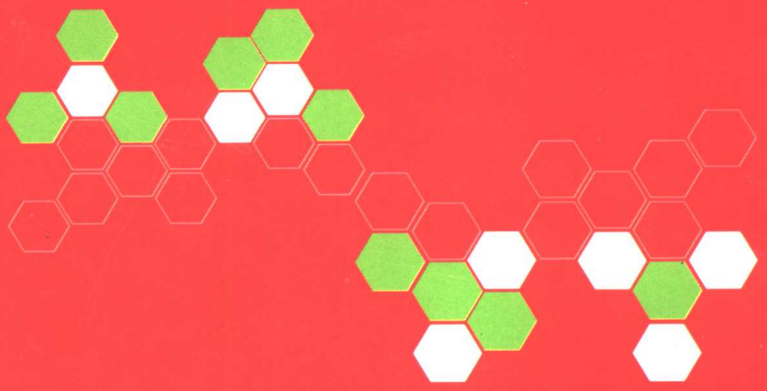
计算机技巧百科

黑客论剑



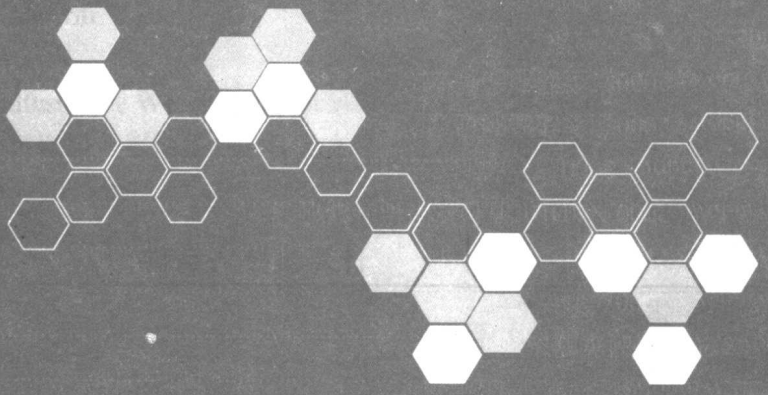
数码时代

今网报 JINWANGYIN

珠海出版社

计算机技巧百科

黑客论剑



珠海出版社

图书在版编目（CIP）数据

黑客论剑/网垠科技编，—珠海：珠海出版社，
2001.9（2004.4 重印）
（计算机技巧百科）

ISBN 7-80607-819-3

Ⅰ.黑… Ⅱ.网… 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 029582 号

计算机技巧百科

责任编辑：雷良波
选题策划：网垠
封面设计：李翔
出版发行：珠海出版社
社　　址：珠海市银桦路 566 号报业大厦三层
邮政编码：519002
电　　话：（0756）2639330
印　　刷：郑州市毛庄印刷厂
开　　本：889×1194mm　1/16
印　　张：166
字　　数：3320 千字　　**印数**：10000~11000 册
版　　次：2004 年 5 月第 1 版第 2 次印刷
书　　号：ISBN 7-80607-819-3/TP·8
定　　价：200.00 元（全十册）

卷首语

Internet在全球蓬勃发展，它给人们的生活带来极大方便，黑客的出现却使这些便利的背后有可能潜伏着致命的陷阱。采取何种有效的方式保障个人、公司乃至国家的信息安全已成为众人瞩目的话题。

本书从网络安全所涉及的攻击和防御正反两个方面入手，在深入剖析各种黑客攻击手段的基础上，对相应的防御对策进行了系统地阐述：第1章主要帮助读者认识黑客和木马，讲述了什么是黑客、黑客简史、黑客基本技能，以及木马类型、特征、原理等；第2章介绍了网络的基本知识，内容有网络结构、网络协议、网络监听、网络攻击、拒绝服务的攻击，以及局域网、广域网的安全等；第3章讲述了黑客攻击手段，内容有攻击的一般模式、追踪黑客、黑客攻击过程、黑客入侵方法等；第4章讲述了黑客攻击及防范，内容有计算机硬件安全问题、攻击的层次、炸弹攻击、DDOS攻击、网络安全工具、防止黑客侵害网络、清除黑客程序、防范OICQ的黑客程序等；第5章讲述了漏洞入门，内容有发现安全漏洞、一些路由协议的漏洞等；第6章讲述了服务器漏洞及解决方案，内容有Windows漏洞及解决、Windows 2000漏洞及解决、Unicode漏洞入侵及解决、缓冲溢出漏洞、CGI漏洞及防范措施、ASP漏洞等；第7章讲述了电脑病毒的防范，内容有病毒的存储结构、病毒工作原理、常见病毒的类型、病毒的分析及解决方法、Burglar病毒的分析和防治、防毒安全工具等。

本书最后附木马的清除集锦、CGI安全漏洞资料速查。本书的最大特点就是可操作性强，除介绍必要的基础知识并深入分析其原理外，还介绍了典型工具及其应用，力求让读者在实际运用中建立起对网络安全深刻的认识。

本书面向广大的计算机网络用户，适合从事网络系统管理的专业技术人员阅读，也可供对网络安全技术感兴趣的读者参考。

内容提要

随着网络技术的日益发展和信息技术的广泛应用，人们对信息网络的依赖程度越来越高，而非法入侵者和黑客所造成的破坏也越来越严重。

本书较全面地介绍了当前计算机黑客使用的各种技术、攻击手段、攻击行为造成的后果及其防范措施。在讲述原理的同时结合了大量的实例，并介绍了各种防范对策，内容包括：黑客与木马入门、网络基本知识、黑客攻击手段、黑客攻击及防范、漏洞入门、服务器漏洞及解决方案、电脑病毒的防范。

本书面向广大的计算机网络用户，适合从事网络系统管理的专业技术人员阅读，也可供对网络安全技术感兴趣的读者参考。

Contents 目录

第一章 黑客与木马入门

第二章 网络基本知识

Contents 目录

Contents
目录

Contents 目录

Contents
目录

第一章　黑客与木马入门

尽管资深的黑客不屑于使用木马，但在对以往网络安全事件的分析统计里，我们发现，有相当部分的网络入侵是通过木马来进行的，包括去年微软被黑一案，据称该黑客是通过一种普通的蠕虫木马侵入微软的系统的，并且窃取了微软部分产品的源码。

木马的危害性在于它对电脑系统强大的控制和破坏能力，窃取密码、控制系统操作、进行文件操作等等，一个功能强大的木马一旦被植入你的机器，攻击者就可以像操作自己的机器一样控制你的机器，甚至可以远程监控你的所有操作。

1.1　认识黑客

不少人认为黑客就是在网络上非法侵入别人机器的人，但除了黑客外，我们还常常听到骇客、怪客的称呼，一些人也郑重其事地站出来声称黑客与骇客是不一样的（对于我们，红客也仅是一个称谓而已，一般可以和黑客一样理解），他们声称黑客创造东西，而骇客只会破坏，另外，还有一些人也将那些只会破坏的入侵者称为怪客。那么，究竟什么才是真正的黑客、骇客、怪客呢？

1.1.1　什么是“黑客”（Hacker）

事实上，黑客也就是英文Hacker的音译，Hacker这个单词源于动词Hack，这个词在英语中有“乱砍、劈、砍”之意，还有一个意思是指“受雇于从事艰苦乏味工作的文人”。Haker的一个引申意义是指“干了一件非常漂亮的事”。在二十世纪60年代的时候，电脑系统是非常昂贵的，都只是存在于各大院校与科研机构的玻璃房中，技术人员使用一次电脑需要很复杂的手续，而且电脑的效率也不是很高，为了绕过一些限制，最大限度地利用这些昂贵的电脑．最初的程序员们就写出了一些简洁而有效的捷径程序，这些程序往往较原有的程序系统更完善，而这种行为便被称为Hack。而在早期的麻省理工学院里，“Hacker”有“恶作剧”的意思。尤指那些手法巧妙、技术高明的恶作剧。可见，至少是在早期，黑客这个称谓并无贬义。

“破解不是学习使用一个什么软件，不是按照说明书来操作，它是一种人和人智力的较量，是一种智慧的战争艺术，是一种知识与知识的较量。从本质上讲，学习破解跟学习其他知识一样，都是要下苦功夫，要靠灵感，要靠自己思考的。”这就是黑客们对自己的行为的诠释。

1.1.2　什么是“怪客”与“骇客”（Craker）

骇客、怪客——是Cracker的音译，就是破坏者的意思。更多地被解释为商业软件、恶意入侵别人的网站造成损失。

怪客具有与黑客同样的本领，只不过是在行事上有些差别而已，这也是我们常常很难分清骇客与怪客的原因之一。

其实，黑客也好，骇客、怪客也好，名称只是一种代号而已（红客也是如此，仅是一种代号，大家不

用刻意追求），应该说他们之间并无绝对的界限，我们也很难将他们区分得很清楚，他们都是非法入侵者。既是非法入侵，再区分什么善意入侵与恶意入侵也没有意义了，而且无论是哪一种入侵，无论是有意还是无意，都有可能造成被入侵者的损失。

1.1.3 怎样才算是一个黑客

首先，黑客绝非是自称的，自称为黑客甚至只是取了一个与黑客相关的名字都会遭到真正的黑客嘲笑。在黑客的圈子里，只有其他的黑客接纳了你，得到其他黑客的认可，你才能算个黑客。其次，你应该具有一定的创造力，仅仅是拿着黑客前辈们所编写的黑客软件到处乱试，一旦出现问题却又束手无策的人，绝对称不上黑客。

此外，一名黑客还应该具有黑客的精神以及黑客的行为，要能够融入黑客们自然形成的黑客文化当中去，你才能算得上是一名黑客。当然，不管怎么样，黑客的技能是必备的。总的来说，要成为一名黑客，你必须是技术上的行家，并且热衷于解决问题，能无偿地帮助他人。

1.2 黑客简史

有一种观点认为黑客对电脑技术的革新作出了不可磨灭的贡献，而近些年来互联网的飞速发展，也有黑客的一份功劳在其中。有些人对此观点嗤之以鼻，但我们只要回顾一下黑客发展的历史，就会发现这种说法并不过分。正如前文所提到的，“Hack”这个称谓在早期是令人自豪的，直到现在，仍有人以被称为Hacker（黑客）而自豪，并以洁身自好的姿态与“Cracher”（怪客）们区分开来。的确，最早的Hacker是一种褒义词，只有那些最优秀的技术专家才能被冠以Haker的称号。这可以追溯到几十年前第一台微机刚诞生的时候。那时因特网的雏形ARPANET也刚刚建立，当时能够使用这个网络的都是一些程序设计专家或科学家等，总之都是一群处于高科技最前沿的人，而正是这些人创造了Hacker这个词。从某种意义上，可以把这些最早的Hacker视为Internet的创始人，正是他们开发出了强大的、迄今仍在使用的Unix操作系统，这就是最早的黑客。他们具有高超的技术、过人的智力以及坚韧的探索未知事物的毅力。他们对电脑技术的发展，对因特网的发展都作出了巨大的贡献，这些“黑客”是值得尊敬的。

但是到了70年代，情况发生了变化，更多的黑客出现了，这些黑客也同样具有高超的技术，他们以侵入别人的系统为乐，随意地修改别人的资料，使黑客这个称谓逐渐变得不那么令人喜欢。同时因为大量的黑客及黑客技术的涌现，加上因特网的发展，让黑客与黑客之间的交流变得更容易，在因特网上也出现了专供黑客交流的BBS。黑客还逐渐形成了科技领域，尤其是电脑领域的一个独特的群体。

1.3 黑客文化

黑客的这个相对群体人数绝对算不上多，但在信息时代的影响却绝不可小看。这些人往往掌握着最先进的技术，一旦他们要将这些技术用于不正当的用途，就是所谓的“怪客行为”的时候，其危害是难以想像的。在黑客出现至今短短的几十年内，他们基本已经形成了自己独有的黑客文化。

要想了解黑客文化，我们可从黑客行为、黑客态度及黑客们自己定下的黑客守规等几个方面来认识。

1.3.1 黑客行为

黑客们一再声称自己与“怪客”的不同，于是便对黑客行为有了各种各样的注释，但总结起来，不外乎以下几条：

1. 不随便攻击个人用户及站点

虽然黑客们在找到系统漏洞并侵入时往往都会很小心避免造成损失，并尽量善意地提醒管理者，但在这过程中有许多因素都是未知的，没有人能肯定最终会是什么结果，因此一个好的黑客是不会随便攻击个人用户及站点的。

2. 多编写一些有用的软件

这些软件都是免费的，但又和一般的共享软件有所不同，因为这些软件的派代码同时也是公开的。

3. 帮助别的黑客测试与调试软件

没有人能写出完全没有一点错误或不要再改进的完美软件，因而对软件的测试与调试是非常重要的，测试与调试软件甚至会比编写软件更耗费精力。但在黑客的世界中，这或许算不了什么，因为在你写出一个软件后，会有许多其他的黑客热心地帮助你测试与调试。

4. 义务做一些力所能及的事

黑客们都以探索漏洞与编写程序为乐，但在黑客的圈子中，除了探索漏洞与编写程序外，还有许多其他的杂事，如维护和管理相关的黑客论坛、新闻讨论组以及邮件列表，维持大的软件供应站台，推动RFC和其他技术标准等等。这些事都需要人来做，但也许并不都是那么令人感到有趣。所以，那些花费大量精力，义务地为网友们整理FAQ、写教程的黑客，以及各大黑客站点的的站主，在网络上都是令人尊敬的。

5. 洁身自好，不与“怪客”混在一起

真正的黑客总是耻于与“怪客”为伍，他们不会随意破解商业软件并将其广泛流传，也不会恶意侵入别人的网站并造成损失。他们所作所为更像是对于网络安全的监督。

1.3.2 黑客精神

1.“Free”（自由　免费）的精神

这是黑客文化的精髓之一，“Free”是黑客最应该具有的态度。

黑客们诞生并成长于开放的互联网，他们解决问题并创造新的东西，他们相信自由并自愿的互相帮助。最明显的一个表现就是在互联网上，黑客们编写的各种黑客软件都是完全免费共享的。甚至连源代码都是公开的。而黑客们在帮助你之后，唯一的要求就是你在成长起来后同样地帮助别人。

“free”可算是黑客的传统精神，也是现代黑客们所尽力保持的。

2. 探索与创新的精神

所有的黑客都是喜欢探索软件程序奥秘的人。他们摸索着程序与系统的漏洞，并能够从中学到很多知识，在发现问题的同时，他们都会提出解决问题的创新方法。

在互联网急剧发展，并在人们生活的方方面面起着越来越重要的作用的时候，正是黑客们探索与创新的精神，使互联网的安全问题得到了人们的重视。

3. 反传统的精神

反传统的精神在黑客们身上表现得最明显不过了，不具备这种精神的人很难想像他会成为一个黑客。而这里的“反传统”主要是指科学技术上的反传统，并不包含任何贬义。

黑客们做得最多的事就是探索与创新（这也是大家要学习的），这都需要他们具有反传统的精神。他们的快乐就源自于攻破传统的东西。

4. 合作的精神

个人的力量是有限的，黑客们很明白这一点，因此才有了那么多供黑客交流的论坛与新闻组。在技术上保守的人是不可能成为黑客的。

最后必须要说明的一点是，所谓的黑客精神不应该是想成为黑客的人所刻意追求的，这是在每一个黑客以及每一个即将成为黑客的人身上自发地表现出来的。

1.3.3 黑客守则

黑客崇尚的是自由，他们有组织，也都是一些松散的、为了讨论技术而存在的组织，而所谓的黑客守则，也不像是我们日常生活中的那样，以各种形式制定的守则，事实上这是一群最崇尚自由的人，他们最不喜欢的就是规则，所以并没有绝对的黑客守则。但黑客对自己的技术都很自豪，不喜欢别人误解自己，也不喜欢别人将黑客与“怪客”、“骇客”之类的混在一起，因而在互联网上便流传着种种黑客们自律的“黑客守则”。

黑客守则有多种版本，比较典型的一种如下：

（1）不要恶意破坏任何的系统，这样做只会给你带来麻烦。

（2）不要破坏别人的软件或资料。

（3）不要修改任何系统文件，如果是因为进入系统的需要而修改了系统文件，请在目的达到后，将它改回原状。

（4）不要轻易地将你要黑的或是经过的站点告诉你不信任的朋友。

（5）不要侵入或破坏政府机关的网络。

（6）已侵入电脑中的账号不得清除或修改。

（7）可以为隐藏自己的侵入而作一些修改，但要尽量保持原系统的安全性，不能因为得到系统的控制权而将门户大开。

（8）不要做一些无聊、单调并且愚蠢的重复性工作。

（9）做真正的黑客，读通所有关于系统安全或系统漏洞的书。

1.4 黑客的基本技能

作为一名黑客，是需要一定的技术深度的，虽然随着技术的发展，黑客们需要不断地学习、尝试使用更新更好的技术，但一些基本的技能应该是必须要掌握的。

1.4.1 程序设计基础

毫无疑问，编程是每一个黑客所应该具备的最基本的技能。但是，黑客与程序员又是不同的，黑客往

往掌握着许多种程序语言的精髓（或说是弱点与漏洞），并且黑客们都是以独立于任何程序之上的概括性观念来思考一件程序设计上的问题。汇编语言、C语言都是黑客们应该掌握的。

黑客们培养这种能力的方法也与常人有所不同，他们也看种种书籍，但更多的是读别人的源代码，这些源代码大多数是前辈黑客们的作品，同时他们也不停地自己写程序。

1.4.2 了解并熟悉各种操作系统

Unix之所以如此受到黑客们的重视，并不仅仅因为它最初就是由黑客所编写的。我们知道，除了Unix外，还有很多操作系统，但能得到源代码任意修改的操作系统只有Unix（还有Linux），更重要的是，Unix是用于网络的操作系统，互联网上有很多主机使用的操作系统都是Unix，至少在目前，互联网还不能没有Unix。因此许多黑客同时也是一个Unix专家，他们清楚Unix这个操作系统的运作过程与基本原理。

除Unix操作系统外，黑客还必须熟知诸如flux Windows Novell等操作系统，才能让自己做黑客如虎添翼。

1.4.3 互联网的全面了解与网络编程

黑客们所创造出来的东西在很多领域都在起着作用，但只有互联网才是黑客们真正的舞台，作为一名黑客，不懂得使用World Wide Web与HTML是不可思议的。

同时，若没有网络知识基础，要做黑客也是无能为力的。

1.5 认识木马

特洛伊木马（以下简称木马），英文叫做“Trojan house”，其名称取自希腊神话的特洛伊木马记，它是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。

1.5.1 什么是木马

木马的定义是具有隐蔽性的，在完成一些有趣功能的同时也做了一些用户不想的功能，并且最终危害到用户的软件。

1.5.2 木马的特征

1. 隐蔽性

很多人的对木马和远程控制软件有点分不清，实际上他们两者的最大区别就是在于这一点，首先举个例子，像国内的血蜘蛛，国外的 Canywhere 等应该是远程控制软件，血蜘蛛等 server 端在目标机器上运行时，目标机器上会出现很醒目的标志。而木马类软件的 server 端在运行的时候应用各种手段隐藏自己，例如，大家所熟悉的修改注册表和 ini 文件以便机器在下一次启动后仍能载入木马程式。有些把 server 端和正常程序绑定成一个程序的软件叫做 exe-binder 绑定程式，可以让人在使用 trojan 化的程式时，木马也入侵了系统，甚至听说有个程式能把 exe 文件和图片文件绑定，在你看图片的时候，木马也侵入了你的系统。

还有些木马可以自定义通信端口，当然这样可以使木马更加隐秘。更改 server 端的图标，让它看起来像个 zip 或图片文件，如果你一不当心，那么就糟了。

2. 功能特殊性

通常木马的功能都是十分特殊的，除了普通的文件操作以外，还有些木马具有搜索 Cache 中的口令，设置口令，扫描 ip 发现中招的机器，键盘记录，远程注册表的操作以及颠倒屏幕，锁定鼠标等功能比较特殊的操作，而远程控制软件的功能当然不会有这么多的特殊功能，毕竟远程控制软件是用来控制的，并非 Hack 的。

这里谈的只是很大一部分的木马工具，但还有些木马工具的功能比较“专”，而且工作的方式也不是 client/server 的方式，例如 Passwd Sender（中文译名：口令邮差）的功能就是潜伏在目标机器里，搜集各种口令的信息，在目标上网的时候，秘密发送到指定的邮箱。在 Unix 下，还有些黑客们修改 ps 的原代码，让 ps 在使用时故意不显示某特殊的进程名，譬如说在系统内的 sniffer 等，还有些黑客们则修改 login，passwd，su 等软件完成一些搜集口令信息或者开放一个后门等功能，这些程序我们都称之为木马。

1.5.3 木马的类型

1. 远程控制型木马

这是现在最流行的木马，每个人都想有这样的木马，因为他们想访问受害人的硬盘，RAT'S （remote accesstrojans）使用起来非常简单，只需要某人运行服务器，你得到受害人的 IP，你对他或她的计算机有完全的访问权，你能做一些事情，它依赖于你使用的木马，但是，RAT'S 有通常的远程控制木马的功能，如：KERLOGGER，上传和下载，MAKE A SCREEN SHOT 等等。有人将木马用于恶意的目的，他们只是想删除又删除……

这是 LAME，但是我们有一个关于使用木马最好方法的指南，你应该读它，有很多用于检测最常用木马的程序，但是新木马每天都出现，这些程序不是最好的防御，木马总是做同样的事情，如果每次 Windows 重新启动的时候木马重启，这意味着它放了什么东西在注册表或 WIN.INI 或其他的系统文件里，因此它能重启，木马也可能在 Windows 系统目录里生成一些文件，这些文件总是看起来像一些受害人认为是正常的 Windows 可执行文件。绝大多数木马隐藏在任务表 Most trojans hide from the Alt+Ctrl+Del menu 中，有人会用 ALT+CTRL+DEL 键来查看哪些进程正在运行，这是不好的，有些程序会正确地告诉你进程和文件来自哪儿，但是有一些木马使用伪造的名字，对有些人来说，要决定哪个进程应该杀死是有一点困难的。

远程控制木马打开一个端口，让每一个人都可以连上你的电脑。有些木马的选项想改变端口和设置密码，以使只有那个感染你的家伙可以使用你的电脑。改变端口选项是非常好的，因为我们确信你不想让你的受害人看见他的电脑上的端口 31377 是开着的。远程控制木马每天都在出现，而且将继续出现。对那些使用这样的木马的人：小心感染你自己，因为那些你想毁灭的受害人将会报复，你将会感到难过。

2. 发送密码型木马

这些木马的目的是得到所有缓存的密码，然后将他们送到特定的 E-mail 地址，不让受害者知道 E-mail。绝大多数情况下，这种木马在 Windows 每次加载的时候不重启，它们使用端口 25 发送邮件，也有一些木马发送其他的信息如 ICQ，计算机信息等等。如果你有任何密码缓存在你电脑的任何地方，这些木马对你是危险的。

3. Keyloggers

这些木马是非常简单的，它们做的唯一的事情就是记录受害人在键盘上的敲击，然后在日志文件中检

查密码。在大多数情况下，这些木马在 Windows 每次加载的时候重启，它们有在线和下线的选项，当用在线选项的时候，它们知道受害人在线，会记录每一件事情。然而，当用下线选项的时候，Windows 开始后被写下的每一件事情会被记录并保存在受害人的硬盘等待传送。

4．破坏型木马

这种木马的唯一功能是毁坏和删除文件，使它们非常简单易用。它们能自动删除你计算机上所有的 DLL，EXE，INI 文件，这是非常危险的木马，一旦你被感染，毫无疑问，如果你没有清除，你的计算机信息将不再存在。

5．FTP型木马

这种木马在你的电脑上打开端口 21，让任何有 FTP 客户软件的人都可以不用密码连上你的电脑并自由上传和下载。

这些是最常用的木马，它们都是危险的，你应该小心使用它们。

1.5.4 木马的发展

1．跨平台性

主要是针对 Windows 系统而言，木马的使用者当然认为一个木马可以在 Windows 95/98 下使用，在 Windows NT、Windows 2000 下也可以更好地使用。在 Windows 95/98 下大家也许没感觉，但 Windows NT 和 Windows 2000 都具有了权限的概念，这和 Windows 95/98 是不同的，黑客 Windows NT、Windows 2000 的木马需要更高的手段，如控制进程等，现在的一些木马也的确做到了这一点。

2．模块化设计

似乎模块化设计是一种潮流，Winamp 就是模块化的典范，现在的木马也有了模块化设计的概念，像 bo，netbus，sub7 等经典木马都有一些优秀的插件在纷纷问世，这就是一个很好的说明。

3．更新更强的感染模式

传统的修改 ini 文件和注册表的手法已经不能适应更加隐秘的需要，目前很多木马的感染方式已经开始在悄悄转变，像前一阶段的 YAI 事件就给了我们很多的启发，像病毒一样的感染，感染 Windows 下的文件，这件事对木马设计者们有很多的启发。

4．即时通知

木马是否已经装入？目标在哪里？如果中招的人是使用固定 IP，还好说，如果目标使用的是动态 IP，那怎么办？现在的木马已经有了即时通知的功能，如 IRC，ICQ 通知等，但还是太少，以后会更加地完善的，说不定某一天木马们的即时通知功能会变成了一个专门的软件。

5．更强更多的功能

每个人都是不满足的，每当出现强大功能的时候，我们就期望更强大的功能，以后木马的功能会如何呢？也许会让大家大吃一惊的。

1.5.5 木马的构成

在介绍木马的原理之前，有一些木马构成的基础知识我们要事先加以说明，因为下面有很多地方会提到这些内容。一个完整的木马系统由硬件部分、软件部分和具体连接部分组成。