软件技术

防木马有绝招

一、“赤手空拳”防木马

步骤一:建立受限账户

打开“运行”对话框,在其中输入命令“net user xiaoyao 123456 /add”,回车执行后,即可在系统中添加一个名为“xiaoyao”的新账户,密码为“123456”。

用“net user”命令添加的新账户,其默认权限为“USERS组”,所以只能运行许可的程序,而不能随意添加删除程序和修改系统设置,这样可避免大部分的木马程序和恶意网页的破坏(如图1)。

步骤二:加固IE

恶意网页是系统感染木马病毒及流氓插件的最主要途径,因此很有必要对IE多一些保护设置。

1.建壳

删除桌面上的IE图标,打开“C:\Program Files\Internet Explorer”文件夹,右键点击“Iexplore.exe”程序,选择“发送到”→“桌面快捷方式”命令,在桌面上创建一个新的IE快捷图标。接着回到桌面,右键点击新建的IE图标,选择“属性”命令,在弹出窗口中,切换到“快捷方式”选项卡,点击“高级”按钮,勾选“以其他用户身份运行”选项(如图2),确定后关闭对话框。

2.脱壳

现在以管理员账户或其他非“xiaoyao”账户登录Windows XP系统后,双击桌面上的IE快捷方式时,就会弹出一个运行身份对话框,在其中输入之前新建的账户名“xiaoyao”及密码,确定后便可进行正常上网操作(如图3)。

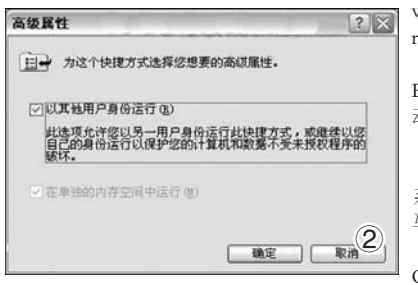
接下来,试试IE是否还能受到恶意插件的骚扰。进入“www.baidu.com”,点击百度页面中的“把百度设为首页”按钮,修改IE的主页。然后点击页面中的“更多”→“搜霸”链接,下载“百度搜霸”。当下载完毕后,该插件将自动运行安装程序,此时会看到它弹出了一个身份认证对话框,默认是以“xiaoyao”身份进行安装的(如图4)。

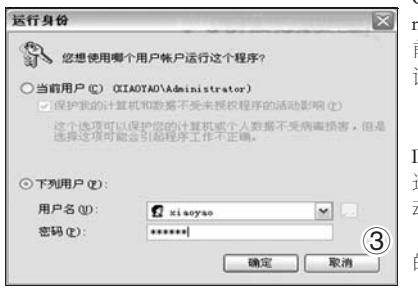
在安装完成后,以“xiaoyao”账户身份再次运行IE时,将会发现首页已变成了百度。以非“xiaoyao”账户运行IE时,可看到IE首页没有任何改变。而之前安装的百度搜霸,则无论以什么账户运行IE,都不会见到它的踪影!

此时是以“xiaoyao”这个USERS组的账户,来进行上网操作的。由于“xiaoyao”账户在当前并未登录,所以百度搜霸根本无法安装并加载到IE中,网页也仅能对“xiaoyao”账户的IE首页进行修改。也就是说,以“xiaoyao”账户身份运行IE后,浏览到的恶意网页只能对“xiaoyao”账户的IE设置进行修改,而恶意网页中的流氓软件或木马间谍运行后,根本无法对当前账户和系统产生任何影响。

3.换壳

如果“xiaoyao”账户的IE设置被更改或破坏,那么可在“运行”对话框中执行“net user xiaoyao/delete”命令,来删除“xiaoyao”账号。之后,再次执行创建账户命令,新建一个名为“xiaoyao”的账户,即可使IE“完好如初”。





步骤三:加固系统

通过网页浏览感染系统,只是木马病毒和流氓插件的一种途径。如果不小心以当前账户身份运行了木马病毒程序,系统还是会被破坏。只是这类破坏迹象都较明显,因此可提前阻止它们。

1.禁止程序启动

很多木马病毒都是通过注册表加载启动的,因此可通过权限设置,禁止病毒和木马对注册表的启动项进行修改。

启动注册表编辑器,依次展开“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”分支,在“Run”分支上点击右键,选择“权限”命令,将当前账户对该分支的“读取”权限设置为“允许”,并取消对“完全控制”权限的选择(如图5)。使用同样方法设置以下注册表启动键的权限:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunEx

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

在“HKEY_CURRENT_USER”下,也有相同的多个注册表启动项需要设置权限(如图5)。

2.禁止服务启动

一些高级的木马病毒会通过系统服务进行加载,对此可禁止木马病毒启动服务的权限。

可依次展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services”分支,将当前账户的“读取”权限设置为“允许”,同时取消其“完全控制”权限。

3.系统安全设置

最厉害的木马病毒会采用DLL注入方式,或者抢先系统启动运行,对此可在注册表中限制其启动权限。

设置的方法同上,需设置权限的注册表项有以下分支:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurentVersion\Winlogon\UserInit

HKEY_LOCAL_MACHINE\Software\Microsoft \Windows NT\CurrentVersion\Winlogon\Shell

HKEY_LOCAL_MACHINE\Software\Microsoft \Windows NT\CurrentVersion\Winlogon\GinaDll

HKEY_LOCAL_MACHINE\Software\Microsoft \Windows NT\CurrentVersion\Winlogon\System

HKEY_CURRENT_USER\Software\Microsoft \Windows NT\CurrentVersion\Policies\

4.保护文件关联

木马还会通过更改系统文件关联,达到启动运行目的。对此可展开“HKEY_CLASSES_ ROOT”分支,将其下的“.exe”、“.com”、“.cmd”、“.BAT”、“.VBS”等项目设置权限,操作方法同上。

使用设置了注册表权限的账户登录系统后,是无法安装软件或进行重要系统更改设置的。如要安装软件,可更换为管理员账户登录系统,并进行正常的安装操作。

二、另类“还原精灵”保系统

1.IE从此无忧

安装这款名为“Sandboxie”的软件后,它会随系统自动运行,利用软件的沙盘功能,即可保护系统不受任何病毒和插件的侵袭。

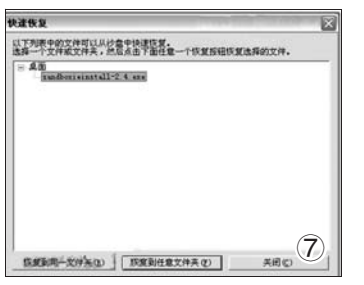
右键点击桌面上的IE图标,在弹出菜单中选择“Run Sandboxed”命令,即可以沙盘保护方式运行IE(如图6)。此时浏览任意恶意带毒的网站,系统都会经过“沙盘”的过滤保护,保证自身不会受到任何影响。即使木马病毒程序已下载到硬盘中,也会随着Sandboxie的关闭而自动消失。

如果要保存通过“沙盘”下载的文件,可右键点击系统托盘区的沙盘图标,在弹出菜单中选择“从沙盘恢复文件”命令。在打开的对话框中,选择沙盘中暂存的文件,点击“恢复到同一文件夹”按钮,即可将文件保存到硬盘中了(如图7)。

2.告别木马病毒

下载了好多软件要安装,但不能确定其中是否夹带着流氓插件或木马,这时可使用右键点击程序文件,通过“Run Sandboxed”命令运行安装,此时程序对系统所作的修改都会被沙盘拦截保护,在关闭沙盘后安装的木马病毒也将随之消失。

如果在沙盘中安装运行后,确认程序是安全的,那么就可再次以正常方式安装运行程序了。



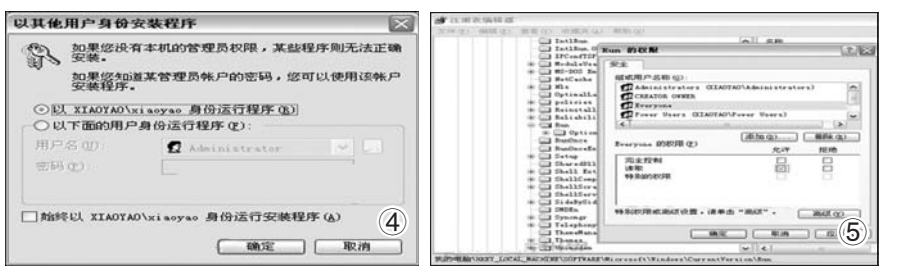
三、程序权限轻松设

安装名为“DropMyRights”的软件,用这个软件启动其他程序,这样启动的程序就只具有基本的权限,无法对系统产生破坏了。方法很简单,以IE为例。

右键点击桌面IE快捷图标,选择“属性”→“快捷方式”,在“目标”位置中输入如下命令(如图8):

“C:\程序安装目录\DropMyRights.exe”?? “C:\Program Files\Internet Explorer\Iexplore.exe” N

程序后面的参数“N”,代表以普通用户权限运行程序。确定后关闭对话框,双击该快捷方式就能以指定的身份启动IE浏览器,以后浏览到恶意网页也不用担心系统会遭到破坏了。 小 网



家电常识

分色洗衣可省电

开始洗衣前,先将脏的衣服在洗衣粉溶液中浸泡至少15分钟,使洗涤剂与衣服上的油垢起反应,然后再放入洗衣机洗涤,这样可大大减少电耗。

若衣服颜色较多最好分色洗涤,先浅色后深色。把颜色不同的衣服分开洗涤,洗得干净,而且也洗得快,比将其混在一起洗省电。

若衣服厚薄不一,如薄软的化纤、丝绸织物等,四五分钟就可洗净,像质地厚的棉、毛织物、麻料等要10分钟左右才能洗净。厚薄衣物分开洗,比混在一起洗省电。

按额定容量操作,这样能省电。若洗涤量过少,白白耗电;相反,一次洗得过多,不仅会增加洗涤时间,而且会造成电机超负荷运转,增加电耗。李 利

如何擦拭液晶屏

1. 使用专用的液晶清洁布或者柔软的纸巾来擦,或是用柔软的眼镜布来擦拭。

2.在擦拭时,切不可太用力,动作一定要轻,否则很容易刮花屏幕。

3.如果是一般的灰尘,用干燥的液晶专用清洁布或纸巾顺同一方向轻轻擦拭液晶屏幕,液晶屏幕上积累的灰尘就可以被清除。

4.如果有顽固的污渍,可在清洁布或纸巾上喷1~2滴专用清洁剂,使清洁布潮湿,然后用清洁布擦拭液晶屏上的顽固污渍。顽固污渍被擦掉后,再用洁净、干燥的清洁布对液晶屏作一次顺同一方向的清洁。

5.液晶屏上的污垢,切记不能用手擦拭,因为人的手指皮肤是带有油性的,用手去点就会留下痕迹,或者手指甲刮花液晶屏。 小 秋