毒软件检测到的危险，所以此类病毒数量很少。

1.5 计算机中毒的可能征兆

系统感染病毒是十分危险的事情，因为你不知道病毒发作会对系统造成什么破坏。所以在计算机出现中毒的征兆时，就应该检测是否感染了病毒，以免病毒发作而后悔莫及。那么到底计算机中毒有哪些征兆呢？以下将作介绍。

1. 计算机执行速度越来越慢

计算机病毒会在后台不断地复制、传播，所以会耗用系统的资源，使得计算机的执行速度越来越慢，因此当发现系统无缘无故地变慢时，就应该考虑是否感染了病毒。这时建议使用查毒软件进行查毒。

2. 原来可以执行的一些文件无缘无故不能执行

文件型计算机病毒会将自己寄生在可执行文件中，因此可能出现文件被病毒感染后无法执行的错误，这时候最好对系统进行查毒工作，看看这些文件是否已经中毒。

3. 系统通常莫名其妙地死机

计算机病毒感染系统是不分对象的，它可能感染 Windows 系统的一些重要的文件，当系统的重要文件被感染时，Windows 系统就变得非常不稳定，甚至常常死机，这时候要找到死机的原困，首先应该考虑系统是否中毒。

4. 网络速度变慢或者一些莫名其妙的网络连接

现在很多新的计算机病毒会利用互联网来进行传播，当这类程序感染系统时，用户会发现连上互联网时，虽然没有执行任何程序，但网络连接状态不断闪烁，而且当你查看本地连接状态时，发现发送和收到的数据包数不断变化。这时用户的系统就很有可能已经感染了病毒或者“特洛伊木马”程序，它们正通过网络向外传播。此时如果发现网络越来越慢，那么计算机中毒的概率就相当高，应尽快对系统进行查毒工作。

[不求人！]