毕业论文（设计）

论文（设计）题目：木马攻击技术彻底剖析

学　　院：理工学院

专　　业（方　向）：计算机科学与技术（网络工程）

年　　级、班　　级：网络 1101

学　生　姓　名：

指　导　老　师：

2015 年 5 月 15 日

论文独创性声明

本人所呈交的毕业论文（设计）是我个人在指导教师指导下进行的研究工作及取得的成果。除特别加以标注的地方外，论文中不包含其他人的研究成果。本论文如有剽窃他人研究成果及相关资料若有不实之处，由本人承担一切相关责任。

本人的毕业论文（设计）中所有研究成果的知识产权属三亚学院所有。本人保证：发表或使用与本论文相关的成果时署名单位仍然为三亚学院，无论何时何地，未经学院许可，决不转移或扩散与之相关的任何技术或成果。学院有权保留本人所提交论文的原件或复印件，允许论文被查阅或借阅；学院可以公布本论文的全部或部分内容，可以采用影印、缩印或其他手段复制保存本论文。

加密学位论文解密之前后，以上声明同样适用。

论文作者签名：

年　　月　　日

木马攻击技术彻底剖析

摘要

如今是大数据的时代，有效的信息能够带来巨大的效益，它作为一种普遍性、共享性、增值型、可处理性和多效用性的资源，使其对于人类具有特别重要的意义。信息安全的实质就是要保护信息系统或网络信息传输中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。信息安全是一个不容忽视的国家安全战略，任何国家、政府、部门、行业都不可避免的问题。因此，在计算机信息安全领域，对计算机木马技术的研究已成为一个重点和热点。本文对计算机木马攻击技术进行了系统的分析和研究，主要工作如下：

1．对木马的基本概念进行说明、攻击机制进行剖析。

2．采用“冰河”实例进行剖析说明。

3．在研究了木马隐蔽技术的基础上，提出了一个动静特征相结合的行为木马特征检测技术基本框架。尽最大能力去检测与防范木马攻击。

【关键词】 木马攻击,计算机信息安全,木马检测,木马防范

Trojan horse attack technologys Thorough analysis

Abstract

Today is the era of big data, effective information can bring huge benefits, it is a kind of universality, sharing, value-added, processing multi utility of resources, which is of special significance for human. The essence of information security is to protect the information systems or information transmission network information resources from various types of threats, interference and destruction, which is to ensure the safety of information. Information security is an important national security strategy, any country, government, departments, industries are inevitable problems. Therefore, in the field of computer information security, research on computer Trojan technology has become a key and hot. This paper carried out a systematic analysis and Research on computer technology of the Trojan horse attack, the main work is as follows:

1. analyze the attack mechanism of basic concepts of Trojan horse.
2. by the analysis of examples to illustrate the "ice age".
3. According to the static characteristics of the Trojan based on the

weaknesses and Trojan hidden methods, put forward the basic framework of the Trojan detection system of the static characteristics o Trojan detection and dynamic behavior of Trojan detection combined, as much as possible to prevent the Trojan horse attack.

[Key words] Trojan attacks,computer information security,Trojan detection, Trojan guard

目录

1 绪论

1.1 木马研究的背景与意义

如今计算机科学技术的迅猛发展和广泛应用，使计算机之间的网络通信成为现代社会不可缺少的基本组成部分，具有全球化的互联网技术影响着人类经济、政治、社会的方方面面，对经济可持续发展、国家信息安全、国民教育和现代化管理都起着重要的作用。随着网络技术的和信息化应用范围的不断扩大，人们享受到网络带来巨大便利的同时也带来了各种各样的安全威胁。例如黑客网络攻击，特洛伊木马、计算机病毒泛滥等。360 的抽样调查统计显示，2014 年国内有约为 31.6%比例的风险人群受到木马病毒攻击，其中有约为 1.19%的高危人群。按照 CNNIC 在 2014 年 7 月发布《第 34 次中国互联网络发展状况统计报告》公布的用 6.32 亿的中国网民来计算，2014 年属于风险人群的网民约有 2 亿，在 90 天内至少会曾遭到一次木马病毒攻击。其中，一个礼拜内至少遭遇一次木马攻击的网民约 752.1 万，属于计算机经常被木马病毒“拜访”的高危人群。它们习惯用的手段是欺骗，让用户在毫不知情的情况下进行隐蔽性安装。将记录获得的信息发送给控制方，因而计算机信息的安全以及个人隐私受到了威胁，人们正常的工作和生活都受到了严重的影响。因此，自己的计算机信息安全该如何去保护是目前的重中之重。

目前很多反病毒软件也能够对特洛伊木马进行检测查杀，但是都基于一种静态特征码来检测，即从不同类别的特洛伊木马和计算机病毒等恶意代码样本中抽取出特征码，放进病毒库中，用来与将要检测的软件进行特征码对比，如果相匹则为恶意代码。但是这静态特征检测技术不能够去适应各种与木马对抗，因为其检测能力完全依赖已知的木马静态

库，属于被动的去检测，有一定的滞后性。检测新型的木马是一项持久繁重的工作，要及时收集、抽取新型木马的静态特征并更新静态特征库。由此提出了一种基于自主的、行为的、动态的木马检测技术，能够弥补基于静态特征检测技术的不足，往后的木马检测技术都是这方向前进。

如何辨别系统行为是否正常和是否有木马在攻击都是基于动态行为检测技术的热点和难点。特洛伊木马的主要特征是行为的潜伏性和目的的针对性。因此管控木马存活的系统资源和木马的潜伏途径以及行为，通过网络间的通信进行过滤和分析。这是木马动态监测技术的主要思想。本文对木马检测的入侵提出了一个基于动态监测系统的基本框架。在网络信息通信间提升木马查杀的可靠性。

1.2 本课题研究的内容

论文对木马攻击与防范技术进行了系统的分析研究，主要工作如下：

1．对木马的基本概念进行系统说明、攻击机制进行剖析。

2．采用“冰河木马”实例进行说明剖析。

3．在研究了木马隐蔽技术的基础上，提出了一个动静特征相结合的行为木马特征检测技术基本框架。尽最大能力去检测与防范木马攻击。

2 木马攻击机制剖析

2.1 概述

“木马”是“特洛伊木马”的简称，源译 Trojan horse。Trojan horse 源自一个古希腊神话故事：传说希腊人攻打特洛伊城，久久不能占领，一个木马计划由此而生，让士兵潜伏于巨大的木马中，大部队故意撤退而将木马弃在特洛伊城，让敌人把它当做战利品拖入城内。之后乘夜晚敌人庆祝胜利、降低警惕时从木马中爬出来，与城外的部队里因外合占领特洛伊城。

而计算机网络中的木马（Trojan），是指潜伏在正常程序中的一段具备特殊功能的代码，它本身也是一种远程控制软件，但它和正规远程控制软件有着质区别：木马是不经过用户授权，以欺骗和网络入侵的手段装置到目标计算机中，而正规远程控制软件是用户自己安装的。因此，若某些行业或部门被安装了木马，如国防、外交和商务部门，造成的损失是不可估量的。

从木马的技术进程来看，总共能够分为四代：

第一代木马主要是以窃取网络密码为主，在网络发展的早期就存在了，在通信和潜伏方面都没有突出地方。

第二代木马在技术上有了质的飞越，使用的架构是标准的 C/S 架构，提供的功能有：目标屏幕监视与拍摄，远程文件管理。但是种植的木马服务器端会打开配置好的默认端口等候客户端连接，很容易被检测出来。如：“冰河”、“Qmitis”。

第三代木马在网络连接方式上做了改动，采用了 ICMP 通信协议进行通信或者使用服务器端自主连接客户端的反向连接技术，这样能够突

破防火墙的拦截。其它功能上与上一代木马没有太大的差别。还有就是在数据传输技术方面也做了不小的改进，制作出了 ICMP 等类型的木马，通过畸形保温传输数据，增加了木马的查杀难度。如：网络神偷、Peep201等。

第四代木马在进程潜伏上采用了内核插入式的嵌入方式，利用远程注入线程技术，嵌入 DLL 线程，实现木马的潜伏。前几代的木马都是独立的木马，用户能够通过启动项的描述内容很快的查杀木马。但这第四代木马选择潜伏方向是注册表，伪装成 DLL 文件注入到正常的启动程序中，在“任务管理器”中是无法查看到正在运行的木马。对木马的查杀难度越来越大了。如：Beast木马。

第五代木马结合了病毒，利用计算机操作系统的漏洞，直接达到入侵植入的目标。例如噩梦 II。

2.2 木马的定义

木马是为了实现特殊目的而制作且植入到目标计算机中的一类程序，能够在你毫不知情的情况下拷贝传输文件或窃走您的密码。

通常完整的木马程序的组成是两部分：控制器程序和服务器端程序。所谓某个系统或计算机成了“肉鸡”，就是指自己计算机上被安装了木马服务器程序。若你的计算机被安装了木马服务器程序，则控制器程序的人就能够通过网络远程管控你的计算机实行盗取密码、上传下载各种文件、程序等。

木马算不上是一种病毒，因为它和病毒有质的区别：病毒以感染为目的，木马更注重于目的性，传播性最弱，跟病毒恰恰相反。病毒以无限不重复感染为主要的特性，而木马是以达到一定的目的性而定点传播。木马在早期主要任务是控制计算机。而现在转换成了了偷窃，主要是用户的私密信息。

2.3 木马的攻击模式剖析

客户端/服务器（Client/Server：简称 C/S）模式是木马的典型结构模式。其工作原理是：目标电脑上的木马服务器端被用户执行后，木马就会打开一个原先配置好的默认端口进行监听，当客户端向服务器端提出连接请求，服务器端就会自主运行相应程序来响应客户端的请求，客户端与服务器端建立连接后，当客户端发出各种指令时，服务器端在目标电脑上对这些指令一一执行，并把数据发送给客户端，以达到通过网络远程控制主机的目的。如图 2.1 所示：

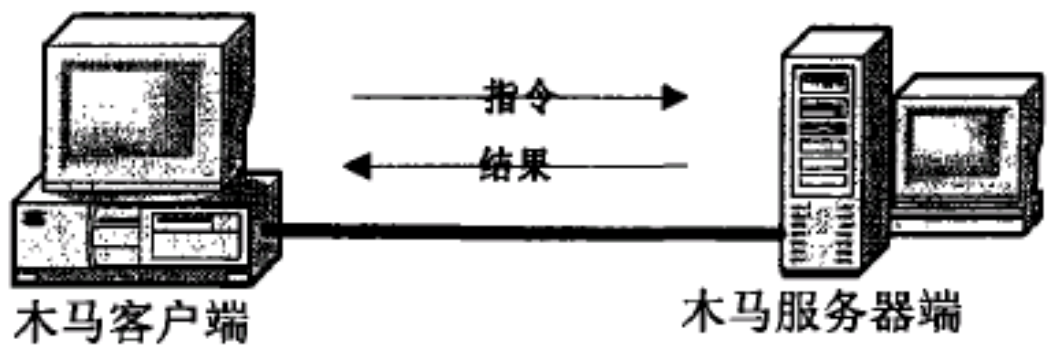

图 2.1 典型木马工作原理

由于这种连接方式易被检测，因此采取了 ICMP 来在端口连接时进行传送封包，让数据直接从木马客户端程序送达服务器端。如图 2-2 所示：

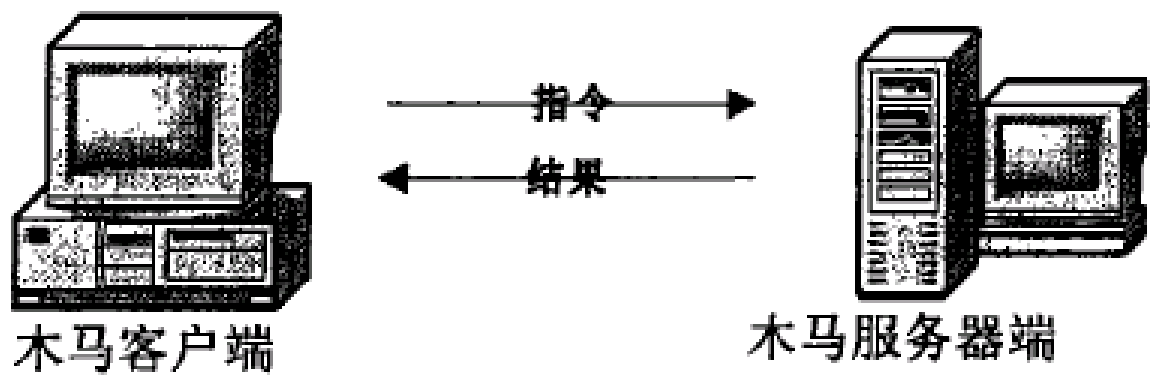

图 2.2 CIMP 传送封包

由于木马服务器端与客户端直接通信的容易被检测，因此采取了间接通信方式。在客户端与服务器端之间加一个中转层，服务器端程序先把数据发送到配置好的指定网站，客户端再从自己指定的网站取出数据。

这种方式让木马的潜伏通信提升了一个层度。如图 2.3所示：

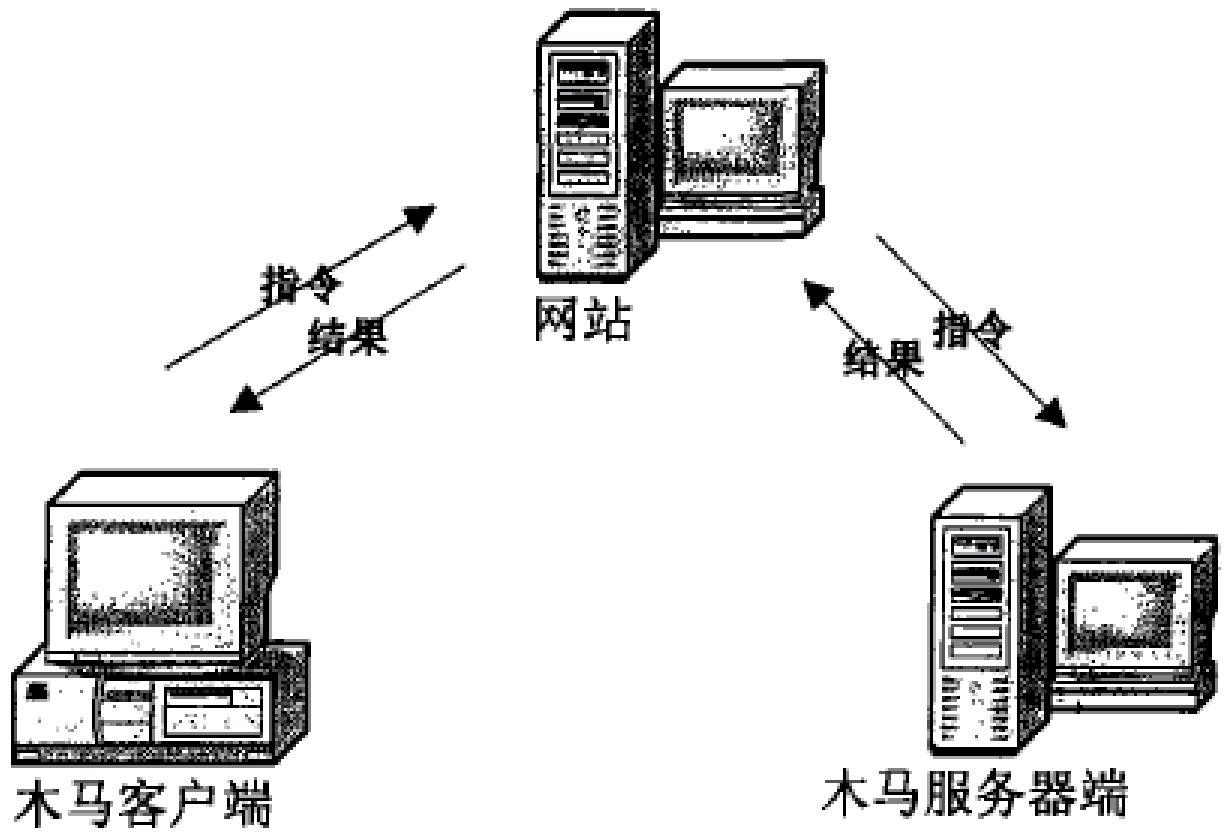

图 2.3 木马服务器端与客户端间接通信

2.4 木马的攻击特点剖析

随着网络技术的发展，木马也在不断演变，出现了各种各样的木马技术。但它们有着许多共同的特征，由于木马程序是受黑客操控，依照黑客的命令来运作，主要目的是偷取文件、机密数据、个人隐私等行为，所以木马的目的都是以窃取信息为主，并具备以下特点：

（1）木马的潜伏性：木马的首要特征是潜伏。只有能够在执行命令是而未被检测到存活下来，潜伏是最重要的，木马服务器端会使用各种手段把自己在目标电脑上潜伏起来，例如大家所熟悉的修改注册表和 ini 文件，便于下次系统启动时而自运行。一般情况下，通过“任务管理器”是查看不到木马的进程。还有的木马能够在配置服务器端时自定义端口，这样是木马潜伏得更深。木马还能够改动图标，使人误以为是个 Zip 压缩文件或图形文件，若用户一双击它则就变成了“肉鸡”。

（2）木马的非授权性：目标计算机被木马控制之后，那么客户端将

享有上传下载修改文件、记录用户键入的账号、密码、监控屏幕、控制目标鼠标、键盘、摄像头等操作权限，然后这些权限不是系统赋予的，而是木马自主窃取的。

（3）木马的欺骗性：木马经常借助目标系统中已有的文件来达到长期潜伏的目的，防止用户检测出来。木马程序通常仿制“dll\win\sys\explore”等字样中的数字为“1”与字母“l”、数字“0”与字母“O”来使人难以辨别的文件名和扩展名潜伏起来。

（4）木马的不可自我复制性：木马与病毒有很大的区别，病毒具备的特性是自我复制性和无限重复感染性，特洛伊木马反倒没具备这些特性，必须经过人工传播，但它的潜在破坏力和危害性却是不可估量的。

（5）木马的运行性：木马在植入目标主机时都会自主的修改系统配置文件或注册表的关联项，达到随计算机系统启动而启动的目的。

（6）木马的自动恢复性：现在的木马不再是如第一代或第二代那样由单一文件组成的独立功能模块，而是具备了多重备份，改动注册表的关联项，使其相互恢复。靠单独删除某个文件就能完全清除木马是不可能的了。

2.5 木马攻击能力剖析

木马能够自主的获取远程目标主机的最高操作权限，客户端能够通过网络对目标主机进行任意的操作，比如删除关闭某个服务程序，锁定注册表，获取用户机密信息，远程重新启动主机等，木马程序的危害是十分巨大的。不同类种的木马具备不同的攻击能力和攻击特征。

（1） FTP 型：FTP 文件传输协议，默认端口号是 21 号，在目标主机上往往会被打开来作为“后门”来响应，让任何有 FTP 客户端软件的用户可以不用密码的连接到此主机上随意上传和下载文件。

（2） 远程访问型：能够通过网络远程的访问目标主机的硬盘，进行摄像监视

（3） 键盘记录型：此类木马能够记录目标用户的敲键行为且能够在 log 文件里面查询密码。能够随着系统的启动而启动。

（4） 发送型：主要任务是窃取用户重要信息，如账号、密码等，并在用户没有察觉的情况下传至指定的信箱。

（5） 代理型：给目标计算机植入代理木马，让其变成一个跳板，对另一个目标进行攻击时，攻击者就能隐蔽自己的踪迹。

（6） 破坏型：这种木马很危险，计算机上的 EXE、INF、DLL 文件，它都可以自动的删除。感染上这类病毒对计算机的破坏巨大。

（7） 进程杀手型：主要为了防止监控软件的检测且关闭监控软件。

（8） 反弹端口型：进入目标计算机在连接时防火墙会进行严格过滤，而目标计算机连接外面时不严格，设计者利用这一特点，设计出了躲避防火墙的过滤的反弹端口型木马，把端口反弹，让防火墙把客户端和木马服务器端的连接误以为是正常的在浏览网页。

2.6 木马实施攻击的步骤剖析

不论是哪种木马，黑客利用它进行网络入侵时，都要经过以下五个流程：

（1） 配置木马：

通常情况下，一个设计成熟的木马都带有配置服务器端的程序，在这个阶段的主要目的是实现木马的伪装和信息反馈两个功能。

木马伪装：木马在配置服务器端功能时要使其尽最大可能的隐

蔽起来，会取用变换图标、多文件捆绑、自定义端口号、自我消除、改变木马名等多种伪装手段木马配置程序为了在服务端尽可能隐藏好木马，会采用多种伪装手段来深层潜伏。

信息反馈：在配置木马服务器端时设置信息反馈的指定地址或方式。如设置信息反馈的 E-Mail 地址、qq 号等。

（2） 传播木马：

因为木马程序不具备病毒的可传染性、自我复制等特性，所以需要通过人工进行传播。木马要尽最大可能的潜伏好，便于在网络中制造网络软件下载或者 E-mail 等多渠道传播。如：将修改图标（将 E-Mail 附件中可执行文件改为文本文件图标等）、与其它安装程序捆绑，当安装程序运行时木马也随之运行并加载等。

（3） 启动木马：

一般木马存放在系统目录：C：\windows\temp 或\system 或\system32 目录下、注册表、启动组、系统文件中，并打开客户端设置的默认端口，使其跟着系统或文件的启动而启动。

（4） 建立连接：

如果服务端与客户端都在线，那么通过定制的端口或通过扫描检测出开放的端口就可建立连接。

（5） 远程控制：

对服务器进行远程控制，如窃取 Cachme 的密码、记录击键动作、各种文件操作（对文件进行新建、删除、修改、上传、下载、运行、更改属性等操作）、修改注册表、系统操作（控制鼠标、键盘、监视桌面操作、查看进程、关闭系统、系统重启、断开网络连接等）。

2.7 木马伪装方法剖析

木马的主要能够衡量木马攻击能力的指标之一就是隐蔽能力。只有在宿主机子里面在攻击时能够不被发现的存活下来，木马才能够发挥出最大的攻击能力。木马攻击技术最重要的方面是研究它的隐蔽技术。宿主机子中，木马主要通过以下四种技术性隐藏：

启动式木马隐藏

注入进程服务式

反连接封包通信式

文件图标欺骗式

木马在宿主主机中想要尽可能的隐蔽，是离不开 Windows 系统中的各项服务体系的。为了剖析木马在 Windows 系统中的伪装技术，首先介绍木马能够在 Windows 中隐蔽所提供的一些服务。

进程(Process)和线程(Thread)

进程是在内存中运行的某一程序，是能够分配到 CPU 执行的实体，由进程内核对象和地址空间两部分组成。操作系统利用内核对象来管理各进程的信息块。地址空间存放着所有的 DLL 模块或 EXE 模块的数据与代码和各项内存空间。进程可拥有一个或多个线程，由线程负责执行进程地址空间中的代码[5]。应用程序运行时，会在内存内产生一个进程，这进程的运行空间是 Windows 系统分配的，此进程的任何操作都在这空间中进行。内存映射文件共享信息是多个进程间交流的主要方式。

线程是进程地址空间中代码的具体执行者，都有自己的 CPU 寄存器和堆栈，用于执行代码和保存数据[5]。进程所拥有的多个线程是相互独立的，能够同步的去完成自己的任务，有一定的独立性，若其中某个线程损坏了，整个进程不一定会崩溃。同一进程中的线程可以互相访问其堆栈。

服务（Service）

服务是 Windows 系统在后台处理各项重要事务的一种后台任务。服务不管是否需要登录，只要系统启动就随之运行，随着系统的关闭而停止。

在 Windows 2003 系统中，服务控制管理器，简称 SCM，是管理员和用户用来管理各种服务的一项工具。通过 SCM 能够对各项服务进行修改启动还是禁用的操作。

消息（Message）和 Hook（勾子）

Windows 是以消息驱动的操作系统，消息提供了应用程序之间以及应用程序与 Windows 系统之间进行通讯的手段，换言之，消息是 Windows 线程之间进行通信的一种手段[1]。

Windows 系统中存在系统消息队列，是系统对每一个正在执行的 Windows 应用程序所建立的“消息队列”，即应用程序队列，程序可能创建的各种窗口消息都存放在里面。有一段称做“消息循环”的代码含于应用程序中，主要用于从消息队列中检索这些消息，并把它们分配到对应的函数窗口中。等窗口函数处理完消息后，控制权又返回给 Windows。

Hook(勾子)是 Windows 系统中处理消息的一种机制。主要用途是可以把对于监视的窗口，当有消息发往这个目标窗口时拦截下来并进行处理，然后才发送给目标窗口。Hook 函数是需要通过系统调用来挂入系统的。

DLL（动态链接库）

动态链接库（Dynamic Link Library），简称 DLL，Windows 系统中的 API 函数都包含在 DLL 中。DLL 文件是不能独立于资源之外的，都是需要通过进程来加载并由线程来调用才发挥其作用。它的构成部件是多个功能函数的组合，没有程序的独立逻辑。DLL 文件在系统中是不可缺少的，

如:Kernel32.dll 包含着管理内存、进程、和线程的各大模块，user32.dll 包含着执行用户界面任务的各个模块，AdvAPI32.dll 包含着事件记录模块和注册表操作以及对象的安全性。

注册表

Windows 系统中最重要的是注册表。注册表在系统中起着核心的作用，里边包含着各种系统参数的配置以及各种文件关联项，是一个关系数据库。程序能通过注册表配置，使其随着 Windows 系统启动而运行的关联。

2.7.1 启动式木马隐藏技术

木马植入到目标主机后，就要想方设法去让自己能够随着宿主主机的启动而运行。这时木马就会采取一些欺骗的手段来欺骗用户执行木马程序，木马的启动式隐藏手段主要有如下两种：

注册表项隐藏启动

多个文件捆绑式或插入式隐藏启动

1. 注册表项隐藏启动

木马在宿主未发觉的情况下安装服务器端时，会利用注册表项的各种功能进行隐蔽启动，可以分为如下两类：

采取启动项隐藏启动

采取文件关联项隐藏启动

特注：在本文中有关注册表根全部使用的是缩写：

注册表项 HKEY_CURRENT_USER 的缩写代表：HKCU

注册表项 HKEY_LOCAL_MACHINE 的缩写代表：HKLM

注册表项 HKEY_USER 的缩写代表：HKU

注册表项 HKEY_CLASSES_ROOT 的缩写代表：HKCR

1.1 注册表启动项隐藏启动

随着 Windows 系统启动而运行的程序位于注册表启动项中。木马就是利用注册表中的启动项来进行隐藏启动，相关启动项有如下：

[HKLM\Software->Microsoft->Windows->CurrentVersion->Run]

[HKLM\Software->Microsoft->Windows->CurrentVersion->RunOnce]

[HKLM\Software->Microsoft->Windows->CurrentVersion->RunServices]

[HKLM\Software->Microsoft->Windows->CurrentVersion->RunServicesOnce]

[HKCU\Software->Microsoft->Windows->CurrentVersion->Run]

[HKCU\Software->Microsoft->Windows->CurrentVersion->RunOnce]

[HKCU\Software->Microsoft->Windows->CurrentVersion->RunServices]

[HKCU\Software->Microsoft->Windows->CurrentVersion->RunServicesOnce]

对于 DLL 类型的木马，还能够利用[HKLM\SYSTEM->ControlSet001->Control->SessionManager->KnownDLLs]此注册表项的 KnownDLLs 子键来进行启动。一些已知 dll 文件的默认路劲都存放在 KnownDLLs 子键下，DLL 木马在增加或修改了某个数值键后，就可以不带踪迹地在进程加载已知正常 DLL 的时候取代此 DLL 文件加载到相应进程[2]。

1.2 文件关联项隐藏启动

在注册表 HKEY_CLASSES_ROOT 和 HKLM\Software\CLASSES 目录下包含许多子文件夹，每一个子文件夹与每一文件类型一一对应，子文件夹中的各项用于建立文件类型和应用程序的关联。如果修改或删除文件夹中所包含的关联项则会改变应用程序与文件类型的关联。木马就是利用

这些目录下的子文件夹中的关联项进行自启动[3]。通常被木马程序修改用于建立木马与某类文件关联进行木马启动的项及键如下：

[HKCR\exefile->shell->open->command]@="%1" %*

[HKCR\comfile->shell->open->command]@="%1" %*"

[HKCR\batfile->shell->open->command]@="%1" %*

[HKCR\htafile->Shell->Open->Command]@="%1" %*

[HKCR\piffile->shell->open->command]@="%1" %*

[HKCR\cmdfile->shell->open->command]@="%1" %*

[HKCR\JSEFile->Shell->Edit->Command]@="%1" %*

[HKCR\JSEFile->Shell->Open->Command]@="%1" %*

[HKCR\JSEFile->Shell->Open2->Command]@="%1" %*

[HKCR\JSFile->Shell->Edit->Command]@="%1" %*

[HKCR\JSFile->Shell->Open->Command]@="%1" %*

[HKCR\JSFile->Shell->Open2->Command]@="%1" %*

[HKCR\VBEFile->Shell->Edit->Command]@="%1" %*

[HKCR\VBEFile->Shell->Open->Command]@="%1" %*

[HKCR\VBEFile->Shell->Open2->Command]@="%1" %*

[HKCR\VBSFile->Shell->Edit->Command]@="%1" %*

[HKCR\VBSFile->Shell->Open->Command]@="%1" %*

[HKCR\VBSFile->Shell->Open2->Command]@="%1" %*

[HKLM\Software->CLASSES->batfile->shell->open->command]@="%1" %*

[HKLM\Software->CLASSES->comfile->shell->open->command]@="%1" %*

[HKLM\Software->CLASSES->exefile->shell->open->command]@="%1"

%*

[HKLM\Software->CLASSES->htafile->Shell->Open->Command]@="%1"

%*

[HKLM\Software->CLASSES->piffile->shell->open->command]@="%1"

%*

这些"%1 %*"需要被赋值,如果将其改为"木马.exe %1 %*"，木马.exe 将在目标主机上用户每次打开 exe/pif/com/bat/hta 文件时被执行。

例如：对于注册表关联项

[HKCR\textfile->shell->open->command]@="%SystemRoot%\system32\notepad.exe %1"

[HKLM\Software->CLASSES->textfile->shell->open->command]@="%SystemRoot%\system32\notepad.exe %1"

如果将其改为"notepad.exe 木马.exe %1 "，木马程序将在每次打开文本文件时调用 notepad.exe 文件后被执行。

注：有的木马程序并不修改系统中已有的文件类型，而是创建一个新文件类型，并修改之进行关联启动。如冰河木马会在系统目录下增加 4 个全部为 259k 大小的冰河服务端程序的副本：lfp.dll、lfp.exe、system32.dll 和 tel.lfp，然后改写注册表，键值如下：

[HKLM\Software->Microsoft->Windows->CurrentVersion->Run]

C:\WINDOWS\SYSTEM\system32.dll

[HKLM\Software->Microsoft->Windows->CurrentVersion->RunServices]

C:\WINDOWS\SYSTEM\system32.dll

这是木马的主加载项，它还会再写入一个假的启动项，起迷惑的作用：

[HKCR\dllfile->shell->Open->Command]@="%1" %*

[HKCR\.lfp]@="lfpfile"

[HKCR\lfpfile]@=""

[HKCR\lfpfile->DefaultIcon]@="C:\\WINDOWS\\SYSTEM\\shell32.dll,-154"

[HKCR\lfpfile->shell->Open->Command]@="\"%1\"%*"

它将 DLL 文件和 LFP 文件的打开方式转化为直接执行，然后自己重新定义一个 lfp 的文件类型，加上图标。这样能在 Windows 系统每一次启动而先运行 System32.dll。之后 tel.lfp（即 Trojan）会跟注册表中子文件夹下的关联项建立关联（如 Bin、Dat、Vxd 等），若用户打开这类文件，则冰河木马被激活。有些能够进行“双启动”版本的冰河木马，其先把得到的信息传至木马，在传至目标 DLL，然后运行正常的 DLL 进行加载而成的。这样就能是木马的启动方式更加隐蔽，更加难于查杀。

2.多个文件捆绑式或插入式隐藏启动

2.1 在某一中类型的文件中插入一小段带有木马功能的程序，这也是木马隐藏启动方式的一种手段。

2001 年 6 月 8 日，美国网络安全权威专家发现有一个新型的木马程序插入到某电影剪辑中，用户只要用电脑观看此电影剪辑，则就会被植入木马，成为木马攻击的对象。

一般情况下木马都会利用 Windows 系统中 PE 格式的 EXE 文件作为主要载体来插入和启动。木马都是把自己隐藏在 PE 文件的个 SectionAlignment 块对齐时产生的空间中，然后修改位于 Section table 的 IMAGE_SECTION_HEADER 结构数组 Misc.VirtualSize、SizeOfRawData 成员和 IMAGE_NT_HEADERS 结构中的 SizeOfImage 成员实现加载启动的。

2.2 木马程序最常见的潜伏传播和隐蔽启动手段就是多个程序捆绑

捆绑程序也就是说把木马捆绑到正常的程序中隐蔽起来，在这些正常程序传播的痛也达到了木马传播的目的。只要这些程序一被打开，则木马程序原配随之安装启动。就如在浏览器上捆绑木马，目标开机时是不会检查到木马打开的默认端口的，在网络中打开了浏览器，木马随之启动发送数据，与客户端进行连接通信。木马常用的捆绑方法：使用 WinRar 软件进行捆绑配置。

捆绑方式都一样，在使用 WinRar 软件进行捆绑时，在配置的时候，将原程序作为做程序，也就是目标用户双击打开时的程序，而木马程序潜伏在其中也随之启动，在用户未察觉的情况下安装上了目标的主机，加载进注册表的启动项和修改关联项。通常情况下木马程序进行捆绑时会进行加密处理来对抗文件特征字符串扫描。

2.7.2 注入进程服务式的隐藏技术

木马植入宿主主机后，运行时必须要有自己的运行形式，不能够被宿主发觉并发现。这时利用注入进程服务式隐藏技术，因为线程在“任务管理器”中是查看不到的，所以利用此技术能达到隐藏运行的目的。首先在宿主主机上自动生成 DLL 文件，然后利用各种手段把此 DLL 文件注入到其它进程内运行。接下来木马程序都是以线程的形式在运行了，有些木马则是通过远程来在进程中创建一个新的线程，然后在线程里注入一段具有特殊功能的程序直接运行。木马在目标系统的运行空间中运行时，具体实现运行形式隐蔽的方法有以下几种：

1. 进程列表欺骗

木马采用进程列表欺骗的运行形式隐蔽时，会在系统中创建一个新的独立进程来运行。木马会监视宿主上来访问它窗口的消息，如果对其本身有害处，则就把此消息拦截下来进行修改，然后在返回发送给用户，达到一种欺骗检测软件，使用户查看不到木马进程的目的。通常查看进

程都是采用 Windows 系统提供的枚举函数来枚举进程。相关信息和方法如下：

利用 Windows 9X 系统所提供的 ToolHelp API 其中的 Process32 First 和 Process32 Next 函数枚举进程。

Windows NT 系统提供实现进程列表的两种方法：一是利用 Process Status 包含在 PSAPI.dll 中的函数 EnumProcesses，二是利用注册表函数访问 Performance Data 数据库(木马极少用此法)。

Windows 9X 系统 与 Windows NT 系统所提供的所有方法都归纳入 Windows 2K 中了，如：ToolHelp API 、Process Status 函数以及注册表函数访问 Performance Data 数据库。

Windows 提供的一种 API 拦截技术，即 Hook，它能够拦截通信双方的消息进行修改，在把修改的消息返回给发送方。木马就是利用这一项技术来拦截应用程序对 PSAPI、ToolHelp API 中与枚举进程相关的函数的调用，当木马进程的 PID 被检测到时就直接跳过，由此实现了木马进程的隐藏。

2.在系统中注册为服务实现运行形式隐藏

在 Windows 98 系统中，有一种未被微软公开的能将进程注册为服务进程的机制，因为此机制在 Windows 后续版本中未被提供，可是依然用计算机高手发现了这个方法，此方法采用了中 RegisterServiceProcess 技术。利用这技术能够把任何程序的进程注册为服务进程，这进程在 Windows 98 进程列表中是不会显示的，所以木马把自己注册成系统服务则能简易地实现运行形式的潜伏，但是此方法有很大的缺陷，就是利用其他第三方进程管理工具即可找到其所在，Windows 2000/XP 中采用此技术进行隐藏的都会显现出来，把该进程关闭后删除木马原文件就能搞定。

3.特洛伊 DLL

特洛伊 DLL 有时又称 DLL 陷阱技术[4]。特洛伊 DLL 是一种能把木马 DLL 替换掉系统内已知的 DLL，截获各进程对此 DLL 的所有函数调用，并进行分析。系统用户对此 DLL 正常调用时，木马 DLL 是无法处理的，必须使用函数转发器直接转发给被替换的系统 DLL。对调用的处理过程如图 3.1 所示：

图 3.1 特洛伊 DLL 调用的处理过程

特洛伊 DLL 在目标主机上的所有操作都会更加的隐蔽，但是技术实现有点难度，所以采用 DLL 形式类的木马很少。大多数的木马只采用 DLL 类型木马来进行监听，只要发现控制端的连接请求消息则激活自身，打开配置的默认端口进行对目标主机的操作，操作结束后又关闭潜伏起来。例如，已知 wsock32.dll 中存放着 Socket1.x 的 Windows 的 Socket1.x 的函数都是存放在 wsock32.dll 中的，攻击者用文件名 wsock32.dll 的特洛伊 DLL 木马替换掉原先的 wsock32.dll(将原先的 DLL 文件重命名为 wsockold.dll)。木马 wsock32.dll 只做两件事，一是如果遇到不认识的调用，就直接转发给 wsockold.dll（使用函数转发器 forward)；二是遇到特殊的请求（事先约定的）就解码并处理。理论上，攻击者把木马 wsock32.dll 植入目标系统后，通过 Socket 远程输入一定的暗号，就可