

# 11 木马与后门

周威

**`weizhou_sec@hust.edu.cn`**

# 本讲提纲

- **11.1 木马的基本概念**
- **11.2 木马的分类**
- **11.3 木马的植入方式**
- **11.4 木马的通信方式**
- **11.5 木马的主要功能及意图**
- **11.6 木马检测思路**
- **11.7 后门**

# 11.1 木马的基本概念

- **木马**：全称为特洛伊木马，来源于古希腊神话。

在古希腊传说中，希腊联军围困特洛伊久攻不下，于是**假装撤退**，留下一具巨大的中空木马，特洛伊守军不知是计，把木马运进城中作为**战利品**。夜深人静之际，木马腹中躲藏的希腊士兵**打开城门**，特洛伊沦陷。

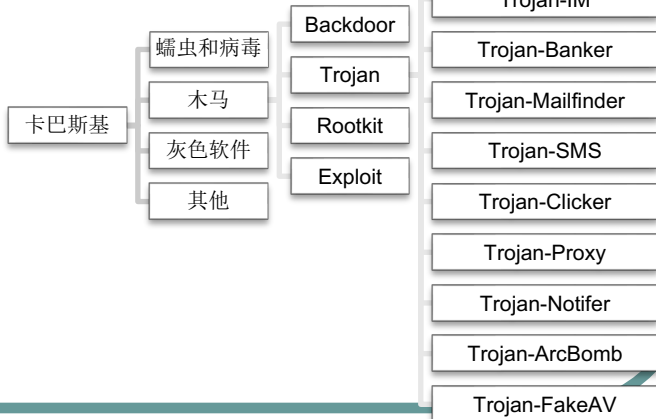
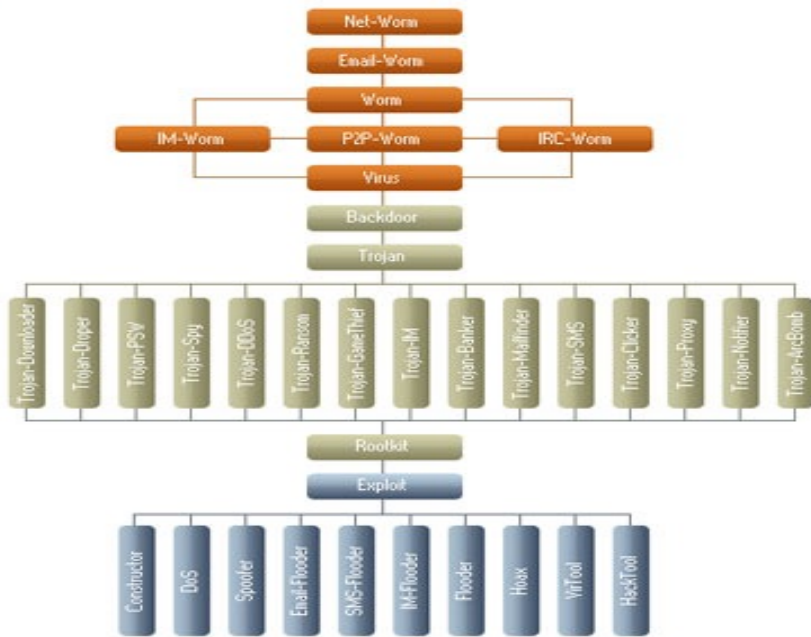


# 11.1 木马的基本概念

- 通过欺骗或诱骗的方式安装，并在用户的计算机中隐藏以实现控制用户计算机的目的。
  - 具有远程控制、信息窃取、破坏等功能的恶意代码；
  - Trojans are malicious programs that perform actions which are not authorized by the user: they delete, block, modify or copy data, and they disrupt the performance of computers or computer networks. Unlike viruses and worms, the threats that fall into this category are unable to make copies of themselves or self-replicate.
- 特点
  - 欺骗性、隐藏性、非授权性、交互性

# 11.2 木马的分类

- 不同的视角有不同的分类 <https://threats.kaspersky.com/en/class/Trojan/>
  - 行为视角（粒度细，如卡巴斯基**SafeStream**病毒库的分类标准）
  - 功能视角（**远程控制型**、信息获取型、破坏型等）



# 11.2 木马的分类

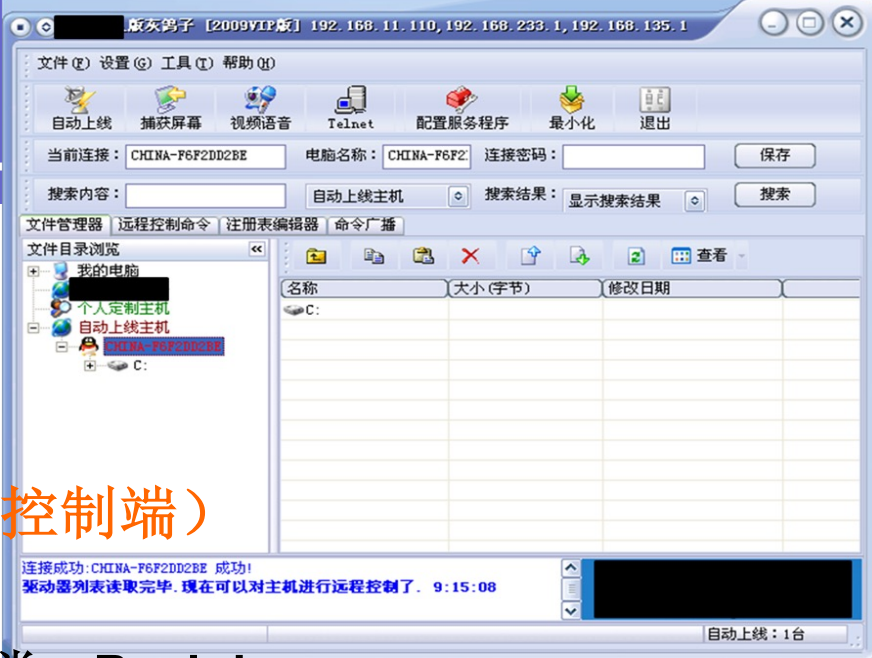
- 远程控制型木马

- 远程控制

- 交互性：双向（攻击者<->被控制端）

- 典型案例：

- 卡巴斯基分类标准下的木马子类：**Backdoor**
    - 冰河、网络神偷、广外女生、网络公牛、黑洞、上兴、彩虹桥、PCShare、灰鸽子等。



# 11.2 木马的分类

## ● 信息获取型木马

### ● 功能：信息获取

- 键盘输入，内存，文件数据等

### ● 交互性：单向交互（攻击者←被控制端）

- 发送至三方空间，文件服务器、指定邮箱等，或者直接开启FTP服务程序等。

### ● 典型案例：

- 卡巴斯基分类标准下的Trojan-Bank、Trojan-GameThief、Trojan-IM、Trojan-Spy、Trojan-PSW(Password Stealing Ware)、Trojan-Mailfinder等。



## 11.2 木马的分类

### ● 破坏型木马等

- 功能：对本地或远程主机系统进行数据破坏、资源消耗等。
- 交互性：单向（攻击者->被控制端），少数无交互
- 典型案例：
  - 卡巴斯基分类标准下的Trojan-DDoS、Trojan-Ransom、Trojan-ArcBomb、Trojan-Downloader、Trojan-Dropper等。



# 11.3 木马的植入方式

- 网页挂马植入

- 自动下载安装（MS06014,MS10002）

- 电子邮件植入

- 附件形式，打开附件被植入
- 电子邮件与恶意网页相结合，即使不打开附件，选中就会被植入

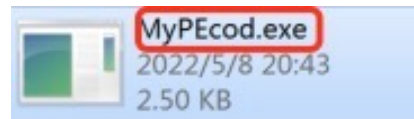
- 文档捆绑植入

- office文档、pdf文档漏洞等

# 11.3 木马的植入方式

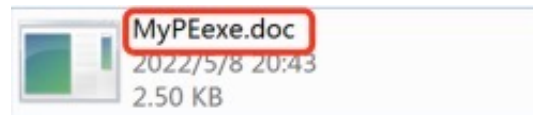
- 伪装欺骗植入

- 更改后缀名（Unicode翻转字符）、图标伪装



- 捆绑植入

- EXE捆绑、文档嵌入、多媒体文件、电子书植入



- 其他

- 特定U盘植入（故意丢弃、或者工作U盘、数据拷贝等）
- 社会工程



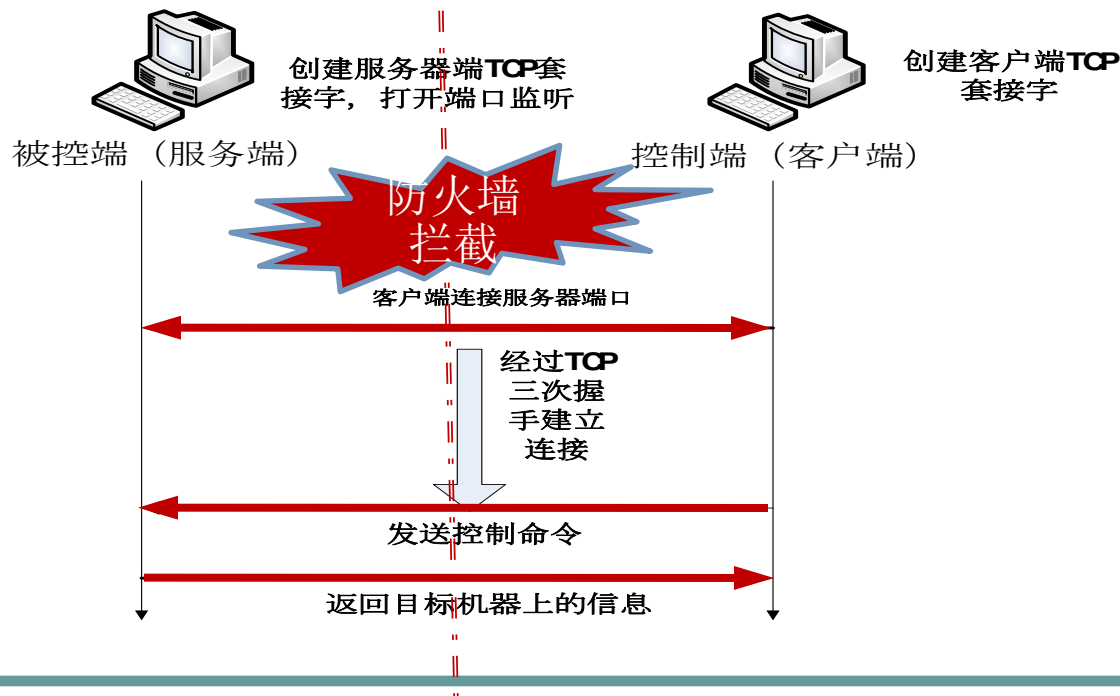
# 11.4 木马的通信方式

- 传输通道构建信息
  - IP地址、端口等信息、第三方网站地址
- 建立通信连接的方式
  - 正向连接
  - 反向连接

# 11.4.1 正向连接

## ● 正向连接

控制端  
主动连接  
被控端



# 正向连接的优缺点

- 优点：

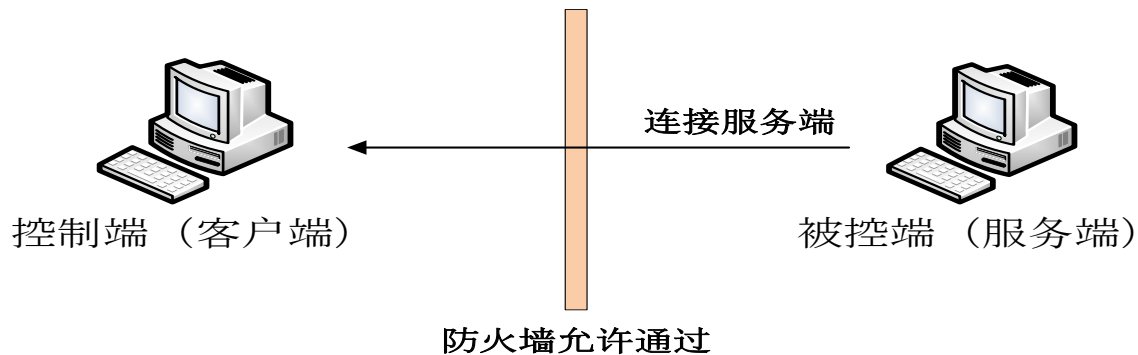
- 攻击者无需公网（外部）**IP**地址
- 木马样本不会泄露攻击者**IP**地址

- 缺点

- 可能被防火墙阻挡
- 被攻击者必须具备公网（外部）**IP**地址
- 定位被攻击者相对困难
  - 被攻击者**IP**是否变化？
  - 目标主机何时上线？

## 12.4.2 反向连接—1

### ● 反向连接1



# 反向连接1的优缺点

- 优点：

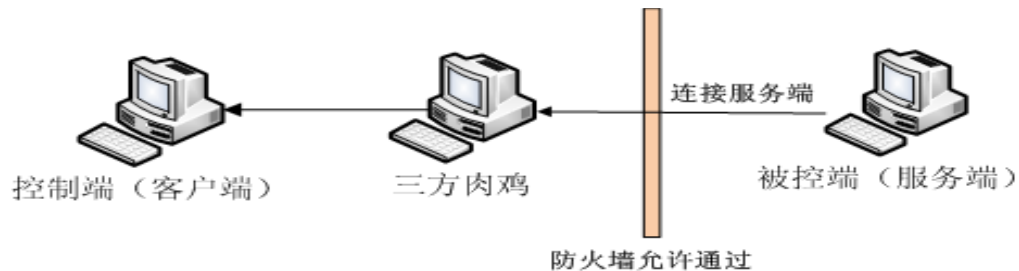
- 通过防火墙相对容易
- 攻击目标随时上线、随时控制
- 可以控制局域网内的（内网）目标

- 缺点：

- 样本会暴露控制服务器信息（域名或IP）
- 攻击者通常应当具有外部IP

## 11.4.2 反向连接一2

### ● 反向连接2



- 被控端和控制端都和第三方通信

- 肉鸡、Web服务器



# 反向连接2的优缺点

- 优点
  - 可绕过防火墙，自动连接上线，不易被发现（代理）
- 缺点
  - 肉鸡的稳定性需要保障

## 11.4.3通信协议

- **TCP协议**

- 稳定、易被发现
- **HTTP协议伪装**

- **UDP协议**

- 和**TCP**一样也有正向、反向两种方式
- 负载比**TCP**少，但是可靠性低

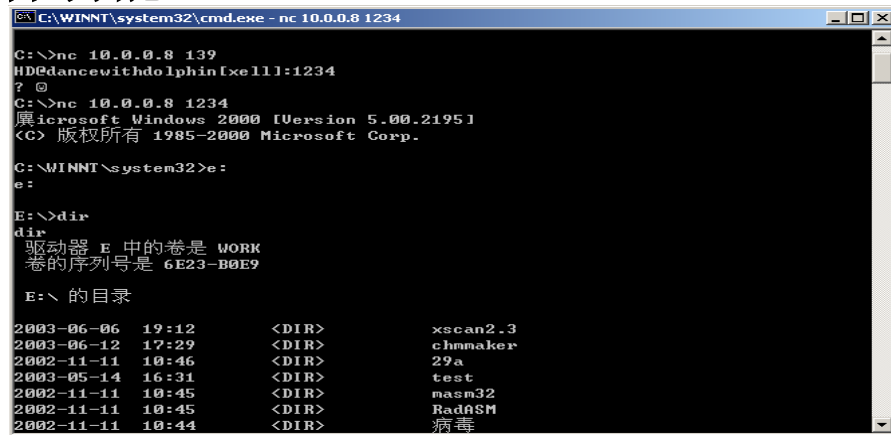
## ● **ICMP+TCP / UDP**

- 监听**ICMP**报文，以感知木马数据
  - **ICMP**报文是由系统内核或进程直接处理而不是通过端口
  - 一般不会被防火墙过滤

# 难以觉察的远程木马- BITS

## --Background Intelligent Transfer Service

- 该程序具有如下特点：
  - 进程管理器中看不到
  - 平时没有端口，只是在系统中充当卧底的角色
  - 提供正向连接和反向连接两种功能



```
C:\WINNT\system32\cmd.exe - nc 10.0.0.8 1234
C:\>nc 10.0.0.8 139
HDEdancewithdolpin[xe11]:1234
? @
C:\>nc 10.0.0.8 1234
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

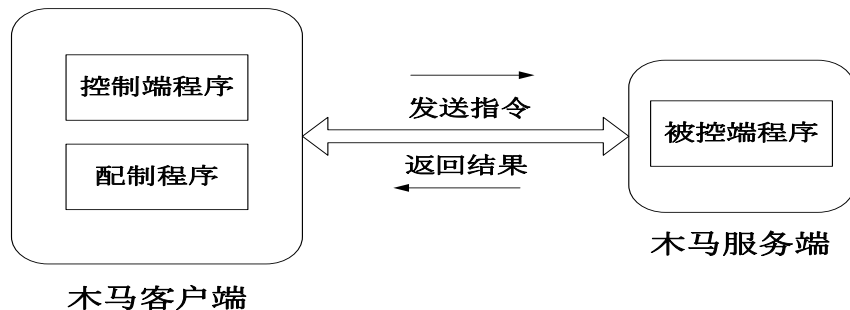
C:\WINNT\system32>e:
e:
E:\>dir
dir
驱动器 E 中的卷是 WORK
卷的序列号是 6E23-B0E9

E:\ 的目录
2003-06-06  19:12    <DIR>          xscan2.3
2003-06-12  17:29    <DIR>          chmmaker
2002-11-11   10:46    <DIR>          29a
2003-05-14   16:31    <DIR>          test
2002-11-11   10:45    <DIR>          masm32
2002-11-11   10:45    <DIR>          RadASM
2002-11-11   10:44    <DIR>          病毒
```

# 11.5 远控木马的常见功能与意图

## ● 1. 木马结构

- 完整的木马一般由**木马配置程序**、**控制端程序**（客户端）和**被控制端程序**（服务端程序）等三部分组成。



# PCShare

PCShare 客户管理-127.0.0.1:1026

上层目录 刷新

屏幕控制 目录浏览 进程列表 窗口列表 服务管理 注册表编辑 键盘记录

我的电脑

名称	类型	大小	可用空间
A:	软驱	0 MB	0 MB
C:	本地磁盘	4994 MB	518 MB
D:	本地磁盘	10234 MB	5082 MB
E:	本地磁盘	7985 MB	324 MB
F:	本地磁盘	7985 MB	1833 MB
G:	本地磁盘	7601 MB	552 MB
H:	本地磁盘	35996 MB	1353 MB
I:	本地磁盘	34992 MB	3802 MB
J:	本地磁盘	35980 MB	378 MB

搜索结果

就绪

共有9个对象

PcShare-主控界面: 192.196.0.1

文件(F) 命令(C) 操作(W) 帮助(H)

管理客户 删除客户 超级终端 参数设置 生成客户

已连接的客户...	客户注释
127.0.0.1:1026	我的电脑

客户属性名称	
客户计算机名称	
客户操作系统	
客户连接IP地址	
客户登录时间	15:09:33
客户连接时长	00:03:08
客户CPU主频	~730 Mhz
客户CPU数量	1 个
物理内存容量	261424 KB
客户内部标识	8888888888888888
当前用户名称	Administrator
当前用户密码	找了, 没找着!
客户注释	我的电脑

发生时间	事件内容
2003年10月30日 15时09分28秒	正在装载控制客户端文件资源
2003年10月30日 15时09分28秒	控制客户端文件资源: 文件大小【65536】版本
2003年10月30日 15时09分28秒	正在获取本机IP地址
2003年10月30日 15时09分28秒	IP地址: 【192.196.0.1】
2003年10月30日 15时09分28秒	正在打开侦听端口
2003年10月30日 15时09分31秒	开始侦听本地端口【33333】
2003年10月30日 15时09分31秒	开始等待客户连接

就绪

当前连接客户1个

文件(F) 设置(G) 工具(T) 帮助(H)



当前连接: 电脑名称: 连接密码:

搜索内容: 自动上线主机 搜索结果: 显示搜索结果

文件管理器 远程控制命令 注册表编辑器 命令广播

灰鸽子远程控制 2 0 0 9 测试版192.168.233.100

文件(F) 设置(G) 工具(T) 帮助(H)



当前连接: TOMPANPAN 电脑名称: TOMPANPAN 连接密码: 保存

搜索内容: 自动上线主机 搜索结果: 显示搜索结果 搜索

文件管理器 远程控制命令 注册表编辑器 命令广播

文件目录浏览

名称	大小(字节)	修改日期
obj		2007-10-10 09:33
objchk		2007-10-10 09:33
buildchk.log	1794	2007-10-10 09:33
MAKEFILE	269	2007-09-29 22:21
notes.txt	213	2007-09-29 22:21
rookit.c	8791	2007-08-20 14:59
Sources	104	2007-09-29 22:21
SysMon.c	42492	2007-10-05 10:33
SysMon.c.bak	42502	2007-09-30 17:01
SysMon.h	19192	2007-09-30 16:39
SysMon.h.bak	18305	2007-09-30 13:38

读取文件列表命令发送成功!  
文件列表读取完毕. 12:39:50

12个对象 当前路径: C:\drv-10-05\

自动上线: 1台 23

自动上线设置 安装选项 启动项设置 代理服务 高级选项 插件功能

IP通知http访问地址、DNS解析域名或固定IP:

192.168.233.100 说明

上线图像: 课程测试

上线分组: 学生甲

上线备注: 123456

连接密码: 说明

## 12.5 远控木马的常见功能与意图

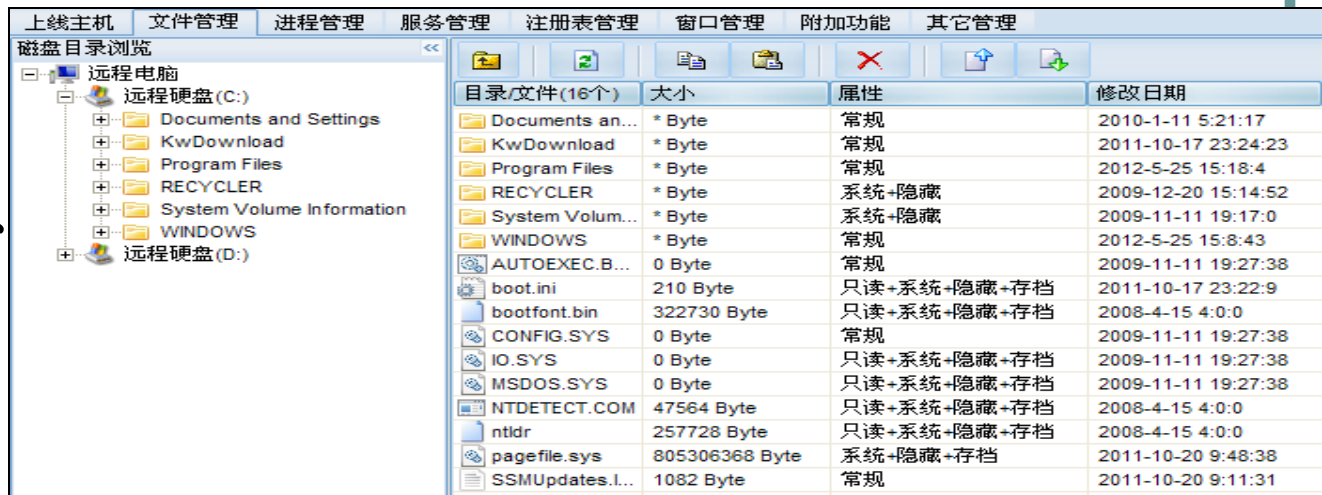
### ● 2.典型功能

- 文件管理
- 进程管理
- 服务管理
- 注册表管理
- 屏幕监控、屏幕截取
- 语音视频截获
- 键盘记录
- 窗口管理
- 远程**Shell**等



# 文件管理

- 获取目标的文件系统信息，通常包括如下功能：
  - 浏览各磁盘文件
  - 上传、下载文件
  - 执行文件
  - 删除文件
  - 修改文件信息
  - （如时间）



# 进程管理

- 查看、结束或者暂停目标系统进程

- 作用:

- 查看目标系统的环境信息

- 安装了哪些软件? 目前对方正在做什么?

- 停止或暂停目标系统的相关程序

- 如反病毒程序

上线主机	文件管理	进程管理	服务管理	注册表管理	窗口管理	附加功能	其它管理
进程名(共 28 个)	PID	PID(父)	线程数	优先级	创建时间	文件路径	
[System Proc...	0	0	1	暂缺		[System Process]	
System	4	0	54	标准	1601-1-1 8:0:0	System	
smss.exe	572	4	3	极高	2011-10-20 9:48:33	\\SystemRoot\\System32\\smss.exe	
csrss.exe	620	572	12	极高	2011-10-20 9:48:42	\\?C:\\WINDOWS\\system32\\csrss...	
winlogon.exe	644	572	19	极高	2011-10-20 9:48:48	\\?C:\\WINDOWS\\system32\\winlo...	
services.exe	688	644	16	高	2011-10-20 9:48:57	C:\\WINDOWS\\system32\\services...	
lsass.exe	700	644	16	高	2011-10-20 9:48:58	C:\\WINDOWS\\system32\\lsass.exe	
vmacthlp.exe	860	688	1	标准	2011-10-20 9:49:2	C:\\Program Files\\VMware\\VMwar...	
svchost.exe	900	688	16	标准	2011-10-20 9:49:4	C:\\WINDOWS\\system32\\svchost....	
svchost.exe	980	688	11	标准	2011-10-20 9:49:6	C:\\WINDOWS\\system32\\svchost....	
SbieSvc.exe	1076	688	7	标准	2011-10-20 9:49:8	C:\\Program Files\\Sandboxie\\SbieS...	
svchost.exe	1088	688	45	标准	2011-10-20 9:49:8	C:\\WINDOWS\\System32\\svchost....	
svchost.exe	1220	688	5	标准	2011-10-20 9:49:9	C:\\WINDOWS\\system32\\svchost....	
svchost.exe	1320	688	11	标准	2011-10-20 9:49:9	C:\\WINDOWS\\system32\\svchost....	
spoolsv.exe	1408	688	11	标准	2011-10-20 9:49:13	C:\\WINDOWS\\system32\\spoolsv.e...	
sysssafe.exe	1596	644	9	标准		sysssafe.exe	
explorer.exe	1656	1608	16	标准	2011-10-20 9:49:20	C:\\WINDOWS\\Explorer.EXE	
VMwareTray....	2044	1656	1	标准	2011-10-20 9:49:29	C:\\Program Files\\VMware\\VMwar...	
VMwareUser....	128	1656	7	标准	2011-10-20 9:49:29	C:\\Program Files\\VMware\\VMwar...	
VStart.exe	136	1656	9	标准	2011-10-20 9:49:29	D:\\tools\\VStart50\\VStart.exe	
ctfmon.exe	172	1656	1	标准	2011-10-20 9:49:30	C:\\WINDOWS\\system32\\ctfmon.exe	
SbieCtrl.exe	180	1656	3	标准	2011-10-20 9:49:30	C:\\Program Files\\Sandboxie\\SbieC...	

# 服务管理

## ● 查看并管理目标系统的服务

- 创建服务
- 启动/停止服务
- 删除服务

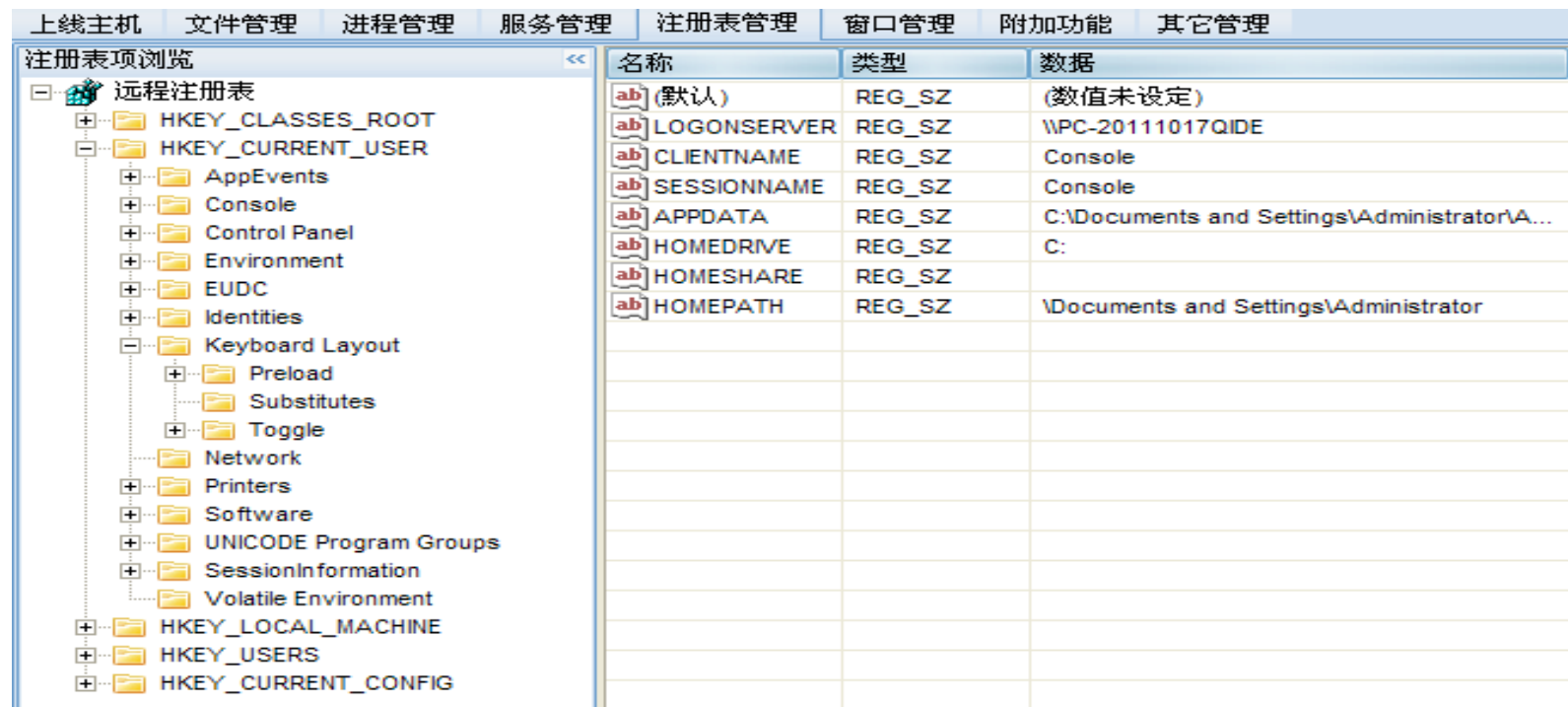
PcShare远程控制服务管理-169.254.246.55:13060

名称	描述	状态	启动类别	登录身份
Alertter	通知所选用户和计算机有关系统管理级警报...	已停止	已禁用	NT AUTHORITY\LOCAL SYSTEM
Application Layer Gateway Service	为 Internet 连接共享和 Windows 防火墙提...	已运行	手动	NT AUTHORITY\LOCAL SYSTEM
Application Management	提供软件安装服务, 诸如分派, 发行以及删除...	已停止	手动	LocalSystem
Windows Audio	管理基于 Windows 的程序的音频设备。如果...	已运行	自动	LocalSystem
Background Intelligent Transfer Service	在后台传输客户端和服务端之间的数据。如...	已运行	自动	LocalSystem
Computer Browser	维护网络上计算机的更新列表, 并将列表提...	已停止	手动	LocalSystem
ClipBook	启用“剪贴簿查看器”储存信息并与远程计...	已停止	已禁用	LocalSystem
COM+ System Application	管理 基于 COM+ 组件的配置和跟踪。如果服...	已停止	手动	LocalSystem
Cryptographic Services	提供三种管理服务: 编录数据库服务, 它确...	已运行	自动	LocalSystem
DCOM Server Process Launcher	为 DCOM 服务提供加载功能。	已运行	自动	LocalSystem
DHCP Client	通过注册和更改 IP 地址以及 DNS 名称来管...	已运行	自动	LocalSystem
Logical Disk Manager Administrative Service	配置硬盘驱动器和卷。此服务只为配置处理...	已停止	手动	LocalSystem
Logical Disk Manager	监测和监视新硬盘驱动器并向逻辑磁盘管理...	已运行	自动	LocalSystem
DNS Client	为此计算机解析和缓冲域名系统 (DNS) 名称...	已运行	自动	NT AUTHORITY\LOCAL SYSTEM

## ● 作用:

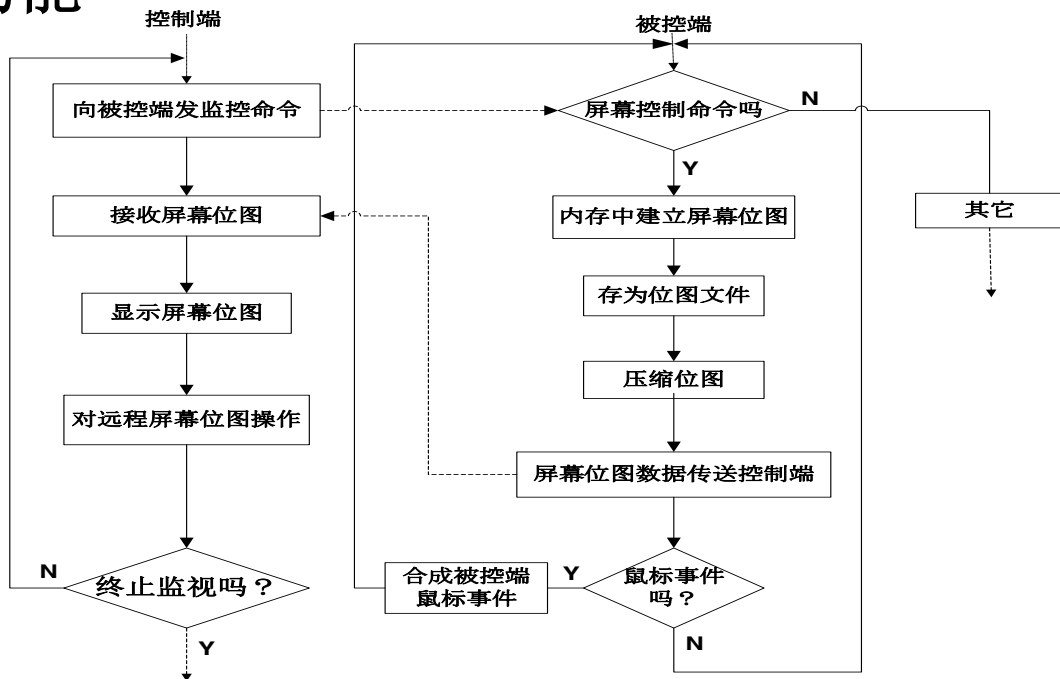
- 查看目标系统的环境信息
  - 安装了哪些软件? 启动了哪些服务?
- 停止或暂停目标系统的相关程序
  - 如反病毒程序

# 注册表管理



# 屏幕控制

## ● 木马屏幕监视功能





# 屏幕截取

- 抓取屏幕
  - 单张
  - 多张连续
- 作用：
  - 了解目标主机的当前操作情况

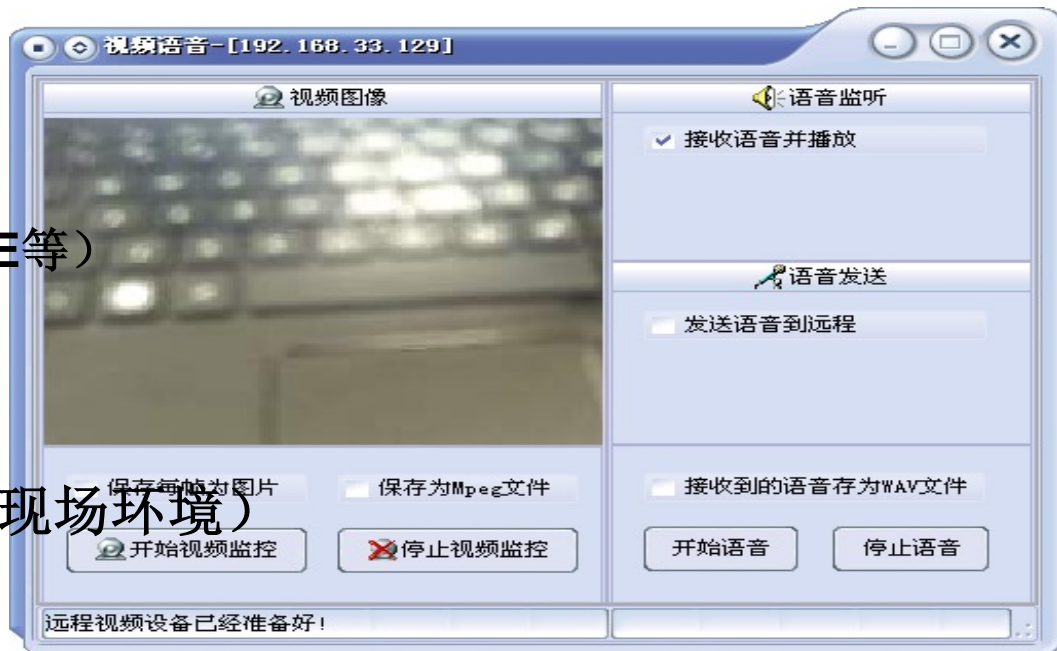
# 语音视频截获

## ● 录音

- 窃取对方谈话信息
- 窃取对方对外语音通话
  - （如**QQ**、微信、**SKYPE**等）

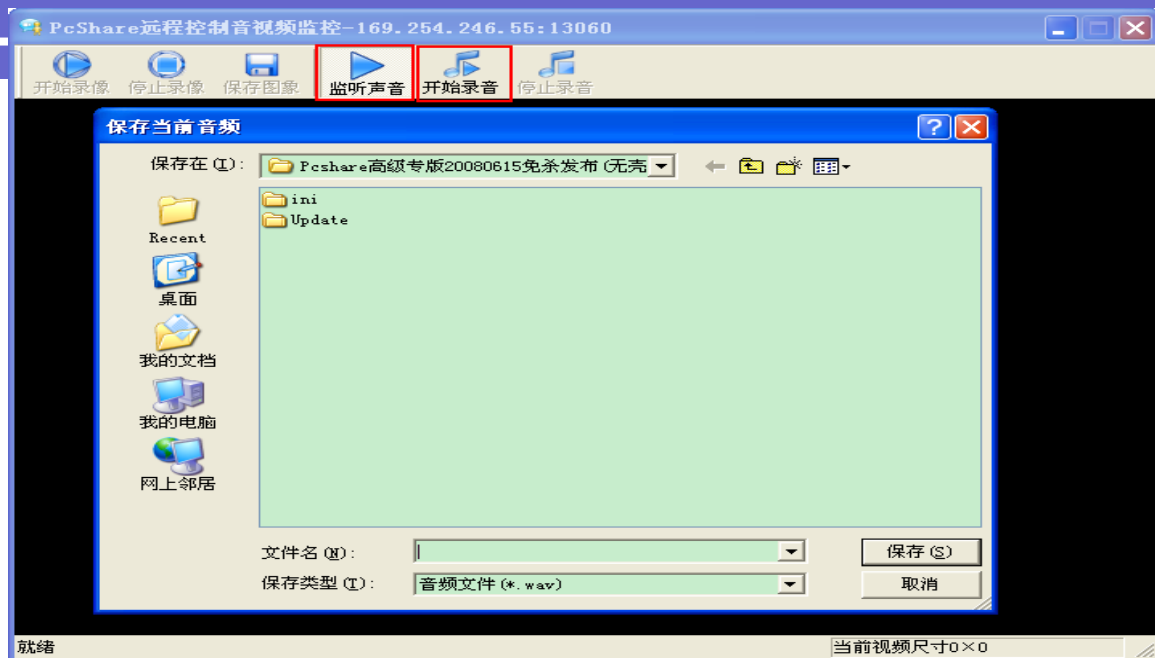
## ● 摄像头

- 打开摄像头（了解对方现场环境）
- 摄像录制（敲诈...）





# 语音监听



# 键盘记录

- 获取目标电脑中的键盘击键信息
  - 用户名、密码信息
    - QQ、邮箱、网银、网上证券、网络游戏、支付宝...
  - 聊天信息
    - 部分木马支持中文汉字记录

# 窗口管理

- 查看目标主机目前开启了哪些窗口
  - 了解目标用户正在做什么？

# 远程Shell

- 交互式或非交互式**Shell**
  - 远程交互的**Cmd.exe**
  - 直接执行命令或第三方程序

# 部分木马功能

木马名称 木马功能	PcShare 2011	大白鲨 2010	大白鲨 2011	华中帝国 2011V13	华中帝国 2011 V28	灰鸽子 2011	黑洞 V1.98
自启动	✓	✓	✓	✓	✓	✓	✓
文件管理	✓	✓	✓	✓	✓	✓	✓
进程管理	✓	✓	✓	✓	✓	×	×
服务管理	✓	✓	✓	✓	✓	×	×
注册表管理	✓	✓	✓	✓	✓	✓	✓
屏幕监控	✓	✓	✓	✓	✓	✓	✓
键盘监控	✓	×	×	✓	✓	×	×
视频监控	×	✓	✓	×	✓	✓	✓
音频监控	✓	×	×	✓	✓	✓	✓

# 木马的关键

- 功能适当 [精简灵活]
- 适用性强 [功能、权限]
- 高效、稳定、隐蔽 [传输]
- 可穿透性
- 自更新、自销毁
- 防追踪、反制对抗
- 持续免杀性能等
  - 特征值、通用主机行为、异常的通信流量...

# 11.6 木马检测思路

- 如何对木马进行检测？
  - 静态文件特征
  - 网络流量特征
  - 系统行为特征
  - 功能行为特征
  - 攻击意图等

# 11.7 后门

- 一种被插入到软件或系统中的隐藏通道，使得攻击者可以对系统进行**非授权访问**的一类程序。
  - 如**Bits**、**WinEggDrop**、**Tini...**
- 特点：
  - 隐蔽性
  - 持续性
  - 主动安装
  - 特殊权限



图：Sunburst数字签名



# 思考题

- 远程控制的木马分为控制端和被控制端又称为客户端和服务端，为什么是这样的对应关系？
- 网络木马的连接方式有几种？ 有哪些优缺点？
- 后门程序和远程控制的木马的区别？
- 木马的文件和资源管理等系统行为和正常的资源管理器的区别是什么？
- 如何对木马提出通用的检测方法，能对未知木马进行检测？