网络安全

安全技巧（二）

狄登峰 主编

目　　录

清除黑客程序

网上的黑客不多，使用黑客程序的不少，不少网友深受黑客程序之害,在这里，我抛砖引玉介绍一些清除黑客程序的简单方法，希望能给大家一些帮助。

1.冰河

冰河是国人自行开发的一种木马程序，中了冰河木马的机器将轻而易举地被远程机器所控制，就像使用自己的机器一样方便进行各种操作。

清除方法一：

如果安装了“冰河”客户端程序，就很简单了。运行客户端程序，在自动扫描中输入自己的IP，看一下扫描结果是否为“OK”，并且左边的“文件管理器”中是否会出现自己的IP。如果有，在“命令控制台”中的“控制类命令”中的“系统控制”中点击“自动卸载冰河”就可以了。

清除方法二：

如果没有“冰河”这个软件，也不用着急，可以用清理注册表的办法的方法查找并解除冰河木马。

运行REGEDIT命令打开注册表编辑器，在KEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run中查看键值中有没有自己不熟悉的自动启动文件，扩展名为EXE。（一般“冰河”的默认文件名为KERNEL32.EXE，注意此文件的名字可能会被种马的人改变）。

如果有，那我们先删除该键值中这一项，再删除

RUNDRIVES 这个键值。一般“冰河”用户端程序的自我保护设为：关联 TXT 文件或 EXE 文件，关联的文件为：SYSEXPLR.EXE。

A.在“查看”菜单中选择“文件夹选项”弹出文件夹选项对话框，选择“文件类型”在“已注册文件类型”框中找到“TXTFILE”这一项，看一下“打开方式”有无变化（一般为：NOTEPAD），如果关联对象不是 NOTEPAD，选择“编辑”按钮，在“操作”框中删除“OPEN”这一项，那关联 TXT 文件的用户程序就失效了。

B.如果是关联的 EXE 文件，那打开注册表编辑器，在 HKEY_CLASSES_ROOT\.exe 中把“默认”的键值随便改成什么（注意看清楚，等会儿要改回来）。

以上这两步做完后，退出 WINDOWS，在 DOS 状态下删除该“冰河”用户端程序，重新启动即可。

注意：要把 EXE 文件的注册表改回来。

附：建议采用第一种办法：）方便简单，如果采用第二种办法，而你对注册表不是太熟悉的话，请一定先备份注册表文件。

2.BackOrifice(BO)

BO 可能是全球影响最大的一种黑客程序了，想必大家都有所耳闻，我就不口罗嗦了。

清除方法：

用清理注册表的办法。运行 REGEDIT 命令，打开注册表编辑器，在 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices 看右边是否有某个 ab 项出现（默认）“.exe”，如果有立即删除这个 ab 项，并确认

删除后原来“.exe”的地方变为(未设置键值)。接着点击开始菜单的“关闭系统”，选择“重新启动计算机并切换到 MS－DOS 方式”。退出后，输入 cdc:\windows\system 回车，输入 delexe～1 回车，输入 delwindll.dll 回车,返回 Windows。

3.Netspy

Netspy 由国内黑客编制，全中文界面，功能较弱，但使用简单，所以在国内危害很大。

清除方法：

还是使用清理注册表的办法。运行 REGEDIT 命令，打开注册表编辑器，在 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 看右边是否有两个 ab 项分别出现 NETSPY 和 SPYNOTIFY,如果有,立即删除这两个 ab 项。用同上的方法退出到 MS－DOS 方式，输入 cdc:\windows\system 回车，输入 delnetspy.exe 回车，输入 delspynot～1.exe 回车，返回 Windows。解决黑客程序的方法还有使用杀毒软件，使用杀毒软件的另一个好处在于可以查找出硬盘中感染黑客程序的文件。以防因再次运行该文件而再次中黑客程序。

此外，还有一点需要说明一下，现在市面上最新版的杀毒软件一般都可以查出一些流行的常见的黑客程序，你可以通过运行杀毒软件的办法检测并清除黑客程序。但是这些黑客程序往往变种极多，所以有时候还是得自己多留意，注意升级你的杀毒软件。

(泥巴)}

《清除黑客程序（续）》

介绍过清除冰河、BO、Netspy 三种黑客程序的方法，

今天再对它进行补充，希望对大家有所帮助，让自己的系统的安全性能得到进一步的保护。

1.Netbus

中了 Netbus 的计算机会有如下特征：1 会在 C:\windows 下生成一个小小的、背景为深蓝色的锅状卫星天线的图标；2 也会在 C:\windows\system 下生成一个中心淡蓝色的锅状卫星天线的图标，名为“查看频道.scf”，这只能够在 Win98 中看到。如果你在此目录下看到上述的两个图标中的其中一个，可以先用鼠标右键点击此图标文件，选择“属性”，看看它的大小是否显示为“461KB”或者是“483KB”，如果是其中的一种，就点击“开始”→“运行”，输入“regedit”，打开注册表编辑器，选 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run，看看里面的 ab 项，与你先前发现的那种图标的文件名是相同的，如果有，看看此 ab 项右边是不是出现“C:\windows\图标的名字.exe／nomsg”，是就删除这个 ab 项，退出到 MS－DOS 方式，进入 windows 子目录，找到图标文件后删除它，然后返回到 Windows。

2.Subseven

谈到木马，大家可能第一个映入脑海的就是 BO，其实还有一个木马的功能不下于 BO 的，可能还有过之而无不及，那就是 Subseven。

它是由 subseven.exe、editsubserver.exe、server.exe 和 icqapi.dll 四个文件组成的，各自分别是客户端程序、设置木马的编辑器、服务器程序。如果它在你的机子里面安家落户，你要发现它，不容易，因为它会隐藏自己

的进程，但是你可以在 C:\Windows\目录下发现一个名为 mcrexe.exe 的文件，如果你打开注册表编辑器，检查 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run，会有一个名为 mcrexe.exe 的子键，删除它们吧！

3.Happy99

这是一种病毒，它附着于 E－mail 附件上，如果你不知道它是病毒而去执行它，你会发现你的屏幕上自动打开了一个名为“Happynewyear1999”的窗口，里面是以黑色为底色的满天焰火，此后只要你发送附带附件的邮件，机子就会死机。

其实，该程序把自身 copy 到 Win95／98 的 System 目录下，命名为 Ska.exe，释放出文件 Ska.dll，并会修改 Wsock32.dll，把修改前的文件备份为 Wsock32.ska，并修改了注册表，所以当你打开 C:\Windows\System，发现其中有 Ska.exe、ska.dll 和 wsock32.ska 三个文件，你就知道你已经中毒了。这时别慌张，照旧打开注册表编辑器，检查 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce 中有无键值 Ska.exe，如果有，请将它删除，然后再删除 C:\Windows\System 中 Ska.exe 和 Ska.dll 两个文件，再将 Wsock32.ska 重新命名为 Wsock32.dll 就行了。

发送匿名电子邮件

为了网络安全有时需要发送匿名邮件,方法如下:

一、初级方法

使用普通的邮件程序或一般 WEB 信箱，只要在发件人一栏填上一个假地址或一个错误的地址就行，或者干脆让发件人一栏空着。但是此时发送的邮件不能做到真正匿名，因为收件人可以从邮件头上看出你上网时的 IP 地址、信件发送过程中所使用过的邮件服务器和发送接收时间等，如果他稍微深究一下，是能够让你“水落石出”的，因而这算不上真正的匿名邮件。

二、利用 WEB 页面发送

可以登录到提供免费发送匿名电子邮件服务的 WEB 页面发送匿名电子邮件,目前笔者就找到三个这样的网址：

(1）匿名邮件 http://home.dqt.com.cn/～xiaodao/mfzy/nmyj.htm；

(2）免费匿名电子邮件 http://kahn.xj.cninfo.net/xinhai/service/fcd55.htm；

(3）Anonymizer 匿名邮件发送，http://personal.sd.cninfo.net/～jgq/free/qita.html。

发送方法非常简单：只要将对方信箱（To:）、主题（Subject:）、正文等分别填入相应的框中，再按“匿名发送”即可。

三、利用匿名邮件服务器发送

如果你嫌登录 WEB 页面既浪费时间，又浪费金钱，还可以利用有些 Internet 服务机构提供的匿名邮件转发服务来发送，比如：remailer@replay.com，mixmaster@remail.obscura.com.cn 等。其方法是：

使用普通邮件程序(比如 OE 或 Foxmail 等)，在收件人一栏填入匿名邮件服务器的地址（不能填入真正收件

人的地址），主题书写无限制，邮件正文格式是：第一行为空，第二行书写“ ::”（半角，不包括双引号，下同），第三行书写“ Anonto: ”后接着书写真正收件人的地址，第四行为空，接下来就书写你要发送邮件的内容了。如果邮件程序中使用了签名功能或者使用的模板中有你的信息……

四、利用匿名邮件程序发送

除了以上三种方法外，还有专门用于发送匿名邮件的程序，比如：

(1) GhostMail4.1 , ftp: 〃216.71.135.233/pub/hacker/GM41.zip，259K；

(2) AnonymousMail , ftp: 〃216.71.135.233/pub/hacker/amial.zip，71K。

以 GhostMail4.1 使用为例：

下载的程序解开执行后有下列四项：

Host:选择由哪一个 MailServer（邮件服务器）发信；

From:随便填写一个名字；

To:为收件人的 MailAddress（邮件地址）；

Subject（主题）:信件标题。在空白处写下你想说的内容再按下“ Send ”（发送）即可。

除采用第一种方法发送的速度与普通邮件一样外，其余三种方法发送时都有延迟。另外笔者要郑重提出的是：因为匿名发送邮件不会被人察觉，所以你一定不得用此来做坏事，特别是发送网友们普遍痛恨的垃圾邮件（带商业味、带铜臭味的垃圾邮件更可恨）!中国电信目前已经发布《中国电信对垃圾邮件处理暂行办法》，发送垃圾邮件将受到关闭帐户直至移送执法机关的处理。

对 COOKIE 说不

Cookie 可谓大名鼎鼎，它能“记录”用户上网时的“足迹”(如浏览过哪些站点、下载过哪些软件、逗留了多长时间等)，并将信息保存在用户的硬盘上，而后当用户再次访问相同网站时，系统就可以有针对性地进行服务。这虽然方便了用户的使用，但同时也给用户的网络安全带来了一定危害（那些网站偷窥了我们太多的秘密之后，难保它们不会干出些“出格”的名堂来）!! 既然如此，那我们又该如何禁止 Cookie 呢？这就要分为普通方法、简便方法和“绝杀技”三种了，现分别介绍给大家：

一、普通方法：

广大用户若拟将 Cookie 关闭或将其设置为“提示”状态，则应执行如下方法：

(一)IE4.0 用户

1.执行“查看”菜单的“Internet 选项”命令，打开“Internet 选项”对话框。

2.单击“高级”选项卡。

3.复选“禁止所有 Cookie 使用”选项。

4.单击“确定”按钮，关闭“Internet 选项”对话框。

(二)IE5.0 用户

1.执行“工具”菜单的“Internet 选项”命令，打开“Internet 选项”对话框。

2.单击“安全”选项卡（如图 1 所示)。

3.在“请为不同区域的 Web 内容指定安全设置”列

表框中选择“Internet”选项（表示对普通 Internet 站点的安全进行设置）。

4.单击“自定义级别”按钮，打开“安全设置”窗口。

5.此时我们就会在“安全设置”窗口的“设置”栏中看到有关 Cookie 的设置（如图 2 所示），主要包括是否允许存储 Cookie 和是否允许使用 Cookie 等两个选项，用户应将它们的默认值“启用”分别修改为“提示”或“禁用”。

6.单击“确定”按钮，关闭“安全设置”窗口。

7.在“安全”选项卡的“请为不同区域的 Web 内容指定安全设置”列表框中选择其他几个选项（如本地、可信站点、首限站点等），然后重复上述步骤，分别对是否允许在这些站点中使用 Cookie 进行设置（其中本地和可信站点可设置为提示状态，表示根据用户需要确定是否使用，而受限站点则务必设置为“禁用”）。

8.单击“确定”按钮，关闭“Internet 选项”对话框。

采用上述方法之后，Cookie 的运行状态就会由原来的“启用”变成了“禁用”或“提示”（若为“禁用”状态，则无论用户访问什么站点，系统都一概禁止 Cookie 的运行，若为“提示”状态，则系统碰到 Cookie 请求时将会弹出一个提示框，询问用户是否运行相应网站中的 Cookie，广大用户只须根据自己的需要以及该网站的安全程度加以选择即可。

二、简便方法

采用上面的方法虽然可以达到禁用 Cookie 的目的，但操作比较麻烦，有没有什么更简单的方法呢？我们只须打开 Windows98 安装文件夹下的 Cookie 子文件夹，

然后再将该文件夹及其下的所有文件全部设置为只读属性，此后由于 Cookie 处于只读状态，因此它就算想要玩什么花招也难了！

三、绝杀技

上面两种方法都只能禁止文件形式的 Cookie，尽管绝大多数 Cookie 都是采用文件形式存在，但确有少数 Cookie 是保存在内存中的——当用户访问某个站点时由系统自动在内存中生成 Cookie，而用户离开该站点时又自动将 Cookie 从内存中删除。对于这些 Cookie，采用上面的方法有时就不管用了，我们又该如何将它们清除呢？别着急，广大用户只须启动 Windows98 的注册表编辑器，然后将 HKEY_LOCAL_MACHINE、Software、Microsoft、Windows、CurrentVersion、InternetSettings、Cache、SpecialPaths、Cookies 分支删除，并将 Windows98 安装文件夹 Cookies 子文件夹下的所有文件删除，最后重新启动计算机。这样无论什么形式的 Cookie 都逃不出我们的手掌心了。

网上冲浪安全防范

因特网的迅速发展，给人们工作、学习、娱乐及生活的各个方面带来了极大的好处，人们对计算机网络的依赖程度也越来越高，近年来，网络黑客也正在严重威胁着网络上的计算机，网络安全问题越来越被人们所重视。本文简要介绍了防范黑客的几条措施。

1．使用防火墙

防火墙是一个或一组实施访问控制策略的系统。用

于控制内部网络与因特网之间或客户机与其它主机之间的网络传输。当用户决定要提供何种水平的连接之后，就由防火墙来保证不允许出现其它超出此范围的访问行为。防火墙是可以使用的最强大的安全手段。可以防止计算机被非法入侵。简单地说，防火墙类似于一个有人把守的城门，只有符合要求的数据才能进出。1.1 防火墙的选择

对于个人而言，目前应用较多的是个人防火墙。因为个人防火墙具有费用低（或免费，或廉价）、文件小（占用硬盘和内存少）、操作简单等特点，而且有些防火墙功能也是很强的。常用的有：天网防火墙个人版、zoneAlarm、SygatePersonalFirewall、Nortonpersonalfirewall、lockDown 等。天网防火墙个人版目前可用于 Win95/Win98/Win2000，只有 700 多 K，使用特别简单，功能也较强，可在 http://www.newhua.com 等站点下载。zoneAlarm 是一个免费软件，具有功能强大、使用简单、小巧的特点，其大小为 996k，可在 http://www.zonelabs.com 下载。对于喜欢集成类工具和 Symentec 忠实的用户来说，Nortonpersonalfirewall 是您的首选。它具有防止病毒、防止恶意连接和防护特洛伊木马三大功能。SygatePersonalFirewall 也是免费软件。SygatePersonalFirewallv2.1.468，大小为 2.54MB，系统平台为 Windows9x/NT/2000，下载地址：http://www.sygate.com/download/Sygate_Personal_Firewall.exe。

2.防火墙的配置

防火墙要实现其应有的功能，关键在于正确的配置，许多有防火墙的站点被攻破，往往不是防火墙本身的缺

陷造成的，而是由于防火墙管理员配置不正确造成的。而要配置好一个防火墙，关键不在对防火墙本身如何使用上，而在于制定好安全策略。对于个人来说，可能的话尽可能配置得保守些。

有了防火墙，并不是说你的计算机就安全了，正如上面所说的那样，许多被攻破的站点也有防火墙。因为防火墙的配置可能不正确，加之防火墙本身也都存在着缺陷，尽管这种缺陷往往较小。目前针对防火墙的攻击研究也正变得流行。基于上述理由，要保证你的计算机安全，还要和其它措施相配合。

3．正确使用密码

密码用于保证只有经过合法授权的用户才能够访问相应的资源。口令入侵是黑客入侵最常用的一种方法，它利用系统、软件的缺陷和用户的疏忽，取得合法密码，然后进行各种操作。其中，用户的密码使用不当是造成这种入侵成功的最重要原因。选取密码时首先要注意避免以下几种易犯的错误：

（1）使用用户名、登陆名及单位名作为密码；

（2）使用以上的变换形式作为密码；

（3）使用用自己或亲友的生日作为密码；

（4）使用常用的英文单词作为密码；

（5）使用 6 位或 6 位以下的字符作为密码。

4.相对应的正确的做法应注意以下几条原则：

（1）限制密码的长度。密码至少有 6 位以上字符数，应尽可能长些；（2）限制密码的组成。密码应包括大小写、数字、字母等，尽可能复杂些；

（3）密码不要太常见。

（4）限制密码使用期限。不要长期使用同一密码。

建议密码每隔一段时间（如 60 天）更改一次。

（5）限制登陆尝试的次数。在授权的检查过程中，建议用户只有有限次（如三次）机会可以输入自己的密码，如果三次都失败了，则取消其访问权。

（6）不同的场合使用不同的密码。

除了系统和应用软件提供的密码功能外，还可以安装其它专门的密码软件，从而在对系统加密码外，还可以对所有敏感的文件进行加密码，使他人不能进入你的计算机，或者即使进入获取了相关文件也不能破译出密码。4．删除、关闭和限制不必要的服务，禁用和删除不必要的软件

由于攻击者不可能通过不存在或关闭的服务侵入系统。因此，组件提供的网络服务越少，攻击者可以利用的“门把手”就越少，必须保护的“门”也越少。

有时不能关闭某种服务，在这种情况下，要对对它的访问进行限制。限制服务指的是某些人在某些时候可以使用（访问）它，限制服务要做的工作就是划出界限，使一些人的访问被拒绝。常用的有；网络源地址、用户身份验证、一天中的时间等。

一个典型的例子是因特网上的用户不要使用“文件及打印机共享”。如果必须使用，必须使用密码，密码的使用必须符合要求。

除了系统的服务可能存在漏洞和被攻击者利用外，已经安装的其它软件可能也存在着被利用的可能，因此不要安装不必要的软件，如果已经安装了，则要：删除能够删除的软件；限制不能删除的软件。

5．应用补丁程序

为已经安装的操作系统收集合适的供应商补丁程

序。操作系统及其它应用软件发布后，随着时间的推移，“bug”不断被发现，如果不及时安装相关的补丁程序，你的计算机被攻击甚至攻破的可能性就会变大，因此要注意收集并安装相关的补丁程序。

除以上介绍的几条措施外，用户必须经常对系统进行查毒、软件升级，在网上不要轻信别人，不要轻易地泄露自己的相关信息等。需要说明的是，网络安全涉及的因素很多，无论你采取多么严密的措施，都没有绝对的安全。但是对于个人用户来说，如果你采取了上面的措施，你的计算机安全性就会大大提高。

网上信息安全的防范技巧十三法

这是因为我们通过表格来注册和提交个人信息时，程序会把这些信息打包发送到目的地，在传送到目的地的过程中需要经过一系列的网站中转，当然被传送的信息就很容易在所经过的网路上留下自己的踪迹，如果这些蛛丝马迹不幸被某些别有用心的人截获并加以利用，麻烦可就大了--虽然这种几率比较低，但面对如今一无法规二无规则、尚显无序的网络，总应该多加小心。下面，笔者就为各个用户提供一些保护网上信息安全的方法措施，希望能够对各位用户。

1、不轻易运行不明真相的程序

如果你收到一封带有附件的电子邮件，且附件是扩展名为ＥＸＥ一类的文件，这时千万不能贸然运行它，因为这个不明真相的程序，就有可能是一个系统破坏程序。攻击者常把系统破坏程序换一个名字用电子邮件发

给你，并带有一些欺骗性主题，骗你说一些：“这是个好东东，你一定要试试”，“帮我测试一下程序”之类的话。你一定要警惕了！对待这些表面上很友好、跟善意的邮件附件，我们应该做的是立即删除这些来历不明的文件。

2、屏蔽小甜饼信息

小甜饼就是 Cookie，它是 Web 服务器发送到电脑里的数据文件，它记录了诸如用户名、口令和关于用户兴趣取向的信息。实际上，它使你访问同一站点时感到方便，比如，不用重新输入口令。但 Cookies 收集到的个人信息可能会被一些喜欢搞“恶作剧”的人利用，它可能造成安全隐患，因此，我们可以在浏览器中做一些必要的设置，要求浏览器在接受 Cookie 之前提醒您，或者干脆拒绝它们。通常来说，Cookie 会在浏览器被关闭时自动从计算机中删除，可是，有许多 Cookie 会一反常态，始终存储在硬盘中收集用户的相关信息，其实这些 Cookie 就是被设计成能够驻留在我们的计算机上的。随着时间的推移，Cookie 信息可能越来越多，当然我们的心境也因此变得越来越不踏实。为了确保万无一失，对待这些已有的 Cookie 信息应该从硬盘中立即清除，并在浏览器中调整 Cookie 设置，让浏览器拒绝接受 Cookie 信息。屏蔽 Cookie 的操作步骤为：首先用鼠标单击菜单栏中的“工具”菜单项，并从下拉菜单中选择“Internet 选项”；接着在选项设置框中选中“安全”标签，并单击标签中的“自定义级别”按钮；同时在打开的“安全设置”对话框中找到关于 Cookie 的设置，然后选择“禁用”或“提示”。

3、不同的地方用不同的口令

对于经常上网的用户，可能会发现在网上需要设置