电脑报 总策划

木马攻防全攻略

万立夫 编著

Trojan

深入剖析
木马入侵手法

揭秘木马伪装的伎俩
真枪实弹向黑客宣战！

走进木马的世界 初探传统的C/S型木马
以无招胜有招 适用于任何环境的B/S型木马
小到无形的杀手 警惕“一句话木马”
让防火墙形同虚设 “反弹连接”成主流
绑架系统进程 “线程插入”技术
IE浏览器被劫持 利用80端口上线的“HTTP隧道技术”
马甲花招 多重木马加壳实战演示
改头换面 修改特征码巧过杀毒软件
道魔谁更高 突破主动防御有新招

10套木马攻防工具

电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

电脑报 总策划

木马攻防全攻略

Trojan

万立夫 编著

电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

内容简介

如今的网络世界中，木马带来的安全问题已经远超病毒，它们如幽灵般地渗入到计算机中，已成为监控、窃取和破坏我们信息安全的头号杀手。本手册融合了作者多年的研究成果，真实再现了木马配置、伪装、防杀、植入的全过程，深入浅出地讲解了如“反弹连接”、“线程插入”、“隧道技术”、“键盘记录”、“特征码修改”、“添加花指令”等热点问题，解决困挠大多数木马研究者的疑问！

一直以来，由于公众对木马知之甚少，才使得木马有机可乘，我们坚信只有将木马的伎俩公诸于众，才能更好地提升公众的安全意识，真正捍卫我们的信息财富。本手册可作为网络管理员、网络安全人员的参考资料；此外，对于那些饱受木马威胁的 Windows 用户也具有积极的指导作用。

警告：本手册在内容讲述中列举了部分木马攻防实例，目的在于揭露木马的真实面目，方便读者理解并更好地鉴别它，防范它。读者切不可利用所讲述的内容入侵他人电脑，否则将被追究法律责任！

光盘要目

1.金山毒霸
2.金山网盾
3.加密工具
4.伪装工具
5.捆绑工具
6.漏洞利用
7.扫描软件

名　　称：木马攻防全攻略
编　　著：万立夫
技术编辑：何　磊
版式设计：向海蓉　姚永福
出版单位：电脑报电子音像出版社
地　　址：重庆市双钢路 3 号科协大厦
邮政编码：400013
对外合作：(023)63658933
发　　行：电脑报经营有限责任公司
经　　销：各地新华书店、报刊亭
CD 生产：苏州新海博数科技有限公司
文本印刷：重庆联谊印务有限公司
开本规格：787×1092mm 1/16　22 印张　400 千字
版　　号：ISBN 978-7-89476-162-0
版　　次：2009 年 6 月第 1 版　2009 年 6 月第 1 次印刷
定　　价：38.00 元(1CD+手册)

前言
PREFACE

关于计算机病毒、网络盗号的新闻，我相信大家通过各种媒体都有所耳闻吧？就在2009年的3月15日晚上，中央电视台的3.15晚会全面曝光了个人信息被窃取等一系列安全事件，比如个人信息被运营商暗中频繁交易并从中获利，黑客通过木马病毒盗号窃取用户的银行资金……

其实作为一个长期关注网络安全的作者，对于“病毒产业链”的勾当也不是现在才知道。但是当这一切真实地展现在自己眼前时，还是觉得那么不可思议、那么触目惊心。于是我开始思考，这些可恶的木马病毒是怎么进入计算机系统，并将用户的系统变为传说中的“肉鸡”，从而在系统里面为所欲为的呢？我突然有了一种想法，就是把自己所了解的，关于黑客从入侵系统到盗号的整个过程，完完整整地展现在各位读者面前，并让整个“病毒产业链”大白于天下。

正巧此时电脑报也在策划一部防范木马入侵的网络安全读物，于是双方很快一拍即合，也就促成了这部《木马攻防全攻略》的最终面市。由于前期规划比较充分，因此在收集内容、撰写稿件的时候比较轻松，甚至可以说是一气呵成。首先我以木马程序为切入点，讲解了各种常用木马的使用、测试、免杀、传播，可以说较为全面地展现了“病毒产业链”的每一个环节。同时还在撰写稿件的时候，全面透切地分析和解读了目前网络中最新的安全事件，让普通读者能够快速了解黑客的最新手法。

如果要说稿件的撰写有没有遇到什么困难，我认为最大的问题就是其中涉及到大量的关于网络安全方面的术语以及PE文件的核心内容。对于第一次接触到汇编语言的读者，在遇到晦涩难懂的代码时可能更会感到痛苦不堪，于是我尽量使用浅显易懂的语言，再加上大量的小知识和小提示，目的让入门读者能够轻松明白文中的意思。希望大家阅读之后，能够更好地保护自己在网络中的利益，不要让那些不愉快的被盗事件再次发生在自己的身边。

《木马攻防全攻略》的最终出版让我感慨万千，虽然我已经撰写网络安全稿件很多年，但是结集成册出版还是第一次。能够把自己多年掌握的网络安全常识与应对技巧和广大的计算机

爱好者共同分享，一种自豪感也从心底油然而生。这既是对自己多年网络经验的一个总结，也是对未来能够为读者提供更多帮助的一种鞭策。

最后，本手册及光盘的制作，得到金山互联网安全公司工程师李铁军、梁佳俊(XO)等人的大力支持，在此特别致以感谢。

万立夫

2009 年 5 月

目录 CONTENTS

Chapter1 快速走进木马的世界

1.1 木马的前世和今生 …… 2

1.2 病毒与木马 …… 3

1.2.1 病毒的特点 …… 3

1.2.2 木马与后门 …… 4

1.3 木马与远程控制 …… 6

1.3.1 什么是远程控制 …… 7

1.3.2 远程控制的实现 …… 9

1.3.3 木马的特殊性 …… 10

1.4 木马的入侵途径 …… 11

Chapter2 C/S 型木马程序

2.1 木马王者——冰河 …… 14

2.1.1 “冰河”的介绍 …… 14

2.1.2 “冰河”的操作 …… 16

2.2 不死鸟——灰鸽子 …… 18

2.2.1 了解“反弹连接”木马 …… 18

2.2.2 配置“灰鸽子”服务端 …… 19

2.2.3 配置“灰鸽子”客户端 …… 24

2.2.4 远程控制服务端 …… 25

2.2.5 线程插入技术 …… 33

2.3 突破主动防御——红狼远控 … 35

2.3.1 配置“红狼”服务端 …… 35

2.3.2 “红狼”服务端操作 …… 36

2.3.3 “红狼”木马的相关技术 …… 41

Chapter3 B/S 型木马程序

3.1 浏览器木马——网络精灵 …… 46

3.1.1 网络精灵的由来 …… 46

3.1.2 网络精灵传统控制 …… 47

3.1.3 浏览器远程控制 …… 47

3.2 蔚蓝色的海洋——海阳顶端网 ASP 木马 …… 53

3.2.1 海阳顶端网 ASP 木马运行环境 … 53

3.2.2 海阳顶端网 ASP 木马的功能 ··· 54
3.2.3 配置海阳顶端网 ASP 木马 ····· 66
3.3 多项全能远程控制——rmtsvc ··· 67
3.3.1 rmtsvc 命令行参数 ····· 67
3.3.2 rmtsvc 的配置文件 ····· 68
3.3.3 rmtsvc 的实际操作 ····· 70

Chapter4 特殊类型木马揭秘
4.1 木马病毒传送带——木马下载者 ····· 82
4.1.1 木马下载者的作用 ····· 82
4.1.2 木马下载者操作演示 ····· 82
4.1.3 木马下载者特殊技术 ····· 84
4.2 脚本木马下载者——一句话木马 ····· 86
4.2.1 什么是“一句话木马” ····· 86
4.2.2 配置“一句话木马” ····· 87
4.2.3 另类“一句话木马” ····· 89
4.3 在内网中飞翔——端口映射 ··· 94
4.3.1 什么是端口映射 ····· 95
4.3.2 端口映射如何实现 ····· 96
4.4 在网络中隐身——网络跳板 ··· 98
4.4.1 什么是跳板 ····· 98
4.4.2 跳板的制作 ····· 100
4.5 由黑变白的“黑洞”远程控制 ··· 104
4.5.1 配置“黑洞”客户端 ····· 104
4.5.2 配置“黑洞”服务端 ····· 106
4.5.3 控制“黑洞”服务端 ····· 108

Chapter5 搭建木马测试环境
5.1 优化配置杀毒软件 ····· 114
5.1.1 优化设置 ····· 114
5.1.2 隔离还原 ····· 116
5.1.3 系统防护 ····· 117
5.1.4 放行木马 ····· 119
5.2 虚拟机的安装配置 ····· 120
5.2.1 什么是虚拟机 ····· 120
5.2.2 虚拟机的种类 ····· 120
5.2.3 虚拟机的配置 ····· 121
5.3 安装配置影子系统 ····· 131
5.3.1 影子系统的介绍 ····· 131
5.3.2 影子系统的操作 ····· 131
5.4 安装配置沙盘安全环境 ····· 137
5.4.1 Sandboxie 的保护方式 ····· 137
5.4.2 Sandboxie 的使用方法 ····· 137
5.4.3 Sandboxie 的其他设置 ····· 141
5.5 搭建脚本运行环境 ····· 142
5.5.1 搭建 ASP 脚本运行环境 ····· 142
5.5.2 快速搭建 ASP 运行环境 ····· 147
5.5.3 搭建 PHP 脚本运行环境 ····· 149

Chapter6 木马防杀技术

6.1 杀毒软件的基础知识 …… 152
6.1.1 杀毒软件原理基础 …… 152
6.1.2 基于文件扫描的技术 …… 153
6.1.3 认识 PE 文件结构 …… 156
6.1.4 认识汇编语言 …… 159
6.2 加壳及多重加壳操作 …… 162
6.2.1 什么是“壳” …… 162
6.2.2 单一壳的操作 …… 162
6.2.3 壳的变异操作 …… 167
6.2.4 多重加壳演示 …… 176
6.2.5 壳中改籽技巧 …… 177
6.3 花指令的添加和修改 …… 182
6.3.1 什么是花指令 …… 182
6.3.2 利用工具加花 …… 182
6.3.3 修改旧花指令 …… 183
6.3.4 编写新花指令 …… 188
6.3.5 添加新花指令 …… 191
6.4 分析查找木马特征码 …… 194
6.4.1 何谓“特征码” …… 194
6.4.2 分析文件特征码 …… 195
6.4.3 修改文件特征码 …… 198
6.4.4 关键字分析修改 …… 201
6.4.5 分析内存特征码 …… 202
6.4.6 其他分析方式 …… 203
6.5 PE 文件头的分析修改 …… 204
6.5.1 PE 文件头的介绍 …… 205
6.5.2 PE 文件头的修改 …… 205
6.6 输入表内容分析修改 …… 217
6.6.1 什么是输入表 …… 217
6.6.2 重建输入表 …… 218
6.6.3 转移函数名称 …… 221

Chapter7 另类木马防杀技术

7.1 附加数据惹的祸 …… 224
7.1.1 附加数据留下线索 …… 224
7.1.2 “PCshare”的修改 …… 224
7.1.3 “灰鸽子”的修改 …… 228
7.2 修改木马关键字符串 …… 231
7.2.1 “移花接木”调换字符串 …… 231
7.2.2 “借尸还魂”替代字符串 …… 233
7.3 木马突破主动防御的手段 …… 235
7.3.1 什么是主动防御 …… 235
7.3.2 突破卡巴斯基主动防御 …… 237
7.3.3 其他杀毒软件主动防御 …… 240
7.3.4 木马程序自定义设置 …… 242
7.3.5 简单设置突破主动防御 …… 243
7.3.6 捆绑程序巧过主动防御 …… 245
7.4 脚本木马免杀方法 …… 246
7.4.1 脚本木马工具免杀法 …… 246
7.4.2 脚本木马手工免杀法 …… 248
7.4.3 其他脚本木马免杀法 …… 255

7.5 网页木马免杀方法 …… 261
7.5.1 网页木马工具免杀法 …… 262
7.5.2 网页木马手工免杀法 …… 264
7.5.3 网页木马免杀延伸 …… 269
7.6 雷客图可以这样躲过 …… 270
7.6.1 修改代码绕过雷客图 …… 270
7.6.2 修改时间继续伪装 …… 273
7.7 反调试躲过杀毒软件 …… 277
7.7.1 SEH 相关知识 …… 277
7.7.2 SEH 操作原理 …… 277
7.7.3 SEH 操作过程 …… 278
7.7.4 SEH 加花操作 …… 278
7.8 SYS 文件的免杀技巧 …… 282
7.8.1 提取 SYS 文件 …… 283
7.8.2 修改特征码 …… 283
7.8.3 调整特征码 …… 285
7.8.4 文件头修改 …… 287
7.8.5 加壳处理操作 …… 288

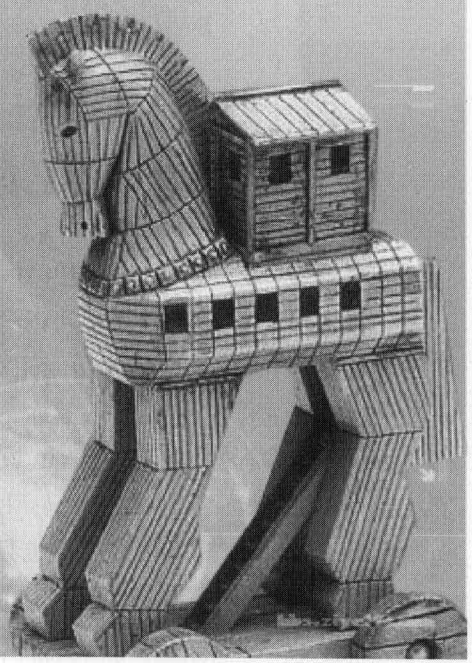
Chapter8 木马伪装的多种方式

8.1 文件捆绑 …… 290
8.1.1 常规捆绑 …… 290
8.1.2 压缩捆绑 …… 291
8.1.3 插入捆绑 …… 300
8.1.4 克隆捆绑 …… 302
8.2 属性伪装 …… 304
8.2.1 属性伪装 …… 304
8.2.2 伪装签名 …… 306
8.2.3 定义签名 …… 307
8.3 图标伪装 …… 311
8.3.1 生成图标 …… 311
8.3.2 替换图标 …… 311
8.4 网页木马 …… 312
8.4.1 制作网页木马 …… 312
8.4.2 网页木马的传播方式 …… 313
8.4.3 网站系统漏洞挂马法 …… 315
8.4.4 IIS 写权限挂马法 …… 320
8.4.5 电子邮件挂马法 …… 322
8.5 端口入侵 …… 324
8.5.1 什么是端口 …… 324
8.5.2 系统服务型 …… 325
8.5.3 网路服务型 …… 331
8.5.4 入侵辅助型 …… 332
8.6 视频伪装 …… 332
8.6.1 RM 文件的伪装利用 …… 332
8.6.2 WMV 文件的伪装利用 …… 333
8.7 漏洞入侵 …… 336
8.7.1 什么是数据溢出 …… 336
8.7.2 专业工具入侵 …… 337
8.7.3 手工批量入侵 …… 339
8.7.4 工具批量入侵 …… 343

Chapter 1

快速走进木马的世界

●距今 3000 多年，发生了一场著名的“特洛伊”战争，希腊士兵使用木马最终获得了胜利。在跨越了几十个世纪以后，木马被一群称为“黑客”的人再次唤醒，并成为他们在网络世界中“攻城拔寨”的一款利器。



1.1 木马的前世和今生

特洛伊木马(以下简称木马),英文叫做“Trojan horse”,其名称取自希腊神话的特洛伊木马记。古希腊传说,特洛伊王子帕里斯在访问希腊时诱走了王后海伦,希腊人因此远征特洛伊。围攻 9 年后到第 10 年,希腊将领奥德修斯献了一计,就是把一批勇士埋伏在一匹巨大的木马腹内,放在城外后佯作退兵。特洛伊人以为敌兵已退,就把木马作为战利品搬入城中。到了夜间,埋伏在木马中的勇士跳出来打开了城门,希腊将士一拥而入攻下了城池。后来,人们就常用“特洛伊木马”这一典故,用来比喻在敌方营垒里埋下伏兵里应外合的活动。

特洛伊木马没有复制能力,它的特点是伪装成一个实用工具或一个可爱的游戏,这会诱使用户将其安装在计算机系统或者服务器上。“中了木马”就是指安装了木马的服务器程序,例如某电脑被安装了木马服务器程序,那么拥有控制器程序的人就可以完全控制住这台电脑,不论是文件、程序,还是账号、密码都毫无安全可言。

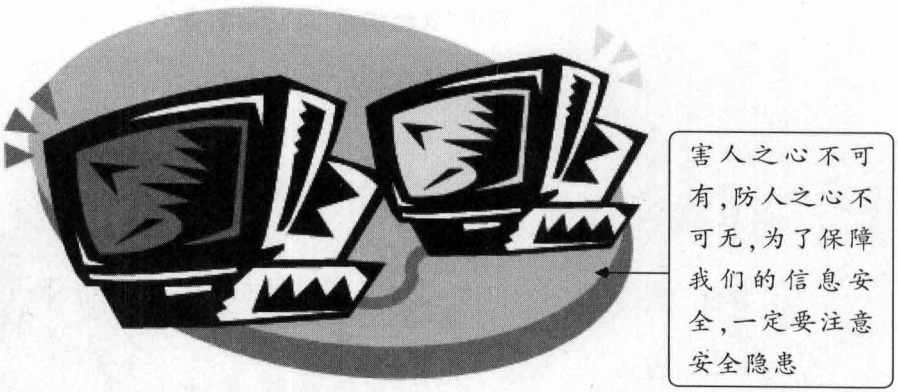
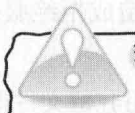
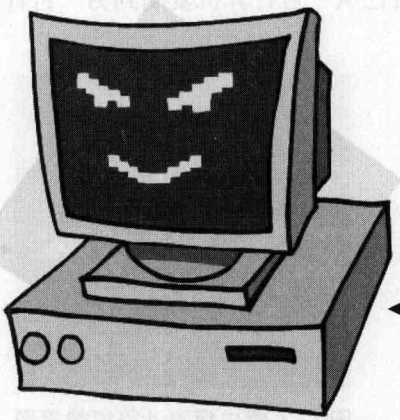


图 1-1 木马能悄悄地入侵他人电脑

从木马的发展来看,基本上可以分为两个阶段。当网络还处于以 UNIX 平台为主的时代木马就产生了,当时的木马程序功能相对简单,往往是将一段程序嵌入到系统文件中,用跳转指令来执行一些远程控制功能,在这个时期木马的设计者和使用者大都是些技术人员,必须具备相当的网络和编程知识。随着 Windows 平台的日益普及,一些基于图形操作的木马程序出现了,用户界面的改善“普及”了木马,让那些不太懂专业知识人都可以熟练地操作木马,因此木马就泛滥了,使用木马入侵的事件也频繁出现。



注 意 现在，木马的功能已经非常完善，破坏力也相当惊人，被木马控制的电脑将毫无秘密可言，人们的隐私信息岌岌可危，我们应该正视网络世界面临的威胁，并采取行动捍卫信息安全。



一点计算机被木马侵蚀，就很难彻底清除，因为缺乏木马知识的用户并不知道木马会潜伏在那个角落

图 1-2 木马已经成为计算机系统中潜伏的幽灵

1.2 病毒与木马

使用计算机的用户都会遇到病毒和木马，我们首先从源头了解一下病毒和木马。

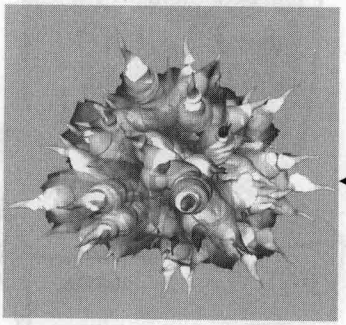
1.2.1 病毒的特点

按照计算机管理条例法对病毒定义有两个最明显的特点，它具有自我传播性，就是我们所说的感染；还有一个是破坏性。一般病毒会带来一定的危害，这两个特性是病毒最重要的特性。目前病毒主要是伴随着网络的发展，需要进行快速的传播。比如说 2003 年的冲击波，是利用的系统漏洞，传播速度非常之快，一天之内感染了全球大部分有漏洞的电脑。病毒主要的发展趋势就是传播，要达到最大泛围的传播。目前在国内外比较流行的一些病毒主要是利用即时通信软件或恶意邮件进行传播。

随着病毒的发展，一种叫做蠕虫(Worm)的病毒逐渐引起人们的注意。一般认为，蠕虫是一种通过网络传播的恶性病毒，它具有传播性、隐蔽性、破坏性等病毒的一些共性，同时具有自

己的一些特征，比如不利用文件寄生(有的只存在于内存中)，对网络造成拒绝服务，以及和黑客技术相结合等等。

普通病毒需要传播受感染的驻留文件来进行复制，而蠕虫不使用驻留文件即可在系统之间进行自我复制，普通病毒的传染能力主要是针对计算机内的文件系统而言，而蠕虫病毒的传染目标是互联网内的所有计算机。它能控制计算机上可以传输文件或信息的功能，一旦系统感染蠕虫即可自行传播，该病毒会将自己从一台计算机复制到另一台计算机，更危险的是它还可大量复制。



尽管计算机病毒是虚拟存在的，但是从此图中我们仍然能感受得出病毒的可怕

图 1-3 蠕虫病毒计算机效果图

在产生的破坏性上，蠕虫病毒也不是普通病毒所能比拟的，网络的发展使得蠕虫可以在短时间内蔓延整个网络，造成网络瘫痪。局域网条件下的共享文件夹、电子邮件、网络中的恶意网页、大量存在着漏洞的服务器等，都成为蠕虫传播的良好途径，蠕虫病毒可以在几个小时内蔓延全球，而且蠕虫的主动攻击性和突然爆发性将使得人们手足无措。此外，蠕虫会消耗内存或网络带宽，从而可能导致计算机崩溃。而且它的传播不必通过“宿主”程序或文件，因此可潜入你的系统并允许其他人远程控制你的计算机，这也使它的危害远较普通病毒为大。

1.2.2 木马与后门

木马跟病毒最本质的区别是病毒以感染为目的，木马更注重于目的性。在技术层面来讲，病毒大部分是要用底层语言编写，而木马则更容易用高级语言编写实现。木马的传播性最弱的，跟病毒恰恰相反。病毒主要的特性是感染很疯狂，而木马为了达到一定的目的性，选择定点传播这样的途径。早期木马最主要的是控制电脑。现在的木马最主要的是转变成偷窃，更关注用户的私密信息。

木马能盗取用户隐秘信息，其根本就是打开了计算机系统的后门，实际上，很多软件自己本身就带有后门。在软件的开发阶段，程序员常会在软件内创建后门，以便修改程序中的缺陷。

如果这些后门被其他人知道，或是在发布软件之前没有删除后门，那么它马上就成了安全风险的来源。后门又称为 BackDoor。

小知识

一台计算机系统上有 65535 个端口。那么如果把计算机看作是一间屋子，那么这 65535 个端口就可以把它看作是计算机为了与外界连接所开的 65535 扇门。

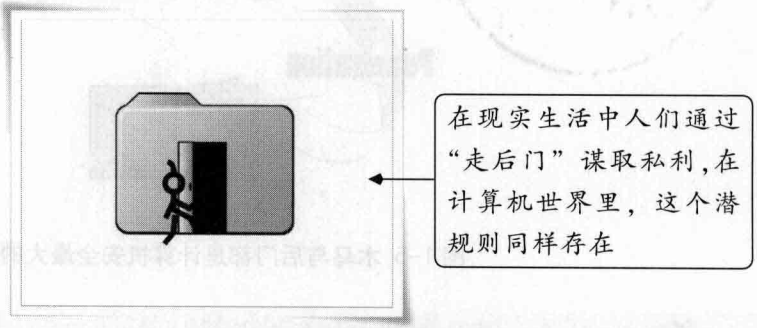


图 1-4 后门程序无处不在

为什么需要那么多扇门呢？因为主人的事务很繁忙，它为了同时处理很多应酬，就决定让每扇门对应一项应酬。所以有的门是主人特地打开迎接客人的（提供服务），有的门是主人为了出去访问客人而开设的（访问远程服务）。理论上，剩下的其他门都该是关闭着的，但偏偏因为各种原因，有的门在主人都不知道的情形下，却被悄然开启。于是就有好事者进入，主人的隐私被刺探，生活被打扰，甚至屋里的东西也被搞得一片狼藉。这扇悄然被开启的门，就是今天我们要讲的“后门”，当然这只是一个比喻。

后门程序一般是指那些绕过安全性控制，而获取对程序或系统访问权的程序方法。照着这种标准来衡量的话，Windows Update 也被人们归纳为后门之一了，2008 年的 Windows XP 黑屏事件就是一个例子。虽然微软“信誓旦旦”地说他们不会搜集个人电脑中的信息，但从 Windows Update 的行为进行分析的话，就会发现它必须搜集个人电脑的信息才能进行操作，所不同的只是搜集信息而已。

后门程序跟我们通常所说的“木马程序”有联系也有区别。联系在于都是隐藏在用户系统中向外发送信息，而且本身具有一定权限以便远程机器对本机的控制。区别在于木马程序是一个完整的软件，而后门程序则体积较小且功能都很单一。而且在病毒命名中，后门一般带有

backdoor 字样，而木马一般则是 trojan 字样。由于它们之间的差别越来越小，所以现在“后门”基本已经被“木马”所取代。

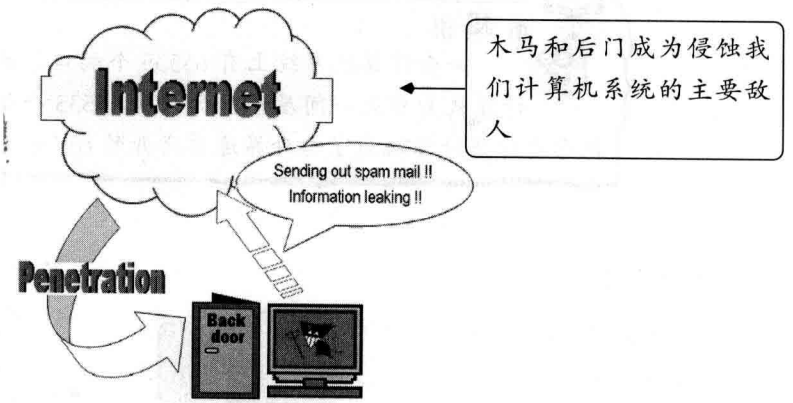


图 1-5 木马与后门都是计算机安全最大的隐患

1.3 木马与远程控制

要详细了解木马程序，首先要知道远程控制软件。远程控制是基于网络才能实现的计算机操作。远程控制技术，始于 DOS 时代，只不过当时由于技术上没有什么大的变化，网络不发达，市场没有更高的要求，所以远程控制技术没有引起更多人的注意。但是，随着网络的高度发展，管理及技术支持的需要，远程操作及控制技术越来越引起人们的关注，远程控制也得到广泛的应用。

注意 需要说明一下，这里所说的“远程”并非等同于远距离，因为被你控制的电脑可以在千里之外的大洋彼岸，也可以是你身旁局域网中的一台电脑。

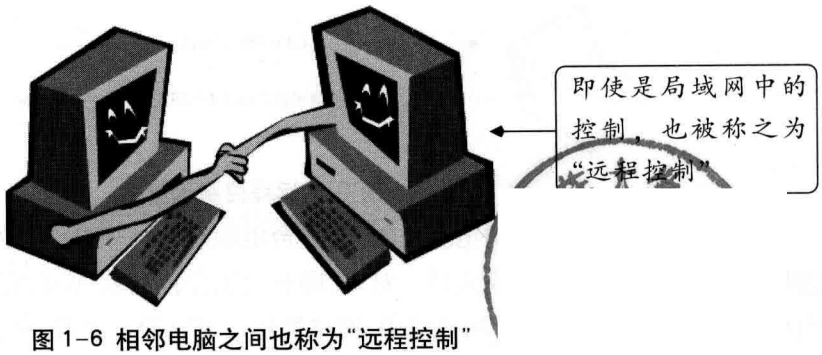


图 1-6 相邻电脑之间也称为“远程控制”

1.3.1 什么是远程控制

远程控制操作是通过远程控制软件来完成的。远程控制软件一般由两部分组成，用于发送指令的发出端被称为主控端或客户端（Client），被客户端控制的计算机称为被控端或服务端(Server)。在进行远程控制操作以前，需要把服务端程序安装到被控制的电脑中，而在本地电脑里也需要安装相应的客户端程序。

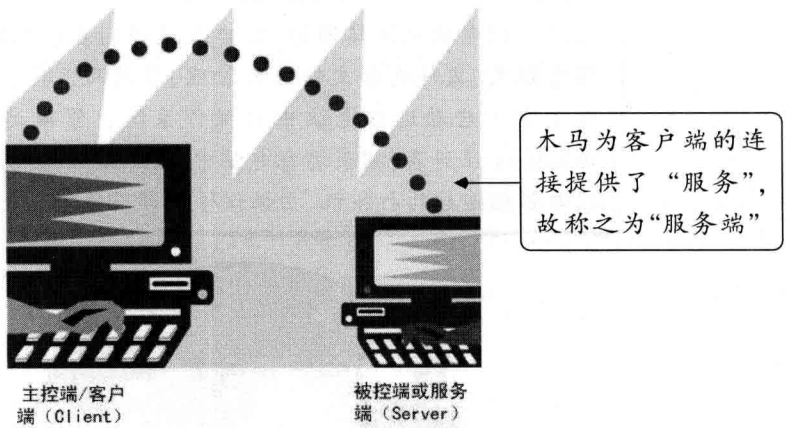


图 1-7 客户端与服务端

如果要进行远程控制，首先由服务端程序在远程电脑中打开一个特定的端口，然后客户端程序向远程电脑中的服务端发出信号，这时服务端就会打开一个端口建立起远程服务，这样，客户端程序就可以远程控制服务端了。

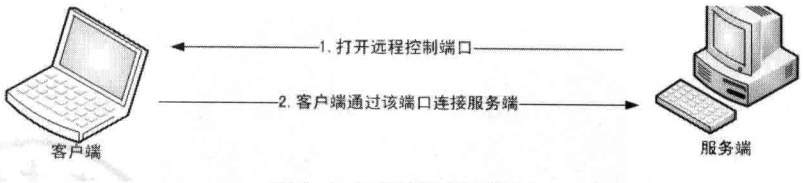


图 1-8 远程控制示意图

这里所说的是一对一的电脑控制，即一台电脑对另外一台电脑的远程控制。其实，基于远程服务的远程控制最多的模式是一对多，即利用远程控制软件，我们可以使用一台电脑控制多台电脑。这种模式多数用于局域网中，网络管理员可以通过远程控制轻松地管理局域网中的每一台电脑。

有了一对多这种模式，当然就有多对一的模式，即利用远程控制软件让多用户同时管理一台远程电脑。这种多对一的控制模式多数时候用于各种教学演示。

小知识

远程控制可以实现本地操作的所有功能，包括获取远程电脑的屏幕图像、窗口及进程列表；对远程电脑的任意磁盘、文件夹和文件进行管理、访问及上传、下载；关闭或者重新启动远端电脑中的操作系统；修改远程电脑的 Windows 注册表；捕获远程电脑中音频、视频信号；操纵和远程电脑相连接的打印机、扫描仪等外部设备等。

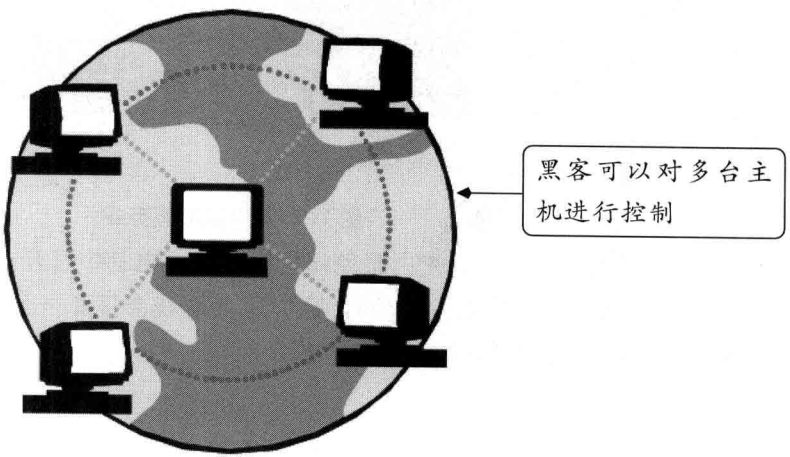


图 1-9 一个客户端可以控制多个服务端