



Network Security Technology

网络安全技术

第九章 木马攻击与防御技术

主讲：李强

E-mail: dr_qiangli@163.com

Office: 明实楼（3号楼）A410

本章内容安排

- **9.1** 木马概述
- **9.2** 木马的实现原理与攻击步骤
- **9.3** 木马实例介绍
- **9.4** 木马的防御技术
- **9.5** 木马的发展趋势
- **9.6** 小结



9.1 木马概述

- 9.1.1 木马基本概念
- 9.1.2 木马的分类
- 9.1.3 木马的特点

What's Inside A

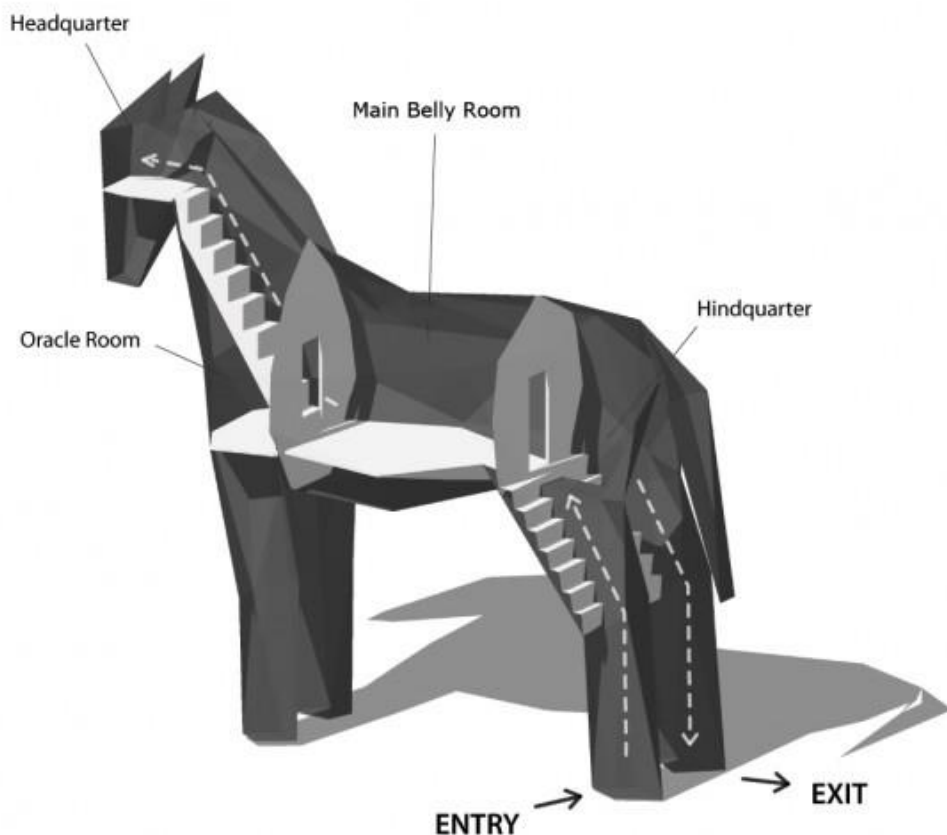


TROJAN HORSE ?



9.1.1 木马基本概念

- 木马的来由
- 木马的定义
- 木马的危害



(1).木马的来由

- ❑ 木马是“特洛伊木马”（**trojan horse**）的简称，据说这个名称来源于希腊神话《木马屠城记》。
- ❑ 如今黑客程序借用其名，有“一经潜入，后患无穷”之意。



特洛伊木马的故事

- 相传在古希腊时期，特洛伊王子帕里斯劫走了斯巴达美丽的王后海伦和大量的财物。斯巴达国王组织了强大的希腊联军远征特洛伊，但久攻不下。
- 有人献计制造一只高二丈的大木马，假装作战马神，让士兵藏匿于巨大的木马中，同时命令大部队佯装撤退而将木马弃于特洛伊城下。
- 城中得知解围的消息后，遂将“木马”作为奇异的战利品拖入城内，全城饮酒狂欢。
- 到午夜时分，全城军民尽入梦乡，匿于木马中的将士出来开启城门及四处纵火，城外伏兵涌入，部队里应外合，彻底攻破了特洛伊城。
- 后世称这只大木马为“特洛伊木马”。







Menelaus.

Paris.

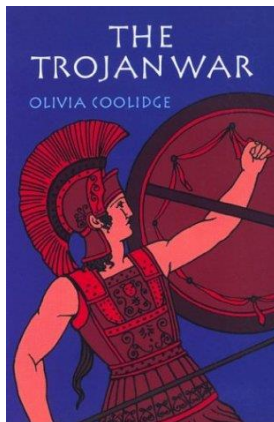
Diomedes.

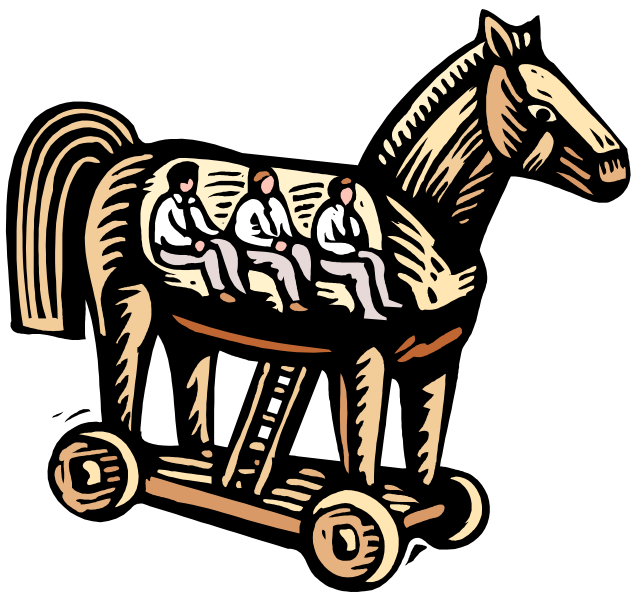
Odysseus.

Nestor.

Achilles.

Agamemnon.





The noble
Achilles



The arrogant
Agamemnon



The traitorous
Paris



The wily
Odysseus

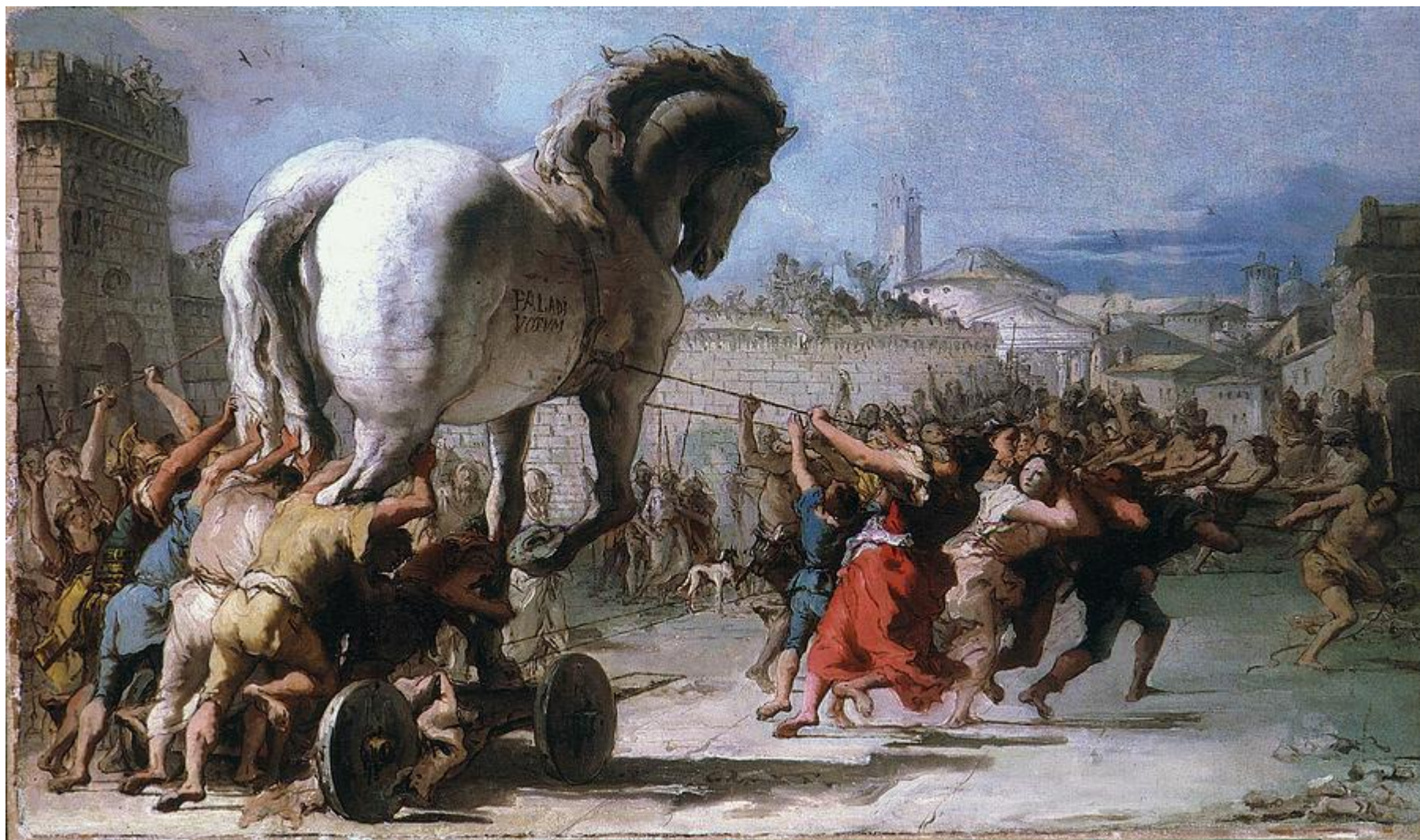


The beautiful
Helen



The royal
Priam

and the famous Wooden Horse!



(2).木马的定义

- 在计算机系统中，“特洛伊木马”指系统中被植入的、人为设计的程序，目的包括通过网络远程控制其他用户的计算机系统，窃取信息资料，并可恶意致使计算机系统瘫痪。



RFC1244对特洛伊木马的定义

□ **RFC1244 (Request for Comments : 1244)** 中是这样描述木马的:“木马程序是一种程序, 它能提供一些有用的, 或是仅仅令人感兴趣的功能。但是它还有用户所不知道的其他功能, 例如在你不了解的情况下拷贝文件或窃取你的密码。”

RFC1244对特洛伊木马的定义(2)

- **RFC1244**的定义虽然不十分完善，但是可以澄清一些模糊概念：
 - 首先木马程序并不一定实现某种对用户来说有意义或有帮助的功能，但却会实现一些隐藏的、危险的功能；
 - 其次木马所实现的主要功能并不为受害者所知，只有程序编制者最清楚。
 - 第三，这个定义暗示“有效负载”是恶意的。

大多数安全专家对特洛伊木马的定义

□ 目前，大多数安全专家统一认可的定义是：“特洛伊木马是一段能实现有用的或必需的功能的程序，但是同时还完成一些不为人知的功能。”

Wikipedia -- A Trojan horse, or Trojan, in computing is **a generally non-self-replicating type of malware program containing malicious code** that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm.



Beast control program.

Beast is a Windows-based backdoor Trojan horse invisible in an infected computer and this program gives full control of that computer.

(3).木马的危害

- 根据传统的数据安全模型的分类，木马程序的企图可以对应分为三种：
 - 试图访问未授权资源；
 - 试图阻止访问；
 - 试图更改或破坏数据和系统。



(3).木马的危害

- 目前木马常被用作网络系统入侵的重要工具和手段。
- 木马利用自身所具有的植入功能，或依附其它具有传播能力的程序等多种途径，进驻目标机器，搜集其中各种敏感信息，并通过网络与外界通信，发回所搜集到的各种敏感信息，接受植入者指令，完成其它各种操作，如修改指定文件、格式化硬盘等。

(3).木马的危害

- ❑ 感染了木马的计算机将面临数据丢失和机密泄露的危险。
- ❑ 木马往往又被用做后门，植入被攻破的系统，以便为入侵者再次访问系统提供方便；或者利用被入侵的系统，通过欺骗合法用户的某种方式暗中散发木马，以便进一步扩大入侵成果和入侵范围，为进行其它入侵活动，如分布式拒绝服务攻击（**DDoS**）等提供可能。

(3).木马的危害

- ❑ 大型网络服务器也面临木马的威胁，入侵者可通过对其所植入的木马而偷窃到系统管理员的口令。
- ❑ 而当一个系统服务器安全性较高时，入侵者往往会通过首先攻破庞大系统用户群中安全性相对较弱的普通电脑用户，然后借助所植入木马获得有效信息（如系统管理员口令），并最终达到入侵系统目标服务器的目的。

(3).木马的危害

- 木马程序具有很大的危害性，主要表现在：
 - 自动搜索已中木马的计算机；
 - 管理对方资源，如复制文件、删除文件、查看文件内容、上传文件、下载文件等；
 - 跟踪监视对方屏幕；
 - 直接控制对方的键盘、鼠标；
 - 随意修改注册表和系统文件；
 - 共享被控计算机的硬盘资源；
 - 监视对方任务且可终止对方任务；
 - 远程重启和关闭机器。

9.1.2 木马的分类

□ 从**木马技术发展的历程**考虑，木马技术自出现至今，大致可以分为四代：

- 第一代木马是伪装型病毒，将病毒伪装成一个合法的程序让用户运行，例如1986年的PC-Write木马；
- 第二代木马在隐藏、自启动和操纵服务器等技术上有了很大的发展，可以进行密码窃取、远程控制，例如BO2000和冰河木马；
- 第三代木马在连接方式上有了改进，利用端口反弹技术，例如灰鸽子木马；
- 第四代木马在进程隐藏方面做了较大的改动，让木马服务器运行时没有进程，网络操作插入到系统进程或者应用进程中完成，例如广外男生木马。

9.1.2 木马的分类

□ 从木马所实现的功能角度可分为:

- (1).破坏型
- (2).密码发送型
- (3).远程访问型
- (4).键盘记录木马
- (5).DoS攻击木马
- (6).代理木马
- (7).FTP木马
- (8).程序杀手木马
- (9).反弹端口型木马

(1).破坏型

- 惟一的功能就是破坏并且删除文件，如电脑上的**DLL**、**INI**、**EXE**文件或其它类型文件，造成系统损坏，用户数据被破坏。
- 功能简单，容易实现，破坏性强。



(2).密码发送型

- ❑ 找到隐藏密码并把它们发送到指定的信箱。
- ❑ 有人喜欢把自己的各种密码以文件的形式存放在计算机中，认为这样方便；还有人喜欢用 **WINDOWS** 提供的密码记忆功能，这样就可以不必每次都输入密码了。
- ❑ 许多木马可以寻找到这些敏感信息，把它们送到黑客手中。



TROJANS

(3).远程访问型

- 使用这类木马，只需有人运行了服务端程序，如果客户知道了服务端的**IP**地址，就可以实现远程控制。
- 这类程序可以实现观察"受害者"正在干什么，当然这个程序完全可以用在正道上的，比如监视学生机的操作。



TROJAN

(4). 键盘记录木马

- ❑ 记录受害者的键盘敲击并且在日志文件里查找可能的密码。
- ❑ 这种木马随着**Windows**的启动而启动。它们有在线和离线记录这样的选项，顾名思义，它们分别记录你在线和离线状态下敲击键盘时的按键情况。
- ❑ 也就是说你按过什么按键，种植木马的人都知道，从这些按键中他很容易就会得到你的密码等有用信息！
- ❑ 当然，对于这种类型的木马，邮件发送功能也是必不可少的。

(5).DoS攻击木马

- 随着**DoS**攻击越来越广泛的应用，被用作**DoS**攻击的木马也越来越流行起来。当你入侵了一台机器，给他种上**DoS**攻击木马，那么日后这台计算机就成为你**DoS**攻击的最得力助手了。
- 这种木马的危害不是体现在被感染计算机上，而是体现在攻击者可以利用它来攻击一台又一台计算机，给网络造成很大的伤害和带来损失。
- 还有一种类似**DoS**的木马叫做邮件炸弹木马，一旦机器被感染，木马就会随机生成各种各样主题的信件，对特定的邮箱不停地发送邮件，一直到对方瘫痪、不能接受邮件时为止。

(6).代理木马

- ❑ 黑客在入侵的同时掩盖自己的足迹，谨防别人发现自己的身份是非常重要的。因此，给被控制的“肉鸡”种上代理木马，让其变成攻击者发动攻击的跳板，就是代理木马最重要的任务。
- ❑ 通过代理木马，攻击者可以在匿名的情况下使用**Telnet**、**ICQ**、**IRC**等程序，从而隐蔽自己的踪迹。

(7).FTP木马

- 这种木马可能是最简单和古老的木马了，它的惟一功能就是打开**21**端口，等待用户连接。
- 现在新**FTP**木马还加上了密码功能，这样，只有攻击者本人才知道正确的密码，从而进入对方计算机。

(8).程序杀手木马

- 上面的木马功能虽然形形色色，不过到了对方机器上要发挥自己的作用，还要过防木马软件这一关才行。常见的防木马软件有 **ZoneAlarm**、**Norton Anti-Virus**等。
- 程序杀手木马的功能就是关闭对方机器上运行的这类程序，让其他的木马更好地发挥作用。

(9).反弹端口型木马

- ❑ 木马开发者在分析了防火墙的特性后发现:防火墙对于连入的链接往往会进行非常严格的过滤,但是对于连出的链接却疏于防范。
- ❑ 于是,与一般的普通木马相反,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**。



反弹端口型木马(2)

- ❑ 反弹窗口木马定时监测控制端的存在，发现控制端上线，立即弹出端口主动连结控制端打开的被动端口；为了隐蔽起见，控制端的被动端口一般开在**80**，即使用户使用扫描软件检查自己的端口，发现类似

TCP UserIP:1026 ControllerIP:80 ESTABLISHED

的情况，稍微疏忽一点，你就会以为是自己在浏览网页。

9.1.3 木马的特点

- 一个典型的特洛伊木马（程序）通常具有以下四个特点：
 - 有效性
 - 隐蔽性
 - 顽固性
 - 易植入性
- 一个木马的危害大小和清除难易程度可以从这四个方面来加以评估。

有效性

- 由于木马常常构成网络入侵方法中的一个重要内容，它运行在目标机器上就必须能够实现入侵者的某些企图。
- 因此有效性就是指入侵的木马能够与其控制端（入侵者）建立某种有效联系，从而能够充分控制目标机器并窃取其中的敏感信息。
- 因此有效性是木马的一个最重要特点。

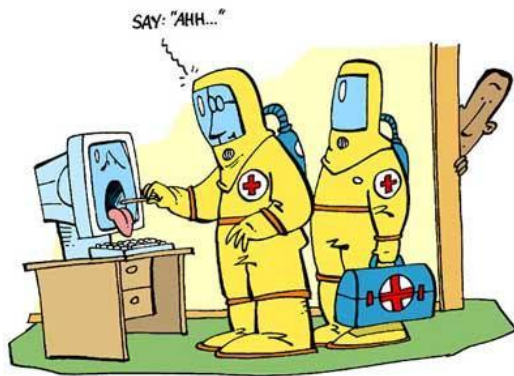


隐蔽性

- ❑ 木马必须有能力长期潜伏于目标机器中而不被发现。
- ❑ 一个隐蔽性差的木马往往会很容易暴露自己，进而被杀毒（或杀马）软件，甚至用户手工检查出来，这样将使得这类木马变得毫无价值。
- ❑ 因此可以说隐蔽性是木马的生命。

顽固性

- 当木马被检查出来（失去隐蔽性）之后，为继续确保其入侵有效性，木马往往还具有另一个重要特性——顽固性。
- 木马顽固性就是指有效清除木马的难易程度。若一个木马在检查出来之后，仍然无法将其一次性有效清除，那么该木马就具有较强的顽固性。



易植入性

- ❑ 任何木马必须首先能够进入目标机器，因此易植入性就成为木马有效性的先决条件。
- ❑ 欺骗是自木马诞生起最常见的植入手段，因此各种好用的小功能软件就成为木马常用的栖息地。
- ❑ 利用系统漏洞进行木马植入也是木马入侵的一类重要途径。
- ❑ 目前木马技术与蠕虫技术的结合使得木马具有类似蠕虫的传播性，这也就极大提高了木马的易植入性。

9.1.3 木马的特点

□ 此外，木马还具有以下辅助型特点：

- 自动运行
- 欺骗性
- 自动恢复
- 功能的特殊性

PANDA
SECURITY

AVG Free
Anti-Virus

KASPERSKY
LAB

TREND
MICRO

bitdefender

F-Secure

NOD32
antivirus system

A-SQUARED

avast!
be free

AntiVir

自动运行

- 通常木马程序通过修改系统的配置文件或注册表文件，在目标系统启动时就自动加载运行。
- 这种自动加载运行不需要客户端干预，同时也不会被目标系统用户所觉察。

欺骗性

- ❑ 木马程序要达到其长期隐蔽的目的，就必需采取各种各样的欺骗手段，欺骗目标系统用户，以防被发现。
- ❑ 比如木马程序经常会采用一种文件名的欺骗手段，如**exploer**这样的文件名，以此来与系统中的合法程序**explorer**相混淆。
- ❑ 木马的编制者还在不断制造新的欺骗的手段，花样层出不穷，让人防不胜防。

自动恢复

- 现在很多木马程序中的功能模块已不再是由单一的文件组成，而是具有多重备份，可以相互恢复。
- 计算机一旦感染上这种木马程序，想单独靠删除某个文件来清除是不太可能的。

功能的特殊性

- 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，有些木马具有搜索并发送目标主机中的口令、记录用户事件、进行键盘记录、远程注册表操作以及锁定鼠标等功能。

9.1.3 木马的特点

- 近年来，木马技术取得了较大的发展，目前已彻底摆脱了传统模式下植入方法原始、通信方式单一、隐蔽性差等不足。
- 借助一些新技术，木马不再依赖于对用户进行简单的欺骗，也可以不必修改系统注册表，不开新端口，不在磁盘上保留新文件，甚至可以没有独立的进程，这些新特点使对木马的查杀变得愈加困难；但与此同时却使得木马的功能得到了大幅提升。
- 采用了新技术的木马可以轻易穿过防火墙与外界（入侵者）通信。

9.2 木马的实现原理与攻击步骤

木马是怎么炼成的

木马都使用哪些关键技术



9.2 木马的实现原理与攻击步骤

- ❑ 9.2.1 木马实现原理
- ❑ 9.2.2 植入技术
- ❑ 9.2.3 自动加载技术
- ❑ 9.2.4 隐藏技术
- ❑ 9.2.5 连接技术
- ❑ 9.2.6 监控技术



9.2.1 木马实现原理

- 本质上说，木马大多都是网络客户 / 服务（**Client/Server**）程序的组合。
- 常由一个攻击者控制的客户端程序和一个运行在被控计算机端的服务端程序组成。

9.2.1 木马实现原理

- 当攻击者要利用“木马”进行网络入侵，一般都需完成如下环节：
 - 向目标主机植入木马
 - 启动和隐藏木马
 - 服务器端（目标主机）和客户端建立连接
 - 进行远程控制

9.2.2 植入技术

- 木马植入技术可以大概分为**主动植入**与**被动植入**两类。
- 所谓**主动植入**，就是攻击者主动将木马程序种到本地或者是远程主机上，这个行为过程完全由攻击者主动掌握。
- 而**被动植入**，是指攻击者预先设置某种环境，然后被动等待目标系统用户的某种可能的操作，只有这种操作执行，木马程序才有可能植入目标系统。

主动植入

- 主动植入，一般需要通过某种方法获取目标主机的一定权限，然后由攻击者自己动手进行安装。
- 按照目标系统是本地还是远程的区分，这种方法又有**本地安装与远程安装**之分。

主动植入

- 由于在一个系统植入木马，不仅需要将木马程序上传到目标系统，还需要在目标系统运行木马程序；所以主动植入不仅需要具有目标系统的写权限，还需要可执行权限。
- 如果仅仅具有写权限，只能将木马程序上传但不能执行，这种情况属于被动植入，因为木马仍然需要被动等待以某种方式被执行。

主动植入--本地安装

□ **本地安装**就是直接在本地主机上进行安装。试想一下，有多少人的计算机能确保除了自己之外不会被任何人使用。而在经常更换使用者的网吧计算机上，这种安装木马的方法更是非常普遍，也非常有效。

主动植入--远程安装

- **远程安装**就是通过常规攻击手段获得目标主机的一定权限后，将木马上传到目标主机上，并使其运行起来。例如，某些系统漏洞的存在，使得攻击者可以利用漏洞远程将木马程序上传并执行。
- 从实现方式上，主要分为：
 - 利用系统自身漏洞植入
 - 利用第三方软件漏洞植入

利用系统自身漏洞植入

- 这是一种主动攻击的方式。攻击者利用所了解的系统的安全漏洞及其特性主动出击。
- 如**IIS**服务器的溢出漏洞，通过一个“**IISHack**”的攻击程序就可使**IIS**服务器崩溃，并同时在被攻击服务器执行“木马”程序。
- **MIME**漏洞则是利用**Internet Explorer**在处理不正常的**MIME**类型存在的问题，攻击者有意地更改**MIME**类型，使**IE**可以不提示用户而直接运行电子邮件附件中的恶意程序等。

利用第三方软件漏洞植入

- 每台主机上都会安装一些第三方软件或者提供服务，但是这些软件可能存在可被利用的漏洞，如果被恶意者利用，你的主机就可以成为木马的“栖息地”。
- 例如：**AT-TFTP Server**在处理带有超长文件名参数的请求时存在漏洞，远程攻击者可能利用此漏洞在服务器上执行任意指令。

被动植入

- 就目前的情况，被动植入技术主要是利用以下方式将木马程序植入目标系统：
 - 网页浏览植入
 - 利用电子邮件植入
 - 利用网络下载植入
 - 利用即时通工具植入
 - 与其它程序捆绑
 - 利用移动存储设备植入

网页浏览植入

- 网页浏览传播：这种方法利用 **Script/ActiveX控件/JavaApplet** 等技术编写出一个 **HTML** 网页，当我们浏览该页面时，会在后台将木马程序下载到计算机缓存中，然后修改系统注册表，使相关键值指向“木马”程序。
- 更可怕的是，黑客还可以利用浏览器的已经或者未知的漏洞，把木马下载到本机并运行。

利用电子邮件植入

- 电子邮件（**E-mail**）进行传播：攻击者将“木马”程序伪装成**E-mail**附件的形式发送出去，收信人只要查看邮件附件就会使“木马”程序得到运行并安装进入系统。

例：利用邮件内嵌的**WSH**脚本

- 通过在邮件内容内嵌**WSH(Windows Scripts Host)**脚本，用户不需要打开附件，仅仅浏览一下邮件的内容，附件中的木马就会被执行。
- 邮件木马已经从附件走到正文中了，有谁会收到邮件后连看都不看就删除呢。

利用网络下载植入

- 一些非正规的网站以提供软件下载为名，将木马程序伪装成用户所希望的其它软件，当用户下载安装时，实际上所安装的是木马程序。
- 通过欺骗用户使木马程序植入到目标主机中。

利用即时通工具植入

- 因为即时通工具有文件传输功能，所以现在也有很多木马通过即时通工具传播。
- 恶意破坏者通常把木马服务器程序通过合并软件和其他的可执行文件绑在一起，然后骗你说是一个好玩的东东或者是漂亮**MM**的照片，你接受后运行的话，你就成了木马的牺牲品了。

与其它程序捆绑

- ❑ 将木马与其它软件捆绑，用户在下载安装其它软件时就不自觉地也安装了木马，这种情况下用户很难察觉。
- ❑ 攻击者还可以在**.doc**、**.ppt**、**.rar**、**.zip**等文件中插入恶意代码，当用户打开这些文档时，就会被植入木马。

例：图片木马

- 有一种**图片木马**，利用用户认为图片文件不可执行，因此不可能是木马这样的心理来欺骗受害者。
- 实际上这是一个后缀名的小把戏。由于**Windows**系统默认不显示已经注册了的文件类型的后缀名，因此**test.jpg.exe**这种文件在系统上就显示为**test.jpg**，木马再采用和图片文件一样的图标，对大多数用户而言，是极具欺骗性的。

利用移动存储设备植入

- 利用移动存储设备传播：利用**Windows**的**Autoplay(autorun.inf)**机制，当插入U盘、移动硬盘或者光盘时，可以自动执行恶意程序。
- 利用**U**盘传播木马或者病毒的方式非常流行，这两年几乎席卷全国。

9.2.3 自动加载技术

- 木马程序在被植入目标主机后，不可能寄希望于用户双击其图标来运行启动，只能不动声色地自动启动和运行，攻击才能以此为依据侵入被侵主机，完成控制。

自动加载技术

- 在**Windows**系统中木马程序的自动加载技术主要有：
 - 修改系统文件
 - 修改系统注册表
 - 添加系统服务
 - 修改文件打开关联属性
 - 修改任务计划
 - 修改组策略
 - 利用系统自动运行的程序
 - 修改启动文件夹
 - 替换系统DLL

(1). 修改系统文件

- 木马程序一般会在第一次运行时，修改目标系统文件以达到自动加载的目的。方法有：
 - 修改autoexec.bat等批处理文件来实现自动启动：常通过修改Autoexec.bat、Winstart.bat、Dosstart.bat等三个批处理文件来实现自动启动。
 - 在系统配置文件实现：通过修改Config.sys文件、Win.ini文件、System.ini文件。
- 这种方法比较古老。

(2). 修改系统注册表

- ❑ 系统注册表保存着系统的软件、硬件及其它与系统配置有关的重要信息。
- ❑ 通过设置一些启动加载项目，也可以使木马程序达到自动加载运行的目的，而且这种方法更加隐蔽。

修改系统注册表(2)

- ❑ **Run、RunOnce、RunOnceEx、RunServices、RunServicesOnce**这些子键保存了**Windows**启动时自动运行的程序。
- ❑ 通过在这些键中添加键值，可以比较容易地实现程序的自动加载，例如：
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunService
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run

(3). 添加系统服务

- ❑ **Windows NT**内核操作系统都大量使用服务来实现关键的系统功能。
- ❑ 服务程序是一类长期运行的应用程序，它不需要界面或可视化输出，能够设置为在操作系统启动时自动开始运行，而不需要用户登录来运行它。
- ❑ 除了操作系统内置的服务程序外，用户也可以注册自己的服务程序。木马程序就是利用了这一点，将自己注册为系统的一个服务并设置为自动运行，这样每当**Windows**系统启动时，即使没有用户登录，木马也会自动开始工作。

(4). 修改文件打开关联属性

- 通常，对于一些常用的文件如**.txt**文件，只要双击文件图标就能打开这个文件。这是因为在系统注册表中，已经把这类文件与某个程序关联起来，只要用户双击该类文件，系统就自动启动相关联的程序来打开文件。
- 修改文件打开关联属性是木马程序的常用手段。比如：正常情况下**.txt**文件的打开方式为**notepad.exe**文件，而木马可能将这类文件的关联程序修改为木马程序，这样只要打开此类文件，就能在无意中启动木马。
- 著名的国产木马——冰河就是这样做的。



例：冰河的自动加载方法

HKEY_CLASSES_ROOT根键中记录的是**Windows**操作系统中所有数据文件的信息，主要记录不同文件的文件名后缀和与之对应的应用程序。

“冰河”就是通过修改

HKEY_CLASSES_ROOT\txtfile\shell\open\command下的键值，将

“**C:\WINDOWS\notepad.exe %1**”

改为“**C:\WINDOWS\system\cmd.exe %1**”，这样一旦你双击一个**TXT**文件，原本应用**Notepad**打开该文件的，现在却变成启动木马程序了。

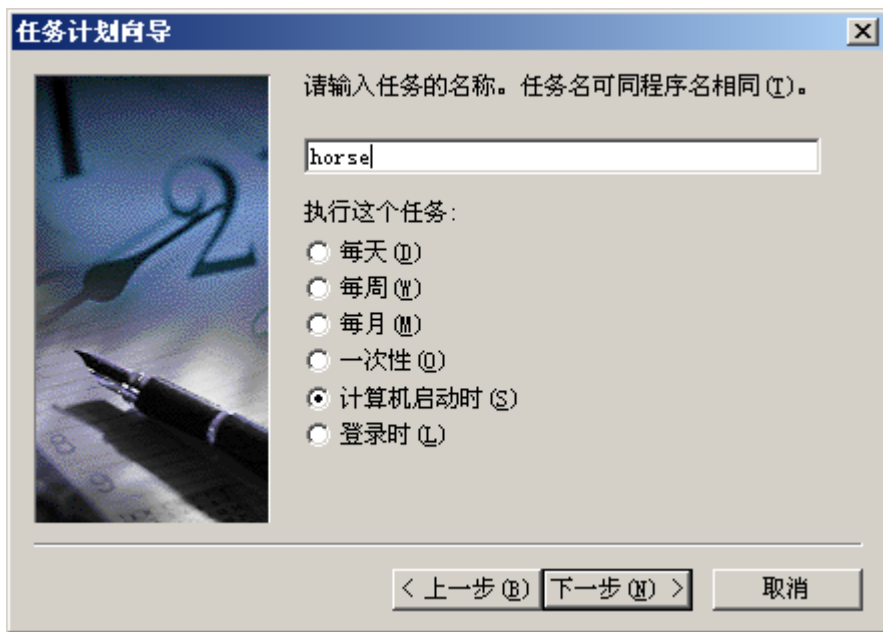
修改文件打开关联(续)

- 不仅仅是**TXT**文件，其它诸如**HTM**、**ZIP**、**RAR**等都是木马的目标，要小心。
- 对付这类木马，只能经常检查**HKEY_CLASSES_ROOT\文件类型\shell\open\command**主键，查看其键值是否正常。



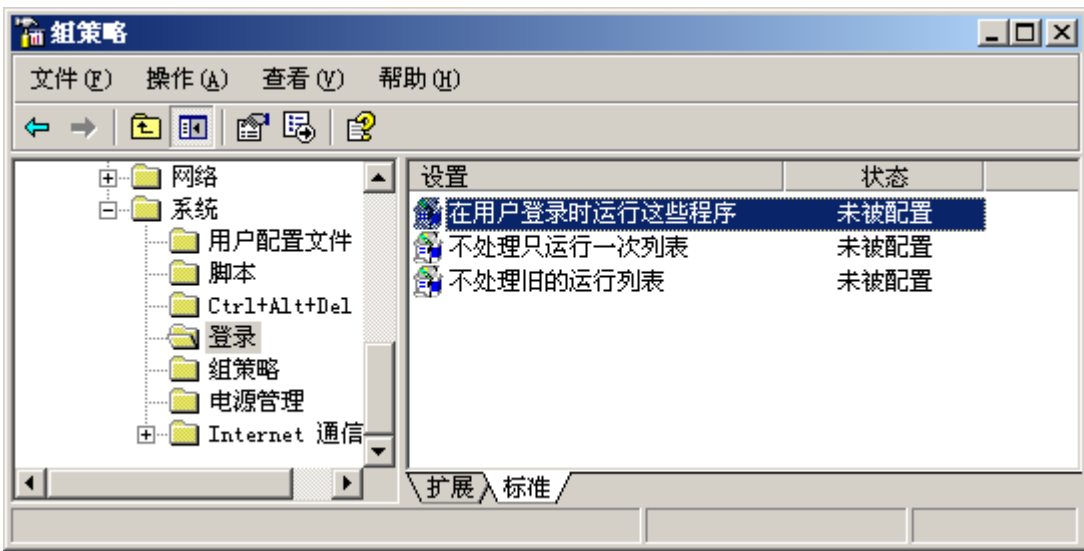
(5). 修改任务计划

- 在默认情况下，任务计划程序随**Windows**一起启动并在后台运行。如果把某个程序添加到计划任务文件夹，并将计划任务设置为“系统启动时”或“登录时”，这样也可以实现程序自启动。



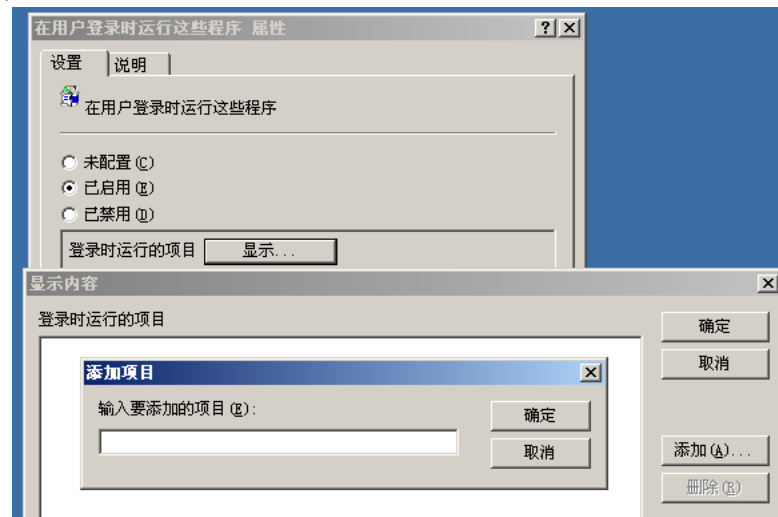
(6). 修改组策略

- ❑ 在“开始”→“运行”中输入“**gpedit.msc**”。
- ❑ 按回车，打开系统组策略窗口，选择“计算机配置”→“管理模板”→“系统”→“登录”，双击右边的“在用户登录时运行这些程序”项。



修改组策略(2)

- 打开其属性对话框，选择“已启用”，再单击“显示”，会弹出“显示内容”对话框，列表中显示的便是藏身于此的自启动程序。
- 如果你也想在这里添加自启动项目，可单击“添加”在出现的“添加项目”对话框中输入可执行文件的完整路径和文件名，“确定”即可。



(7). 修改启动文件夹

□ 当前登陆用户的“启动”文件夹

- 这是许多应用软件自启动的常用位置。当前登陆用户的“启动”文件夹一般在：**C:\Documents and Settings\<用户名字>\「开始」菜单\程序\启动**

□ 对所有用户有效的启动文件夹

- 不管用户用什么身份登录系统，放入该文件夹的快捷方式总是自动启动——这是它与用户专有的启动文件夹的区别所在。该文件夹一般在：**C:\Documents and Settings\All Users\「开始」菜单\程序\启动**



(8). 利用系统自动运行的程序

- ❑ 在**Windows**系统中，有很多程序是可以自动运行的。
- ❑ 如在对磁盘进行格式化后，总是要运行“磁盘扫描”程序（**Scandisk.exe**）；
- ❑ 按下**F1**键时，系统将运行**Winhelp.exe**或**Hh.exe**打开帮助文件；
- ❑ 系统启动时，将自动启动系统栏程序**SysTray.exe**、注册表检查程序**scanreg.exe**、计划任务程序**mstask.exe**、输入法程序、电源管理程序等。
- ❑ 这为恶意程序提供了机会，通过覆盖相应文件就可获得自动启动的机会，而不必修改系统任何设置。

(9). 替换系统DLL

- ❑ 这种方法通过**API HOOK**启动，也称为**DLL陷阱**技术。
- ❑ 它通过替换**Windows**系统中正常的**DLL**文件（动态链接文件），如**kernel32.dll**和**user32.dll**这些随系统一起启动的dll。
- ❑ 启动之后，如果是系统正常的调用请求，它就把请求转到原先的**DLL**进行处理，如果是约定的木马操作，则该**DLL**文件就实现木马服务器端的功能。

9.2.4 隐藏技术

- ❑ 木马犹如过街老鼠，人人喊打。
- ❑ 木马想要在目标主机上存活下来，还须注意隐藏自己，潜伏下来，使自身不被主机合法用户所发现。
- ❑ 隐蔽性是木马程序与其它程序的重要区别。



隐藏技术

- 想要隐藏木马的服务端，可以是伪隐藏，也可以是真隐藏。
- **伪隐藏**是指程序的进程仍然存在，只不过是让它消失在进程列表里。
- **真隐藏**则是让程序彻底的消失，不以一个进程或者服务的方式工作。



隐藏技术

- 设置窗口不可见 (从任务栏中隐藏)
- 把木马程序注册为服务 (从进程列表中隐藏)
- 欺骗查看进程的函数 (从进程列表中隐藏)
- 使用可变的高端口 (端口隐藏技术)
- 使用系统服务端口 (端口隐藏技术)
- 替换系统驱动或系统**DLL** (真隐藏技术)
- 动态嵌入技术 (真隐藏技术)

设置窗口不可见

- 这是最基本的隐藏方式。如果在**windows**的任务栏里出现一个莫名其妙的图标，傻子都会明白是怎么回事。
- 要实现在任务栏中隐藏在编程时是很容易实现的。我们以**VB**为例，只要把**from**的**Visible**属性设置为**False**，**ShowInTaskBar**设为**False**，程序就不会出现在任务栏里了。

把木马程序注册为服务

- ❑ 让木马从进程列表中消失，是木马最基本的技术了；如果木马程序出现在进程列表中，只能说这是一个很“烂”的木马。
- ❑ 在**Windows 9X/NT/2000/xp/2003**下，把木马服务端程序注册为一个服务就可以了，这样，程序就会从任务列表中消失了，因为系统不认为它是一个进程，在任务管理器中就看不到这个程序的进程。
- ❑ 但是，这种方法对于**WindowsNT/2000/xp/2003**等操作系统来说，通过服务管理器，同样会发现在系统中注册过的服务。

欺骗查看进程的函数

- ❑ 在**Windows**中有多种方法可以看到进程的存在，例如，**PSAPI(Process Status API)**、**PDH(Performance Data Helper)**和**ToolHelp API**等。
- ❑ 如果我们能够欺骗用来察看进程的函数（例如截获相应的**API**调用，替换返回的数据），就可以实现进程隐藏。

使用可变的高端口

- 一台机器有**65536**个端口，**1024**以下是系统服务端口，占用这些端口可能会造成系统不正常，这样的话，木马就会很容易暴露，大多数木马使用的端口在**1024**以上，而且呈越来越大的趋势。
- 也许你知道一些木马占用的端口，你或许会经常扫描这些端口，但现在的木马都提供端口修改功能。

使用系统服务端口

- 现在大部分木马一般在占领主机后会在**1024**以上不易发现的高端口上驻留；有一些木马也会选择一些常用的端口，如**80**、**23**。
- 有一种木马还可以做到在占领**80HTTP**端口后，收到正常的**HTTP**请求仍然把它交与**Web**服务器处理，只有收到一些特殊约定的数据包后，才调用木马程序。

替换系统驱动或系统**DLL**

- ❑ 攻击者使用自己的**DLL**文件替换掉**Windows**系统中正常的**DLL**文件。
- ❑ 这种方法利用了**Windows**系统的驱动或**DLL**，既可以启动木马，也可以隐藏木马。
- ❑ 它不使用进程，属于真隐藏技术。

替换系统驱动或系统DLL(2)

- ❑ **DLL是Windows的基础，所有API函数都是在DLL中实现的。DLL文件没有程序逻辑，由多个功能函数构成，它并不能独立运行，一般都是由进程加载并调用。正因为DLL文件不能独立运行，所以在进程列表中并不会出现DLL。**
- ❑ **DLL木马通过别的进程来运行它，如果这个进程是可信进程，就没有人会怀疑它是木马，那么这个DLL木马作为可信进程的一部分，就成为了被信赖的一部分而为所欲为。**

替换系统驱动或系统**DLL**(3)

- 这种方法与一般方法不同，它基本上摆脱了原有的木马模式---监听端口，而采用替代系统功能的方法(改写虚拟设备驱动程序**vxd**或动态链接库**DLL**文件)，木马会将修改后的**DLL**替换系统已知的**DLL**，并对所有的函数调用进行过滤。

替换系统驱动或系统**DLL**(4)

- ❑ 攻击者的**DLL**文件一般包括有函数转发器。在处理函数调用时，对于系统正常的调用请求，它就把请求直接转发给被替换的系统**DLL**进行处理；如果是约定的相应操作(事先约定好的特殊情况)，则按照约定完成所请求的功能。
- ❑ 这样做的好处是没有增加新的文件，不需要打开新的端口，没有新的进程，使用常规的方法监测不到它。

替换系统驱动或系统DLL(4)

- 需要注意的是，微软对**Windows**系统中重要的动态库有一定的保护机制。在**Windows system32**目录下有一个**dllcache**的目录，下面存放着大量**DLL**文件和重要的**.exe**文件，**Windows**系统一旦发现被保护的**DLL**文件被改动，它就会自动从**dllcache**中恢复这个文件。所以在替换系统**DLL**文件之前必须先把**dllcache**目录下的对应的系统**DLL**文件也替换掉。但是，如果系统重新安装、安装补丁、升级系统或者检查数字签名等均会使这种木马种植方法功亏一篑。

动态嵌入技术

- 另一种利用**DLL**隐藏木马的方法是动态嵌入技术，也就是将木马程序的代码嵌入到正在运行的进程中
- **Windows**系统中的每个进程都有自己的私有内存空间，一般不允许别的进程对其进行操作。但可以通过窗口**hook**（钩子函数）、挂接**API**、远程线程等方法进入并操作进程的私有空间，使木马的核心代码运行于其它进程的内存空间。这种方法比**DLL**替换技术有更好的隐藏性。

9.2.5 连接技术

- 在网络客户端/服务器工作模式中，必须具有一台主机提供服务（服务器），另一台主机接受服务（客户端），这是最起码的硬件必需，也是“木马”入侵的基础。
- 建立连接时，木马的服务端会在目标主机上打开一个默认的端口进行侦听（**Listen**），如果有客户机向服务器的这一端口提出连接请求（**Connect Request**），服务器上的相关程序（木马服务器端）就会自动运行，并启动一个守护进程来应答客户机的各种请求。

连接技术(2)

□ 其实现原理我们可以在**VB**中用**Winsock**控件来模仿实现：（**G_Server**和**G_Client**均为**Winsock**控件）

□ 服务器：

G_Server.LocalPort = 7626（木马计划打开的默认端口，可以按需改为别的值）

G_Server.Listen（等待连接）

连接技术(3)

□ 客户端:

G_Client.RemoteHost = ServerIP
(设置远端地址为服务器地址)

G_Client.RemotePort = 7626 (设置远程端口为前面所设置的默认端口, 在这里可以分配一个本地端口给, 如果不分配, 计算机将会自动分配一个)

G_Client.Connect (调用**Winsock**控件的连接方法)

连接技术(4)

- 一旦服务端接到客户的连接请求
ConnectionRequest, 就接受连接:
Public Sub
G_Server_ConnectionRequest(ByVal requestID As Long)
G_Server.Accept requested
End Sub
- 客户机端用**G_Client.SendData**发送命令, 而服务器在**G_Server_DataArrive**事件中连接并执行命令
(很多木马功能都在这个事件处理程序中实现)

连接技术(5)

- 如果客户断开连接，则关闭连接并重新侦听端口：

Private Sub G_Server_Close

G_Server.Close（关闭连接）

G_Server.Listen（再次监听）

End Sub

- 其他的部分用命令传递来进行，客户端上传一个命令，服务器解释并执行命令。

连接技术(6)

- ❑ 在建立连接过程中，对目标主机空闲端口的侦听是木马赖以建立连接的根本。目前所知的木马程序，基本都要用到侦听主机端口这一技术。
- ❑ 在计算机的**6**万多个端口中，通常把端口号**1024**以内的端口称为公认端口（**Well Known Ports**），它们紧密绑定于一些系统服务，木马程序很少应用到此类端口进行连接。而对于端口号为**1025**到**49151**的注册端口（**Registered Ports**）和端口号为**49152**到**65535**的动态或私有端口（**Dynamic or Private Ports**）则常常被木马程序所相中，用于建立与木马客户端的连接，从而实现网络入侵。

常见木马使用的端口

端口号	木马软件	端口号	木马软件
8102	网络神偷	23445	网络公牛、netbull
2000	黑洞2000	31338	Back Orifice、DeepBO
2001	黑洞2001	19191	蓝色火焰
6267	广外女生	31339	Netspy Dk
7306	网络精灵3.0、Netspy3.0	40412	The Spy
7626	冰河	1033	Netspy
8011	WRY、赖小子、火凤凰	121	BO jammerkillahv
23444	网络公牛、netbull	4590	ICOTrpjan

反弹窗口的连接技术

- ❑ 传统的木马都是由客户端（控制端）向服务端（被控制端）发起连接，而反弹窗口木马是由服务端主动向客户端发起连接。
- ❑ 这种连接技术与传统的连接技术相比，更容易通过防火墙，因为它是由内向外发起连接。

9.2.6 监控技术

- ❑ 木马连接建立后，客户端端口和服务端口之间将会出现一条通道，客户端程序可由这条通道与服务器上的木马程序取得联系，并对其进行远程控制。
- ❑ 木马的远程监控功能概括起来有以下几点：
 - 获取目标机器信息
 - 记录用户事件
 - 远程操作

(1). 获取目标机器信息

- ❑ 木马的一个主要功能就是窃取被控端计算机的信息，然后再把这些信息通过网络连接传送到控制端。
- ❑ 一般来讲，获取目标机器信息的方法就是调用相关的**API**，通过函数返回值，进行分解和分析有关成分，进而得到相关信息。

(2). 记录用户事件

- 木马程序为了达到控制目标主机的目的，通常想知道目标主机用户目前在干什么，于是记录用户事件成了木马的又一主要功能。
- 记录用户事件通常有两种方式：
 - 其一是记录被控端计算机的键盘和鼠标事件，形成一个文本文件，然后把该文件发送到控制端，控制端用户通过查看文件的方式了解被控端用户打开了哪些程序，敲了那些键；
 - 其二是在被控端抓取当前屏幕，形成一个位图文件，然后把该文件发送到控制端显示，从而通过抓取得屏幕知道目标用户的操作行为。

(3). 远程操作

- ❑ 木马程序的远程操作功能如远程关机、重启，鼠标与键盘的控制，远程的文件管理等等。
- ❑ 木马程序有时需要重新启动被控制端计算机，或者强制关闭远程计算机，当被控制计算机重新启动时，木马程序重新获得控制权。
- ❑ 在木马程序中，木马使用者还可以通过网络控制被控端计算机的鼠标和键盘，也可以通过这种方式启动或停止被控端的应用程序。
- ❑ 对远程的文件进行管理，比如共享被控端的硬盘，之后就可以进行任意的文件操作。

9.3 木马实例

- 下面我们就来看看三种比较流行的特洛伊木马，并详细介绍冰河：
 - Back Orifice
 - SubSeven
 - 国产冰河

Back Orifice

- ❑ **1998年，Cult of the Dead Cow开发了Back Orifice。**这个程序很快在特洛伊木马领域出尽风头，它不仅有一个可编程的**API**，还有许多其他新型的功能，令许多正规的远程控制软件也相形失色。
- ❑ **Back Orifice 2000（即BO2K）按照GNU GPL（General Public License）发行，希望能够吸引一批正规用户，以此与老牌的远程控制软件如pcAnywhere展开竞争。**

Back Orifice

- ❑ 但是，它默认的隐蔽操作模式和明显带有攻击色彩的意图使得许多用户不太可能在短时间内接受。
- ❑ 攻击者可以利用**BO2K**的服务器配置工具配置许多服务器参数，包括**TCP**或**UDP**、端口号、加密类型、秘密激活、密码、插件等。

Back Orifice

- ❑ **Back Orifice**的许多特性给人以深刻的印象，例如键盘事件记录、**HTTP**文件浏览、注册表编辑、音频和视频捕获、密码窃取、**TCP/IP**端口重定向、消息发送、远程重新启动、远程锁定、数据包加密、文件压缩，等等。
- ❑ **Back Orifice**带有一个软件开发工具包（**SDK**），允许通过插件扩展其功能。

Back Orifice界面

The screenshot shows the Back Orifice interface with several red annotations:

- 服务器命令 (Server Commands):** A tree view on the left containing folders like 'Simple' (with 'Ping' and 'Query' sub-items) and 'System' (with 'Reboot Machine', 'Lock-up Machine', 'List Passwords', 'Get System Info', 'Key Logging', and 'Log Keystrokes' sub-items). A red arrow points to the 'Simple' folder with the label '控制指令' (Control Command).
- 服务器反应 (Server Response):** A text area showing command execution results. A red arrow points to the text with the label '执行的结果' (Execution Result). The text includes:


```

      E$ [Unknown] (E:\) '默认共享'
      IPC$ [Unknown] ( ) '远程 IPC'
      D$ [Unknown] (D:\) '默认共享'
      ADMIN$ [Unknown] (C:\WINNT) '远程管理'
      C$ [Unknown] (C:\) '默认共享'
      
```
- 服务器列表 (Server List):** A table at the bottom showing connected servers. A red arrow points to the 'Machine' column with the label '控制的计算机在这里添加' (Add controlled computer here). Another red arrow points to the 'Address' column with the label 'IP地址' (IP Address).

Machine	Address	Connection	Encryption	Authentication
的	61.177. **	TCPIO: Back ...	XOR: B02K Si...	NULLAUTH: Si...

Other interface elements include a menu bar (File, Edit, View, Plugins, Help), a toolbar, and a right-hand panel with fields for 'Name' (的) and 'Addr' (61.177. **), a 'Disconnect' button, checkboxes for '允许入坞' (Allow Docking) and '自动-查询' (Auto-Query), a '传送命令' (Send Command) button, and a '清除反应' (Clear Response) button. A red arrow points to the 'Name' field with the label '第一步: 配套服务端数据' (Step 1:配套服务端数据).

SubSeven

- ❑ **SubSeven**可能比**Back Orifice**还要受欢迎，这个特洛伊木马一直处于各大反病毒软件厂商的感染统计榜前列。
- ❑ **SubSeven**可以作为键记录器、包嗅探器使用，还具有端口重定向、注册表修改、麦克风和摄像头记录的功能。
- ❑ 下页图显示了一部分**SubSeven**的客户端命令和服务端配置选项。

SubSeven通过客户端操作服务端





SubSeven服务端配置说明

配置类型	说明
启动方法 (Startup method)	使用启动方法来控制 SubSeven 的启动方式。 常用选项包括在 Windows 注册表的 RunService 或 Run 键下添加注册表项。 Key name 表示注册表中出现的表项的名称。
通知选项 (Notification options)	这个选项指定了如何将感染主机的信息通知攻击者。 可选的通知方法包括： ICQ 、 IRC 、 E-mail 。
保护服务器 (Protect server)	在服务端添加一个口令，这样其他人就不能够使用服务端配置编辑器来编辑该服务端了。这个口令与安装选项中的口令所起的作用是不相同的。
安装 (Installation)	指定希望 SubSeven 使用的端口号，默认为 27374 。 这里也可以设置一个口令，只有拥有这个正确口令的客户端才能够连接到本配置得到的服务端上。此外还可以选中 fake error message 选项，当 SubSeven 在服务端运行时，让粗心的用户不会怀疑正在安装木马。

SubSeven(2)

- **SubSeven**具有许多令受害者难堪的功能：攻击者可以远程交换鼠标按键，关闭/打开**Caps Lock**、**Num Lock**和**Scroll Lock**，禁用**Ctrl+Alt+Del**组合键，注销用户，打开和关闭**CD-ROM**驱动器，关闭和打开监视器，翻转屏幕显示，关闭和重新启动计算机等等。

SubSeven(3)

- ❑ **SubSeven**利用**ICQ**、**IRC**、**email**甚至**CGI**脚本和攻击发起人联系，它能够随机地更改服务器端口，并向攻击者通知端口的变化。
- ❑ 另外，**SubSeven**还提供了专用的代码来窃取**AOL Instant Messenger**（**AIM**）、**ICQ**和屏幕保护程序的密码。

冰河

- ❑ 冰河是一个非常有名的木马工具，它包括两个可运行的程序**G_Server**和**G_Client**，其中前者是木马的服务器端，就是用来植入目标主机的程序，后者是木马的客户端，也就是木马的控制台。
- ❑ 运行客户端后其界面如下页图所示。

冰河客户端界面





冰河的主要功能

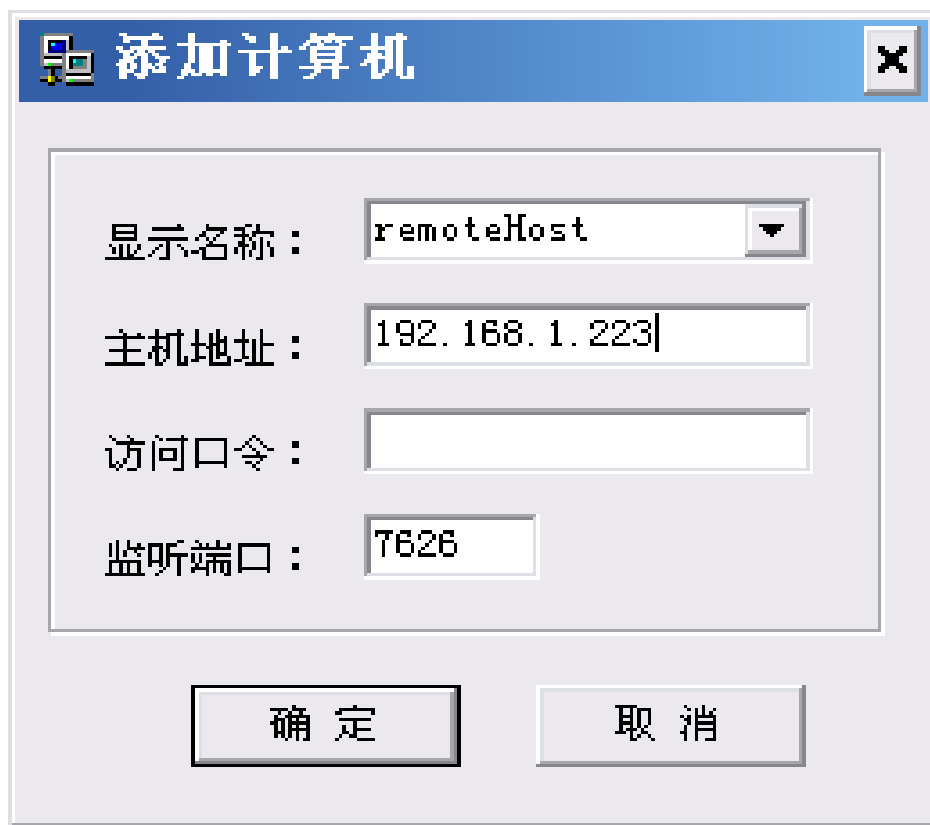
- ❑ 自动跟踪目标机屏幕变化(局域网适用)
- ❑ 完全模拟键盘及鼠标输入(局域网适用)
- ❑ 记录各种口令信息
- ❑ 获取系统信息
- ❑ 限制系统功能
- ❑ 远程文件操作
- ❑ 注册表操作
- ❑ 发送信息
- ❑ 点对点通讯

冰河的使用

- 通过使用冰河木马，我们可以实现对远程目标主机的控制。在远程目标主机上运行 **G_Server**，作为服务器端，在当前主机上运行 **G_Client**，作为控制台。

冰河的使用—连接服务器

- ❑ 服务器端运行后，可以在控制台上进行连接。单击工具栏上的快捷按钮“添加主机”，弹出如图所示的对话框，输入远程主机的相关信息即可。



添加计算机

显示名称: remoteHost

主机地址: 192.168.1.223

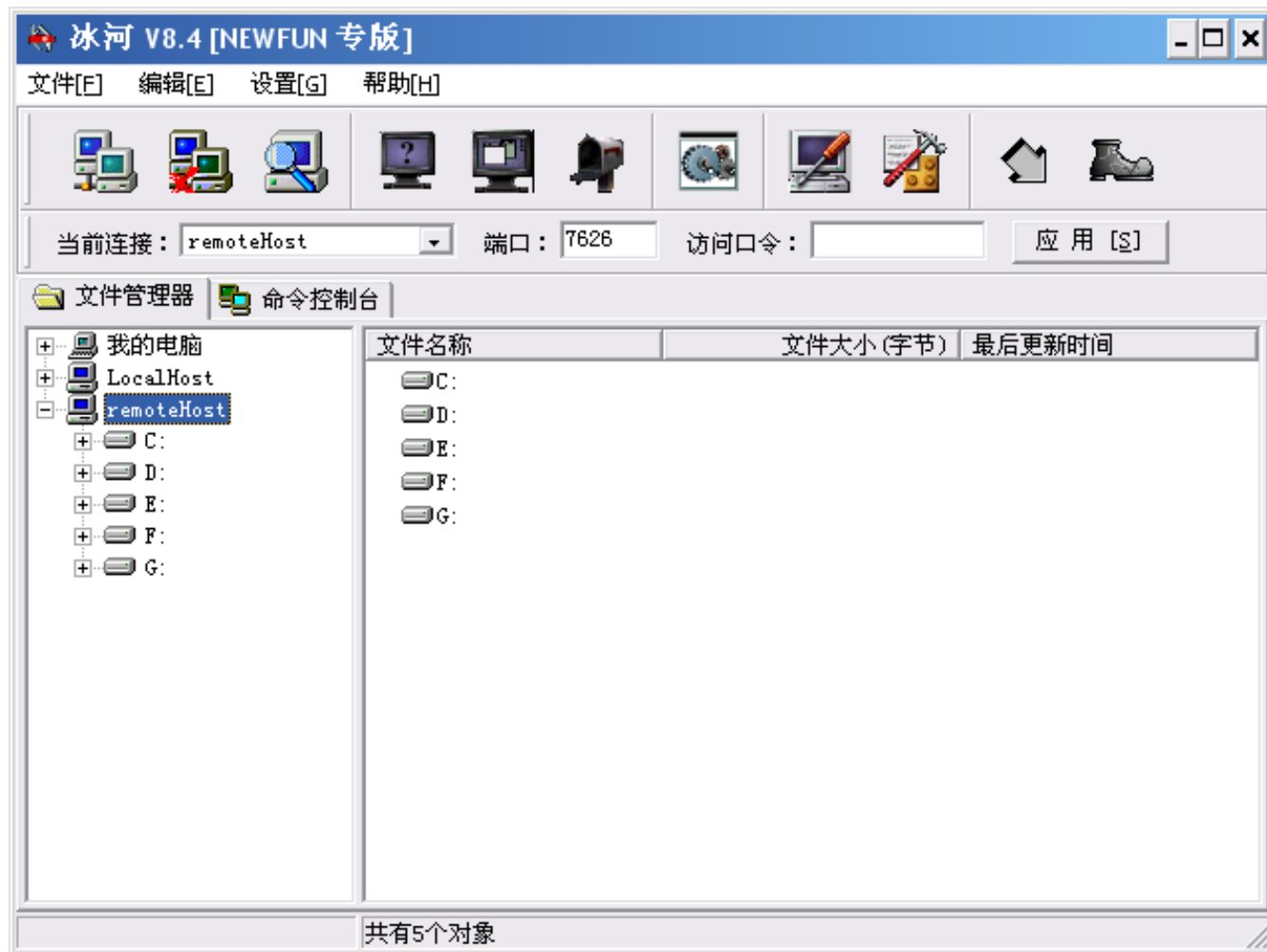
访问口令:

监听端口: 7626

确定 取消

冰河的使用—连接成功后的信息

连接成功后，则会显示远程主机上的信息如硬盘盘符等，如图所示。



冰河的使用—搜索服务器

- 以上直接连接是一种方法，冰河还可以自动搜索已经中了冰河木马的主机，只需要简单的设置即可。
- 下面两页的图是一个搜索过程。

搜索服务器



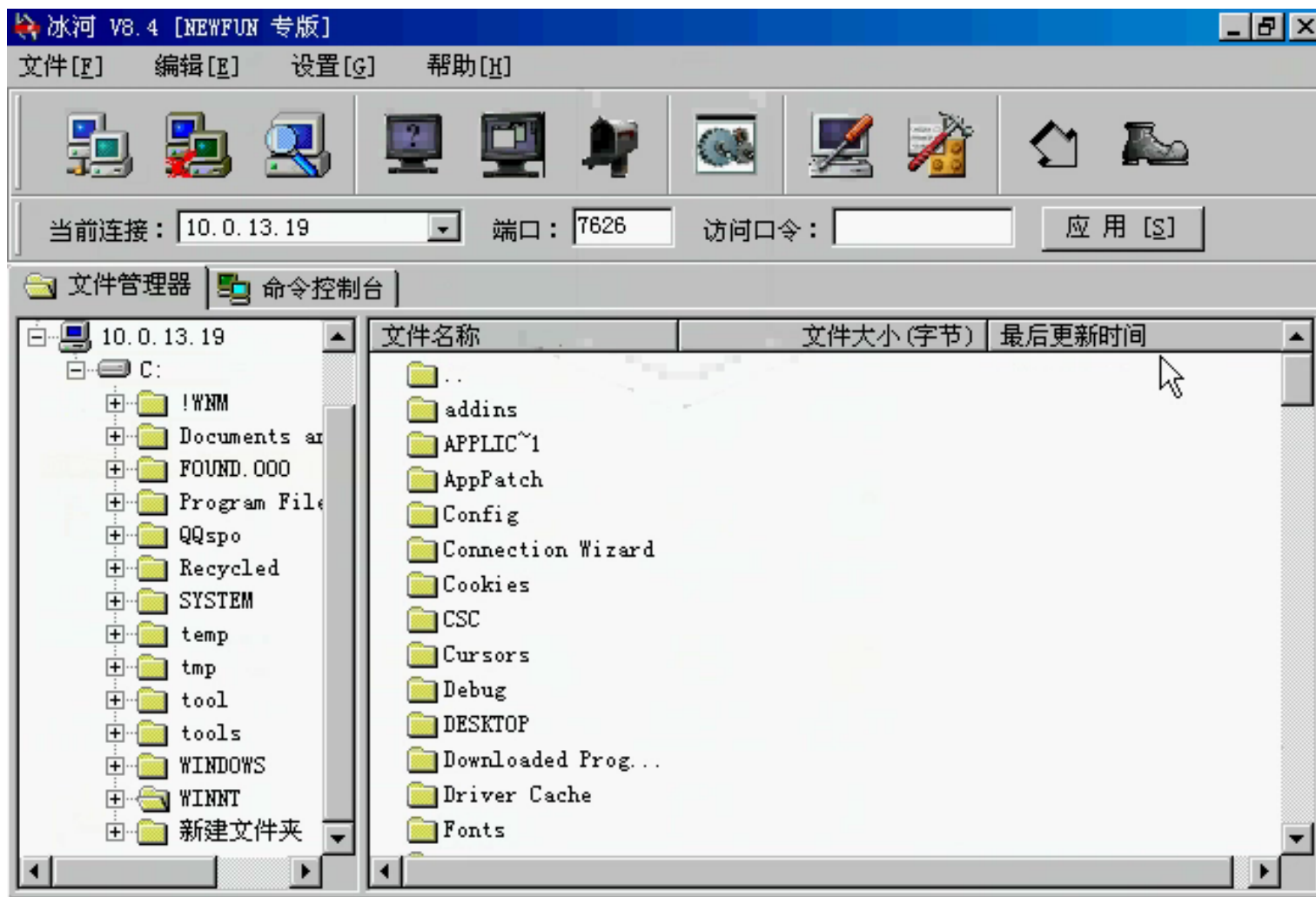
搜索到10.0.13.19



冰河的使用(续)

- 得到**10.0.13.19**中有木马服务器。下面便可对这台计算机进行操作了。
- 冰河的功能非常强大，它有“**文件管理器**”和“**命令控制台**”两个选项卡。
- 点击“文件管理器”可以管理被入侵的电脑的硬盘。如下页图所示。

文件管理器



文件管理器—下载文件



冰河的使用(续)

- 单击“命令控制台标签”，可以看到这里有众多的功能，如下页图所示。

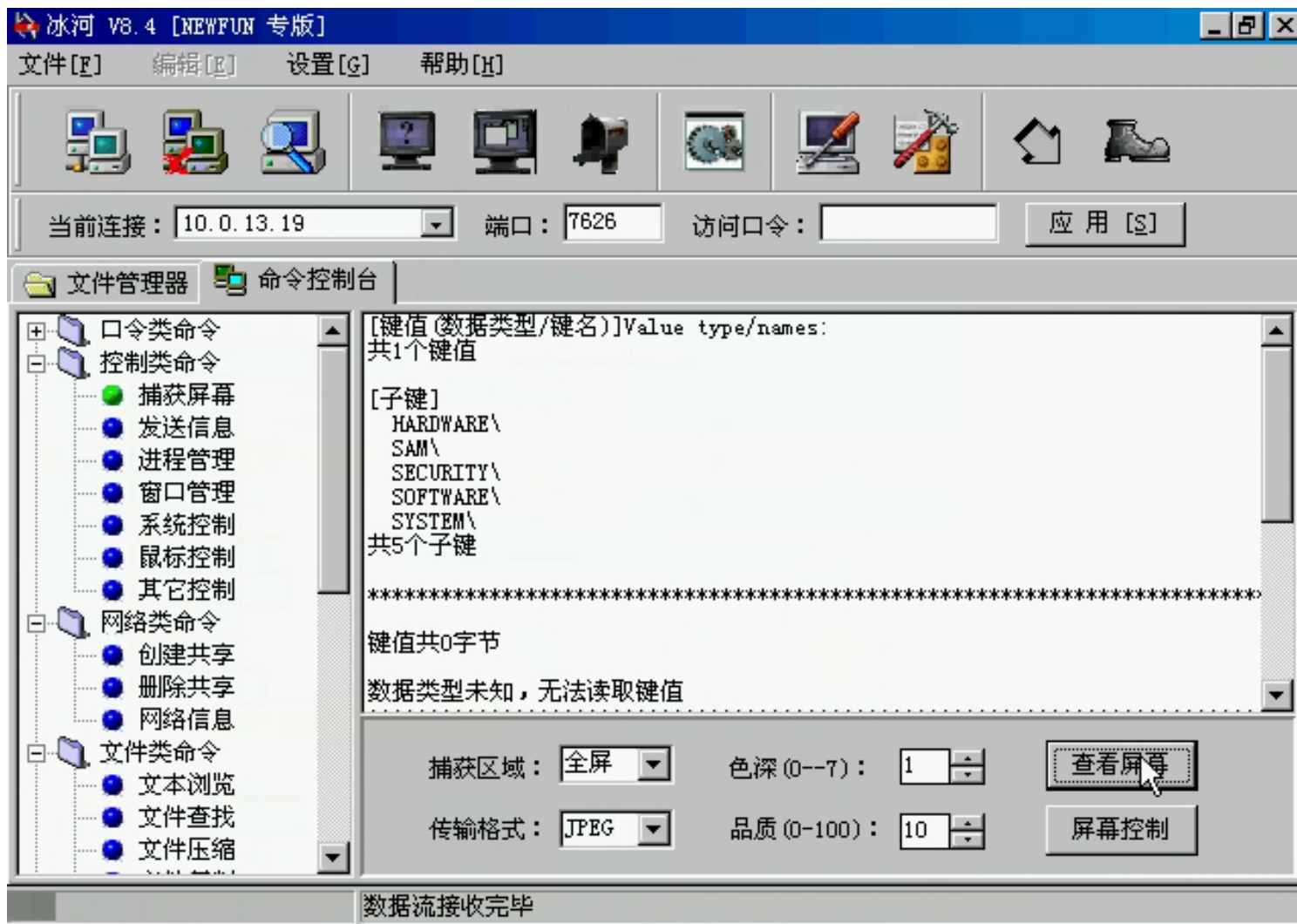
冰河的命令控制台



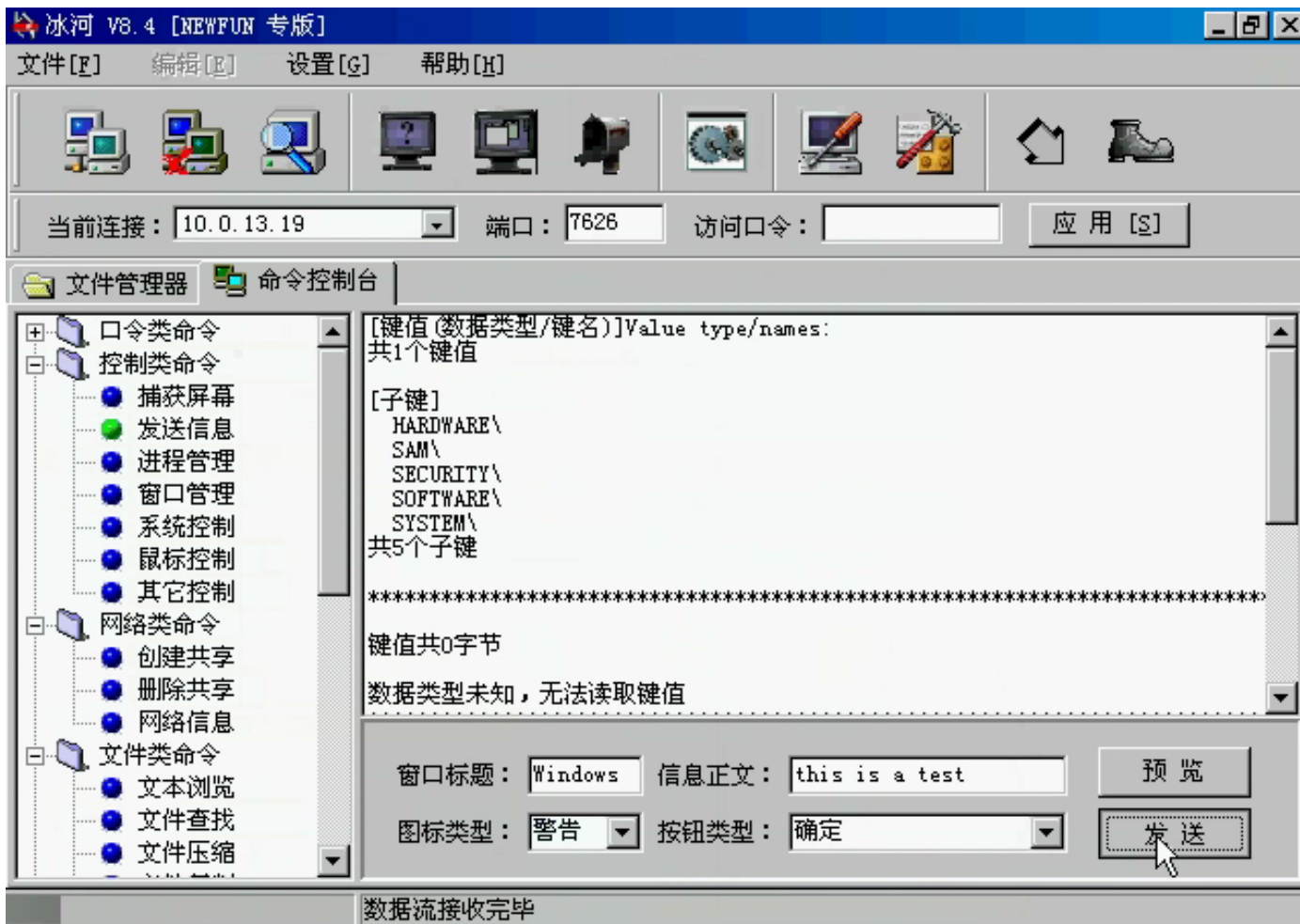
获得系统信息和口令



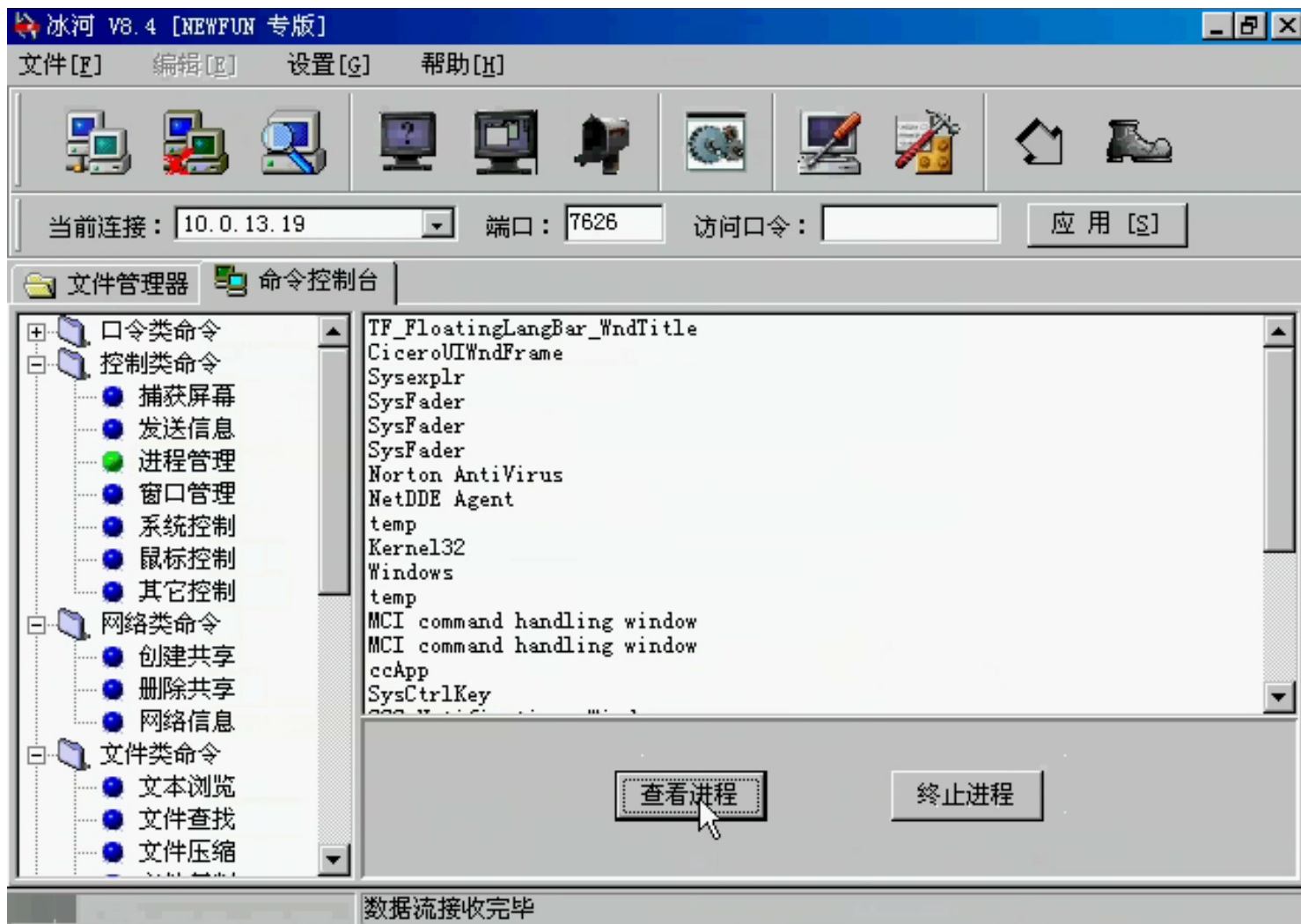
捕获对方屏幕



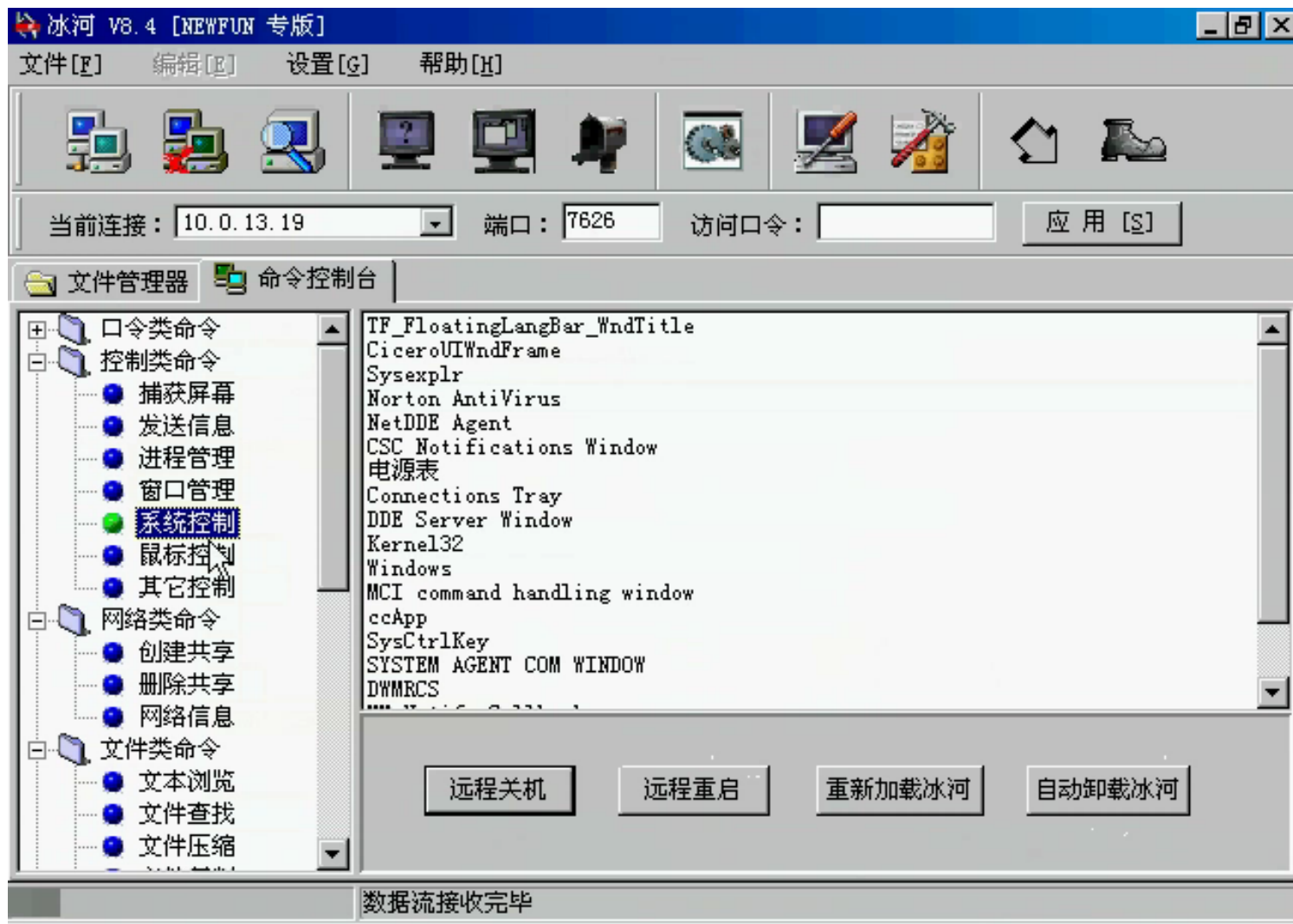
向对方发送信息



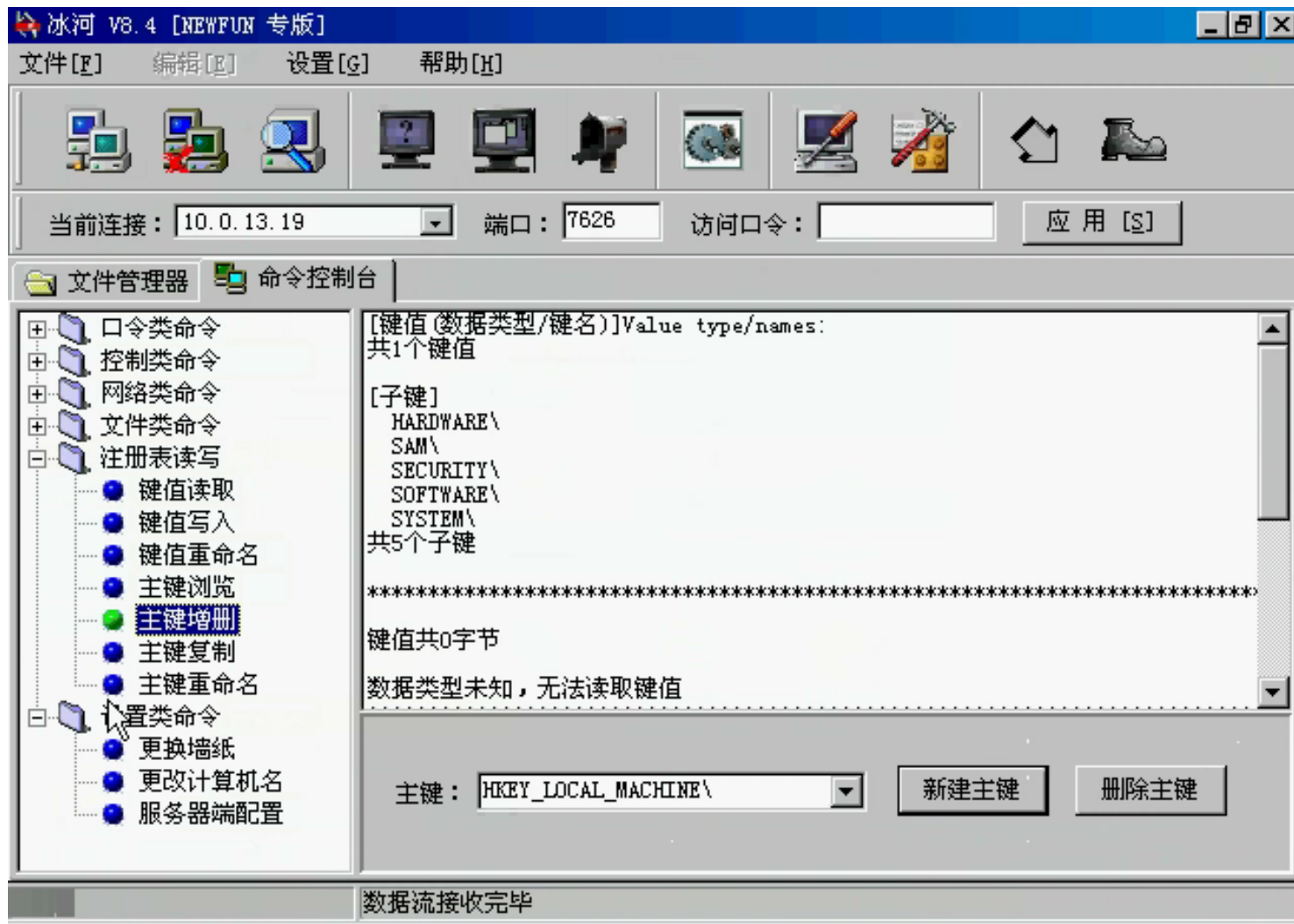
管理对方的进程



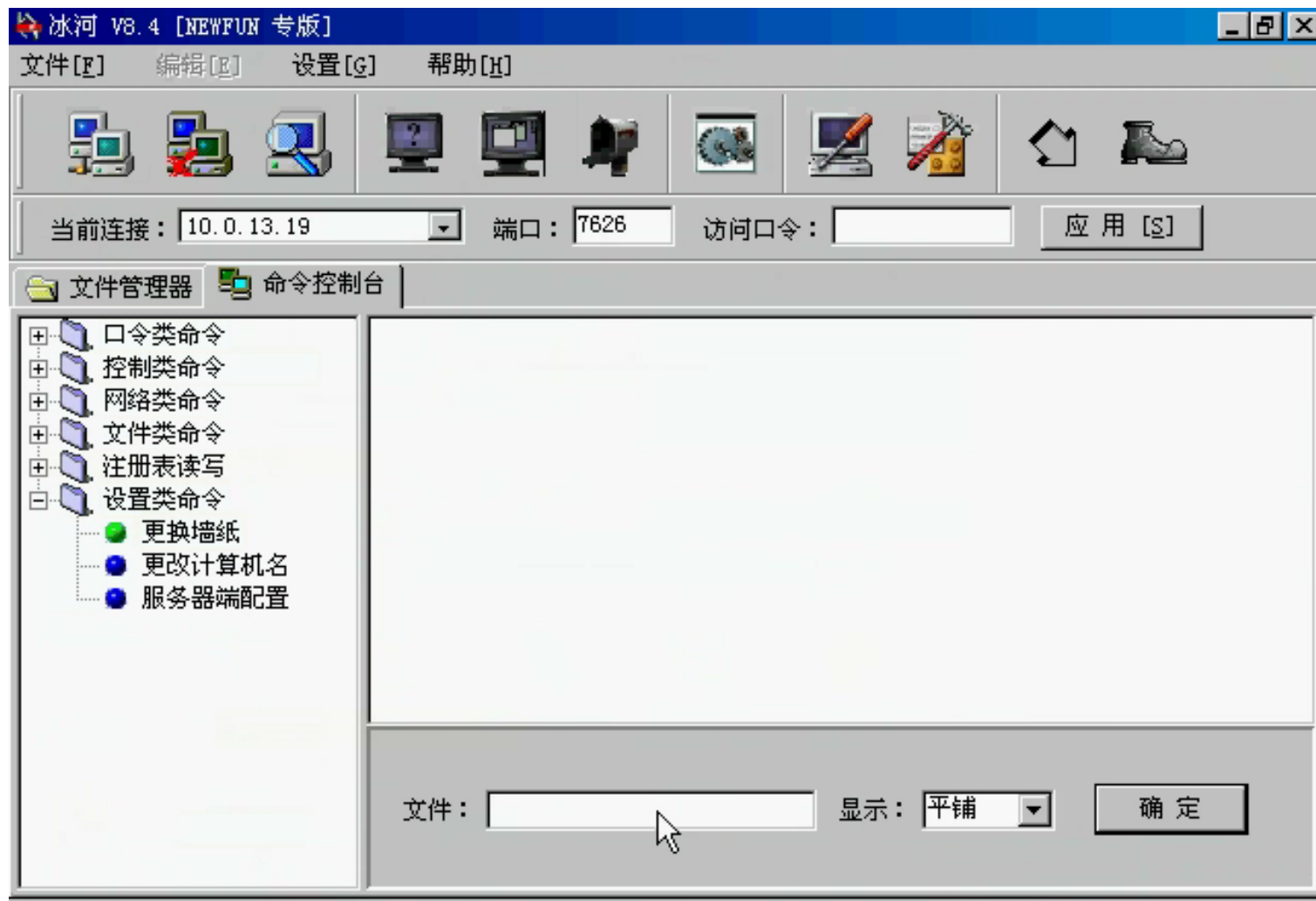
控制对方系统



注册表管理



甚至可以对桌面等其它信息设置



冰河的使用(总结)

- ❑ 可以看出，冰河的功能非常强大。几乎可以对入侵的计算机进行完全的控制。
- ❑ 可以看出，冰河可以当作一个远程管理工具使用。



9.4 木马的防御技术

- 9.4.1 木马的检测
- 9.4.2 木马的清除与善后
- 9.4.3 木马的防范

9.4.1 木马的检测

- 根据木马工作的原理，木马的检测一般有以
下一些方法：
 - 端口扫描和连接检查
 - 检查系统进程
 - 检查ini文件、注册表和服务
 - 监视网络通讯

端口扫描

- 扫描端口是检测木马的常用方法。大部分的木马服务端会在系统中监听某个端口，因此，通过查看系统上开启了那些端口能有效地发现远程控制木马的踪迹。
- 操作系统本身就提供了查看端口状态的功能，在命令行下键入“**netstat -an**”可以查看系统内当前已经建立的连接和正在监听的端口，同时可以查看正在连接的远程主机**IP**地址。

端口扫描(2)

- 对于**Windows**系统，有一些很有用的工具用于分析木马程序的网络行为。
- 例如**Fport**，它不但可以查看系统当前打开的所有**TCP / UDP**端口，而且可以直接查看与之相关的程序名称，为过滤可疑程序提供了方便。

网络测试命令**Netstat**

- **Netstat**命令可以帮助网络管理员了解网络的整体使用情况。
- 命令格式:
 - netstat [-r] [-s] [-n] [-a]
- 参数含义:
 - -r 显示本机路由表的内容;
 - -s 显示每个协议的使用状态(包括TCP协议、UDP协议、IP协议);
 - -n 以数字表格形式显示地址和端口;
 - -a 显示所有主机的端口号。

Fport工具

- ❑ **FPort**可以把本机开放的**TCP/UDP**端口同应用程序相关联，并可以显示进程**PID**，名称和路径。
- ❑ 通过**Fport**，用户可以根据端口号来查找程序名称和路径。
- ❑ 和使用 ‘**netstat -an**’命令产生的效果类似。

检查系统进程

- ❑ 既然木马的运行会生成系统进程，那么对系统进程列表进行分析和过滤也是发现木马的一个方法。
- ❑ 虽然现在也有一些技术使木马进程不显示在进程管理器中，不过很多木马在运行期都会在系统中生成进程。因此，检查进程是一种非常有效的发现木马踪迹的方法。
- ❑ 使用进程检查的前提是需要管理员了解系统正常情况下运行的系统进程。这样当有不属于正常的系统进程出现时，管理员能很快发现。

检查.ini文件、注册表和服务

□ **Windows**系统中能提供开机启动程序的几个地方:

- 开始菜单的启动项，这里太明显，几乎没有木马会用这个地方。
- **win.ini / system.ini**，有部分木马采用，不太隐蔽。
- 注册表，隐蔽性强且实现简单，多数木马采用。
- 服务，隐蔽性强，部分木马采用。

检查ini文件、注册表和服务(2)

- 在**win.ini**和**system.ini**中启动的木马比较容易查找，只要使用记事本打开这两个文件，查看“**run=**”、“**load=**”或是“**shell=**”后面所加载的程序，如果所加载的程序有你不知道的程**序**，那就要小心了，这就有可能是木马了。

检查ini文件、注册表和服务(3)

- 前面说过，在注册表中，**Run**、**RunOnce**、**RunOnceEx**、**RunServices**、**RunServicesOnce**这些子键保存了**Windows**启动时自动运行的程序。

- 所以在注册表中，最有可能隐藏木马的地方是：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce



检查ini文件、注册表和服务(5)

- 当然，在注册表中还存在其他可以实现开机自动加载的地方。



检查ini文件、注册表和服务(6)

- ❑ 在**Win NT/2000/xp/2003**系统中，一些木马会将自己做为服务添加到系统中，甚至随机替换系统中没有启动的服务程序来实现自动加载。
- ❑ 检测这类木马需要对操作系统的所有常规服务有较深入的了解。

监视网络通讯

- 一些特殊的木马程序(如通过**ICMP**协议通讯), 被控端不需要打开任何监听端口, 也无需反向连接, 更不会有什么已经建立的固定连接, 使得**netstat**或**fport**等工具很难发挥作用。

监视网络通讯(2)

- 对付这种木马，除了检查可疑进程之外，还可以通过**Sniffer**软件监视网络通信来发现可疑情况。首先关闭所有已知有网络行为的合法程序，然后打开**Sniffer**软件进行监听，若在这种情况下仍然有大量的数据传输，则基本可以确定后台正运行着恶意程序。
- 这种方法并不是非常的准确，并且要求对系统和应用软件较为熟悉，因为某些带自动升级功能的软件也会产生类似的数据流量。



9.4.2 木马的清除与善后

- (1). 清除木马
- (2). 处理遗留问题

(1). 清除木马

- 知道了木马加载的地方，首先要作的当然是将木马登记项删除，这样木马就无法在开机时启动了。
- 不过有些木马会监视注册表，一旦你删除，它立即就会恢复回来。因此，在删除前需要将木马进程停止，然后根据木马登记的目录将相应的木马程序删除。

清除木马(2)

- 随着木马编写技术的不断进步，很多木马都带有了自我保护的机制，木马类型不断变化，因此，不同的木马需要有针对性的清除方法。
- 因此，对于普通用户来说，清除木马最好的办法是借助专业杀毒软件或是清除木马的软件来进行。普通用户不可能有足够的时间和精力没完没了地应付各种有害程序；分析并查杀恶意程序是各大安全公司的专长，所以对于大多数用户来说，安装优秀的杀毒软件和防火墙软件并定期升级，不失为一种安全防范的有效手段。



实例：检测与清除“冰河”

- ❑ 下面以手工检测及清除“冰河”为例，向大家讲解对一般木马的清除方法。
- ❑ 先检测冰河木马是否存在，如果存在，再清除。

检测“冰河”(1)

- ❑ **1)**首先运行注册表编辑器，检查注册表中**txt**文件的关联设置，如果注册表项 **HKEY_LOCAL_MACHINE \ SOFTWARE \ Classes \ txtfile \ shell \ open \ command** 处的键值是 **<winpath> \ notepad.exe %1 (<winpath>是指您的WINDOWS所在目录，如“c:\windows”)**，则该设置项为正常。

检测“冰河”(2)

- 2)接着检查注册表中的**EXE**文件关联设置，如果注册表项 **HKEY_LOCAL_MACHINE \ SOFTWARE \ Classes \ exefile \ shell \ open \ command**处的键值是“%1”%*，则该项设置正常。
- 3)冰河在运行时会将自身与**txt**文件或**exe**文件关联，如果这两个注册表项都正常，则系统上没有安装有冰河软件。

清除“冰河” (1)

- ❑ 打开注册表，在键目录 **HKEY_LOCAL_MACHINES\SOFTWARE\Microsoft\Windows\CurrentVersion\Run** 和 **HKEY_LOCAL_MACHINES\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices** 中查看有没有 **kernel32.exe** 键值，这就是冰河所设置的随系统自启动，需要删除。
- ❑ 事实上，这两个键目录也经常是其他一些木马或病毒设置键值的地方。



清除“冰河” (2)

- 进入系统目录**System32**，删除冰河木马的可执行文件**kernel32.exe**和**sysexplr.exe**。

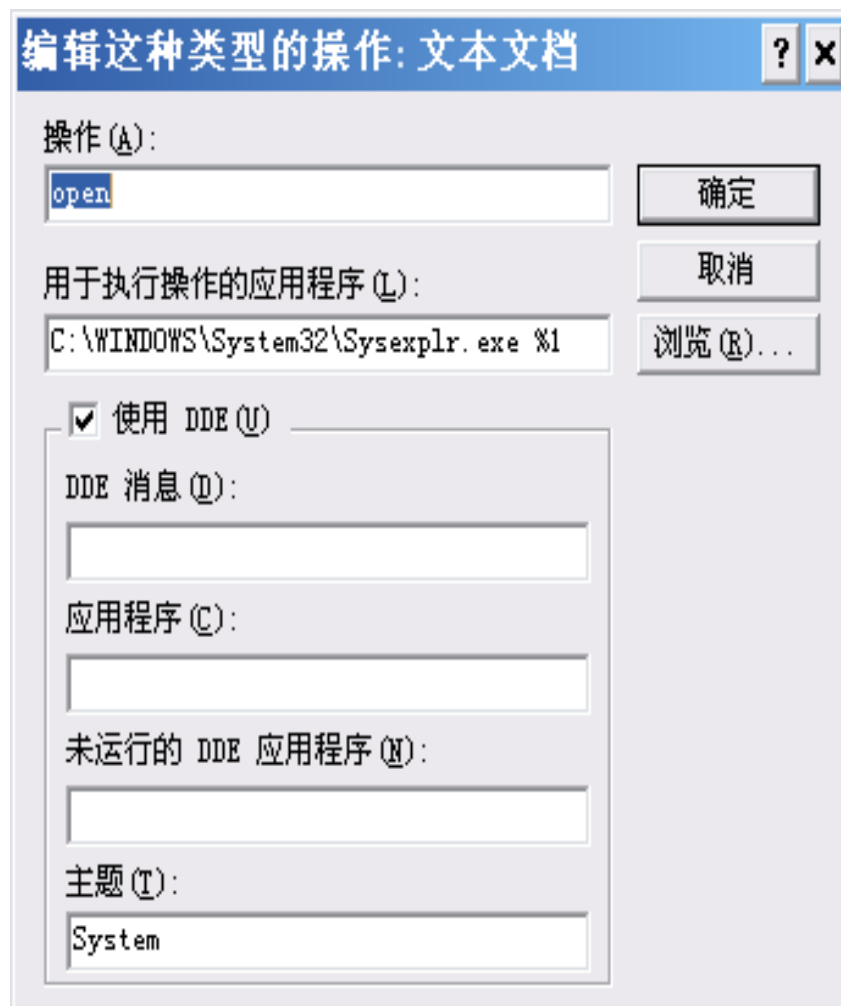
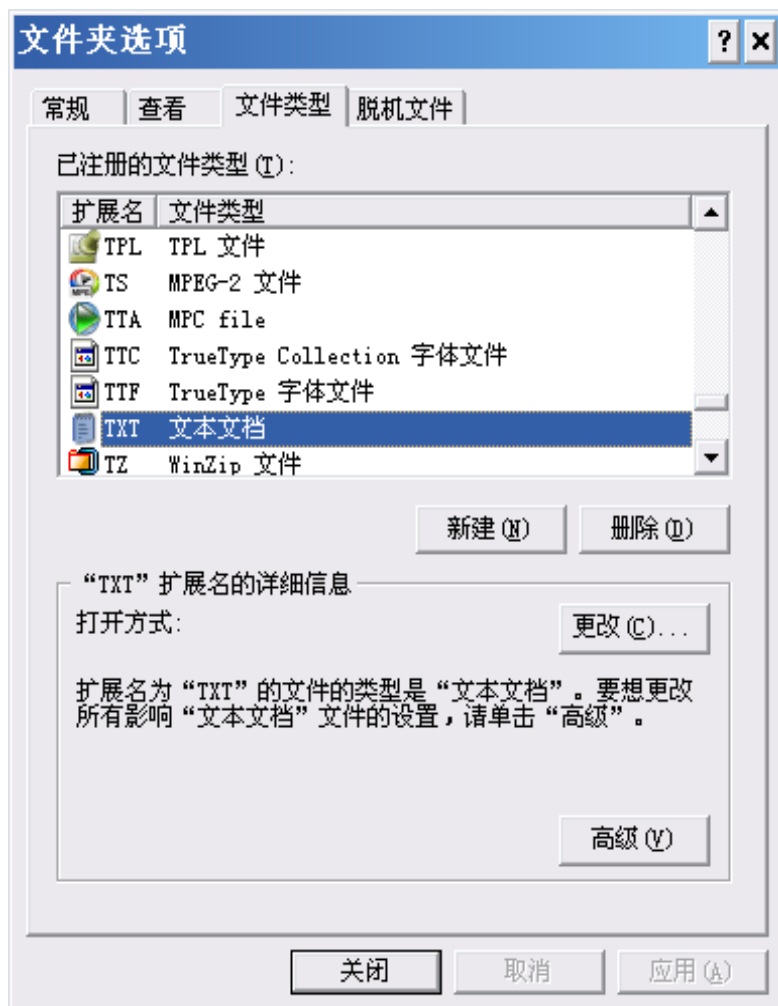
清除“冰河”(3)

□ 最后修改文件关联。

冰河木马会将记事本文件**TXT**的缺省打开方式由记事本变为木马程序，可以通过在“我的电脑”中的菜单“工具”中的“文件夹选项”来修改文件关联，如下页第**1**个图所示。

□ 将记事本文件的打开由木马程序恢复为 **notepad.exe**，如下页第**2**个图所示。对于**html**、**exe**、**zip**、**com**文件也都需要采用同样的方法修改。

修改文件关联的图示



清除“冰河” (4)

- 最后重新启动，然后用杀毒软件对系统进行一次全面的扫描，这样可以排除遗漏的木马程序。

(2). 处理遗留问题

- 检测和清除了特洛伊木马之后，另一个重要的问题浮现了：远程攻击者是否已经窃取了某些敏感信息？危害程度多大？要给出确切的答案很困难，但你可以通过下列问题确定危害程度。

处理遗留问题(2)

- 首先，特洛伊木马存在多长时间了？文件创建日期不一定值得完全信赖，但可供参考。

利用**Windows**资源管理器查看特洛伊木马执行文件的创建日期和最近访问日期，如果执行文件的创建日期很早，最近访问日期却很近，那么攻击者利用该木马可能已经有相当长的时间了。

处理遗留问题(3)

- 其次，攻击者在入侵机器之后有哪些行动？攻击者访问了机密数据库、发送**Email**、访问其他远程网络或共享目录了吗？攻击者获取管理员权限了吗？仔细检查被入侵的机器寻找线索，例如文件和程序的访问日期是否在用户的办公时间之外？

处理遗留问题(4)

- 在安全要求较低的环境中，大多数用户可以在清除特洛伊木马之后恢复正常工作，只要日后努力防止远程攻击者再次得逞就可以了。至于安全性要求一般的场合，最好能够修改一下所有的密码，以及其他比较敏感的信息（例如信用卡号码等）。
- 在安全性要求较高的场合，任何未知的潜在风险都是不可忍受的，必要时应当调整管理员或网络安全的负责人，彻底检测整个网络，修改所有密码，在此基础上再执行后继风险分析。对于被入侵的机器，重新进行彻底的格式化和安装。

9.4.3 木马的防范

- 虽然木马程序隐蔽性强，种类多，攻击者也设法采用各种隐藏技术来增加被用户检测到的难度，但由于木马实质上是一个程序，必须运行后才能工作，所以会在计算机的文件系统、系统进程表、注册表、系统文件和日志等中留下蛛丝马迹，用户可以通过“**查、堵、杀**”等方法检测和清除木马。

木马的防范(2)

- 其具体防范技术方法主要包括：检查木马程序名称、注册表、系统初始化文件和服务、系统进程和开放端口，安装防病毒软件，监视网络通信，堵住控制通路和杀掉可疑进程等。

木马的防范(3)

□ 以下是一些常用的防范木马程序的措施:

- 及时修补漏洞，安装补丁
- 运行实时监控程序
- 培养风险意识，不使用来历不明的软件
- 即时发现，即时清除

及时修补漏洞，安装补丁

- 及时安装系统及应用程序的补丁可以保持这些软件处于最新状态，同时也修复了最新发现的漏洞。通过漏洞修复，最大限度地降低了利用系统漏洞植入木马的可能性。

运行实时监控程序

- 选用实时监控程序、各种反病毒软件，在运行下载的软件之前用它们进行检查，防止可能发生的攻击。同时还要准备如**Cleaner**、**LockDown**、木马克星等专门的木马程序清除软件，用于删除系统中已经存在的感染程序。有条件的用户还可以为系统安装防火墙，这能够大大增加黑客攻击成功的难度。

培养风险意识，不使用来历不明的软件

- 互联网中有大量的免费、共享软件供用户下载使用，很多个人网站为了增加访问量也提供一些趣味游戏供浏览者下载。
- 而这些下载的软件很可能就是一个木马程序，对于这些来历不明的软件最好不要使用，即使通过了一般反病毒软件的检查也不要轻易运行。

培养风险意识，不使用来历不明的软件

- ❑ 对不熟悉的人发来的**E-mail**不要轻易打开，带有附件就更要小心了。
- ❑ 加强邮件监控系统，拒收垃圾邮件。
- ❑ 如实在想接收，最好用查杀病毒或是木马软件进行查杀一下，然后再打开。

即时发现，即时清除

- 在使用电脑的过程中，注意及时检查系统，发现异常情况时，如突然发现蓝屏后死机；鼠标左右键功能颠倒或者失灵；文件被莫名其妙地删除等，请按前面的办法立即查杀木马。
- 另外严禁物理接触，提防他人使用后台监视记录程序来监控自己的计算机。不要以为自己计算机中没有什么吸引人的东西而疏忽大意，很多人使用木马只是出于好奇，想过一把黑客瘾，先用木马控制你的计算机，然后以你的计算机为基础对其它服务器进行攻击，这是潜在的危险因素。

9.5 木马的发展趋势

□ 随着计算机网络技术和程序设计技术的发展，木马程序的编制技术也在不断变化更新。目前主要体现出以下一些发展趋势：

- 跨平台
- 模块化设计
- 无连接木马
- 主动植入
- 木马与病毒的融合

跨平台

- 对于**Windows**系统而言，一般木马的使用者都希望一个木马既可以在**Windows98**下使用，也可以在**Windows2000/XP/2003**下使用，即希望木马具有跨平台特性。
- 但是**Windows 2000/XP/2003**的工作机制毕竟与**Windows 9x**有一定的差别，例如在**Windows2000/XP/2003**中具有了权限的概念，编写**Windows 2000/XP/2003**下的木马需要更高的手段，如进程隐藏、进程控制等。
- 现在有些木马已经实现了这种跨平台运行的功能，随着**Windows**操作系统新版本的不断推出，木马的跨平台运行能力将是未来木马程序所必须具备的。

模块化设计

- 模块化设计是软件开发的一种趋势，模块化使得软件具有很好的可扩展性。现在很多木马程序已经有了模块化设计的概念。
- 比如，**BO**、**Sub7**等经典木马都有一些优秀的插件相继问世。
- 木马程序在开始运行时可以很小，这样有利于植入；一旦植入，在控制过程中，可以从控制端传送某些模块到被控制端，扩展程序的功能。

无连接木马

- ❑ 传统的远程控制木马使用**TCP**协议进行工作，因此，服务端程序在工作时，需要打开一个端口，与客户端程序建立**TCP**连接。
- ❑ 对一个稍具网络常识的用户来说，只要使用一个简单的**netstat**命令就可以发现木马的蛛丝马迹。

无连接木马(2)

- 针对这种情况，未来的木马可能采用其他的网络协议进行通讯而非**TCP**协议。
- 例如使用**ICMP**协议，这样的通信报文是不需要通过端口的，由系统内核进行处理。
- 利用**ICMP**协议通信的木马可以通过监听主机上的**ICMP**报文，一旦在报文中发现包含控制命令，就执行相应的操作。
- 这样的木马在理论上是不需要工作端口的。当然这样的木马也存在局限性，最主要的问题是无法进行交互式的操作，控制端发送一个命令过去后，无论执行是否成功，客户端都不会获得响应的，还有无法进行数据传递等一系列问题。

无连接木马(3)

- 所以，无连接木马技术需要与传统的木马技术相结合使用。正常情况下木马不开启端口，只监听**ICMP**数据报。
- 一旦在**ICMP**报文中发现有控制命令，就打开一个端口等待客户端的连接。客户端完成连接控制后，木马又将端口关闭，回到隐藏的状态。

主动植入

- ❑ 大多数的木马程序都是通过目标系统用户打开邮件、点击网页等方式被动植入目标系统的。
- ❑ 但是从木马使用者的角度考虑，更希望木马能够具有主动植入的功能。
- ❑ 这样，攻击者就没有必要等待目标系统用户的某个随机行为，而是可以完全主动的将木马程序植入目标系统。
- ❑ 这样的技术已经逐渐成熟，现在，利用一些系统漏洞直接从远程主动植入木马已经实现。

木马与病毒的融合

- 从理论上讲，木马和病毒的定义划分是比较清晰的。但是随着技术研究的深入，在实际应用的过程中，各种技术有了相互借鉴、取长补短的趋势。从而使得一个具体的程序，你很难定性的说它是木马不是病毒或者说它是病毒而不是木马。
- 从传统意义来看，木马与病毒最基本的区别就在于病毒有很强的传染性而木马没有。也正是由于这个原因，为了借鉴病毒的传播特性，向病毒化发展可以说是一个趋势。可以想象一下，一个具有病毒一样传染能力的木马对互联网的安全将是一个多大的威胁。

9.6 小结

- 由于网络的广泛使用，为了避免计算机感染木马程序，造成难以估量的损失，保障安全，最好的办法就是尽量熟悉特洛伊木马的类型、工作原理，掌握如何检测、防范和清除这些不怀好意代码的方法和手段。



Thank you for your attention!

