

# 常见网页木马识别防范 20 招

智恒联盟 2007-9-17

第 1 招：禁止使用电脑现象描述：尽管网络流氓们用这一招的不多，但是一旦你中招了，后果真是不堪设想！浏览了含有这种恶意代码的网页其后果是：“关闭系统”、“运行”、“注销”、注册表编辑器、DOS 程序、运行任何程序被禁止，系统无法进入“实模式”、驱动器被隐藏。

解决办法：一般来说上述八大现象你都遇上了的话，建议重装。

第 2 招：格式化硬盘现象描述：这类恶意代码的特征就是利用 IE 执行 ActiveX 的功能，让你无意中格式化自己的硬盘。只要你浏览了含有它的网页，浏览器就会弹出一个警告说“当前的页面含有不安全的 ctiveX，可能会对你造成危害”，问你是否执行。如果你选择“是”的话，硬盘就会被快速格式化。

解决办法：除非你知道自己是在做什么，否则不要随便回答“是”。该提示信息还可以被修改，如改成“Windows 正在删除本机的临时文件，是否继续”，所以千万要注意！此外，将计算机上 Format.com、Fdisk.exe、Del.exe、Deltree.exe 等命令改名也是一个办法。

第 3 招：下载运行木马程序现象描述：在网页上浏览也会中木马？当然，由于 IE5.0 本身的漏洞，使这样的新式入侵手法成为可能，方法就是利用了微软的可以嵌入 exe 文件的 eml 文件的漏洞，将木马放在 eml 文件里，然后用一段恶意代码指向它。上网者浏览到该恶意网页，就会在不知不觉中下载了木马并执行，其间居然没有任何提示和警告！

解决办法：第一个办法是升级您的 IE，此外，安装 Norton 等病毒防火墙，它会把网页木马当作病毒迅速查截杀。

第 4 招：注册表的锁定现象描述：有时浏览了恶意网页后系统被修改，想要用 Regedit 更改时，却发现系统提示你没有权限运行该程序，然后让你联系管理员。

解决办法：能够修改注册表的又不止 Regedit 一个，找一个注册表编辑器，例如：Reghance。将注册表中的

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System 下的 DWORD 值“DisableRegistryTools”键值恢复为“0”，即可恢复注册表。

第 5 招：默认主页修改现象描述：一些网站为了提高自己的访问量和做广告宣传，利用 IE 的漏洞，将访问者的 IE 不由分说地进行修改。一般改掉你的起始页和默认主页，为了不让你改回去，甚至将 IE 选项中的默认主页按钮变为失效的灰色。

解决办法：

起始页的修改。展开注册表到

HKEY\_LOCAL\_MACHINE\Software\Microsoft\InternetExplorer\Main，在右半部分窗口中将“StartPage”的键值改为“about:blank”即可。同理，展开注册表到

HKEY\_CURRENT\_USER\Software\Microsoft\InternetExplorer\Main，在右半部分窗口中将“StartPage”的键值改为“about:blank”即可。注意：有时进行了以上步骤后仍然没有生效，估计是有程序加载到了启动项的缘故，就算修改了，下次启动时也会自动运行程序，将上述设置改回来，解决方法如下：

(1). 运行注册表编辑器 Regedit.exe，然后依次展开

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 主键，然后将下面的“registry.exe”子键(名字不固定)删除，最后删除硬盘里的同名可执行程序。退出注册

编辑器，重新启动计算机，问题就解决了。

(2). 默认主页的修改。运行注册表编辑器，展开 HKEY\_LOCAL\_MACHINE\Software\Microsoft\InternetExplorer\Main\，将 Default-Page-URL 子键的键值中的那些恶意网站的网址改正，或者设置为 IE 的默认值。

(3). IE 选项按钮失效。运行注册表编辑器，将 HKEY\_CURRENT\_USER\Software\Policies\Microsoft\InternetExplorer\ControlPanel 中的 DWORD 值“Settings”=dword:1、“Links”=dword:1、“SecAddSites”=dword:1 全部改为“0”，将 HKEY\_USERS\.\DEFAULT\Software\Policies\Microsoft\InternetExplorer\ControlPanel 下的 DWORD 值“homepage”的键值改为“0”。

第 6 招：. 修改 IE 标题栏现象描述:在系统默认状态下，由应用程序本身来提供标题栏的信息。但是，有些网络流氓为了达到广告宣传的目的，将串值“WindowsTitle”下的键值改为其网站名或更多的广告信息，从而达到改变 IE 标题栏的目的。

解决办法:展开注册表到 HKEY\_LOCAL\_MACHINE\Software\Microsoft\InternetExplorer\Main\下，在右半部分窗口找到串值“WindowsTitle”，将该串值删除。重新启动计算机。

第 7 招: 修改默认搜索引擎现象描述: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网络流氓想要你去的网站。

解决办法:运行注册表编辑器，依次展开 HKEY\_LOCAL\_MACHINE\Software\Microsoft\InternetExplorer\Search\CustomizeSearch 和 HKEY\_LOCAL\_MACHINE\Software\Microsoft\InternetExplorer\Search\SearchAssistant，将 CustomizeSearch 及 SearchAssistant 的键值改为某个搜索引擎的网址即可。

第 8 招: IE 右键修改现象描述:有的网络流氓为了宣传的目的，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\InternetExplorer\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\InternetExplorer\Restrictions，将其 DWORD 值“NoBrowserContextMenu”的值改为 0。

第 9 招: 篡改地址栏文字现象描述:中招者的 IE 地址栏下方出现一些莫名其妙的文字和图标，地址栏里的下拉框里也有大量的地址，并不是你以前访问过的。

解决办法:1. 地址栏下的文字。在 HKEY\_CURRENT\_USER\Software\Microsoft\InternetExplorer\ToolBar 下找到键值 LinksFolderName，将其中的内容删去即可。2. 地址栏中无用的地址。在 HKEY\_CURRENT\_USER\Software\Microsoft\InternetExplorer\TypeURLs 中删除无用的键值即可。

第 10 招: 启动时弹出对话框现象描述:1. 系统启动时弹出对话框, 通常是一些广告信息, 例如欢迎访问某某网站等等。2. 开机弹出网页, 通常会弹出很多窗口, 让你措手不及, 恶毒一点的, 可以重复弹出窗口直到资源耗尽而死机。

解决办法:1. 弹出对话框。打开注册表编辑器, 找到 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon 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启动时出现提示框的现象了。2. 弹出网页。点击“开始-运行-输入 msconfig”, 选择“启动”, 把里面后缀为 url、html、htm 的网址文件都勾掉。

第 11 招: IE 窗口定时弹出现象描述:中网页木马的机器每隔一段时间就弹出 IE 窗口, 地址指向网络注册的个人主页。

解决办法:点击“开始-运行-输入 msconfig”, 选择“启动”, 把里面后缀为 hta 的都勾掉, 重启。

第 12 招: 比如网络上流行的木马 smss.exe 现象描述:这个是其中一种木马的主体 潜伏在 98/winme/xp c:windows 目录下 2000 c:winnt .....

解决办法: 假如你中了这个木马 首先我们用进程管理器结束正在运行的木马 smss.exe 然后在 C:windows 或 c:winnt 目录下 创建一个假的 smss.exe 并设置为只读属性~ (2000/XP NTFS 的磁盘格式的话那就更好 可以用“安全设置” 设置为读取)

经过这样的修改后, 我现在专门找别人发的木马网址去测试, 实验结果是上了大概 20 个木马网站, 有大概 15 个防病毒会报警, 另外 5 个防病毒没有反映, 而机器没有添加出来新的 EXE 文件, 也没有新的进程出现, 只不过有些木马的残骸留在了 IE 的临时文件夹里, 他们没有被执行起来, 没有危险性, 所以建议大家经常清理临时文件夹和 IE。

第 13 招: 初步防御:预备阶段这一阶段, 我还是建议大家首先试一下各种杀毒工具, 把基本的能杀的病毒都给先杀了, 以减轻自己的工作量。比如 IE 病毒专杀工具如 360, 以及金山毒霸, 瑞星, 江民等常见杀毒工具。你需要在预备阶段做的工作就是利用一些杀毒工具把常见的大部分病毒都给杀除了。另外, 如果不能杀除, 你可以再尝试在系统启动时按 F8 进入安全模式在这个情况下再启动杀毒工具和 IE 修复工具进行查杀。

第 14 招: 反击病毒:扫描进程进行查杀笔者的电脑就曾经 CPU 滚烫无比, 发现 RUNDLL32.EXE 这个文件运行了 99%的 CPU 资源, 而这个文件是 WINDOWS 下的 SYSTEM32 文件夹里的, 不应该是病毒。而最大的可能, 它就被用来运行了某些病毒的 DLL 文件。而造成严重损害的。针对进程问题, 首先大家可以用最简单的方法先进行表面清楚, 就是在“开始”里点“运行”, 键入 MSCONFIG, 然后进入启动项设置, 看到不正常的启动项, 比如各种莫名其妙的名字, 以及特别是在非 WINDOWS 系统文件夹下的(可以直接删除都没事), 以及各种奇怪的可执行文件, .exe 的, 给予坚决取消启动。并可找到那个文件的位置, 给予删除, 如果非系统文件夹下的, 你大可以放心删除。另外, 推荐大家一款免费的进程扫描工具 hijackthis, 大家可以找它的汉化版的, 用来扫描进程。尤其是隐藏在 SYSTEM32 文件夹下的, 某些异常的.exe 文件, 以及它的上级文件夹。不要怕, 进入 c:/windows/system32, 进去之后, 找到那个文件, 以及它的父文件夹。有时候, 你会很惊讶的发现, 这个可执行文件病毒就被你发现了, 有的病毒执行程序, 你查看属性时, 竟然写到了某某广告公司, 这些病毒往往都是一个单的可执行文件, 放在 SYSTEM32 下或者一个文件夹里。马上彻底删除!有的无法删除, 正在运行的, 你要借助一些文件粉碎机来删除。而好象 SP2 的 WINXP 自带粉碎文件功

能。就这样，你根据可疑进程，特别是扩展名为 .exe 的文件，找到它隐藏的文件夹，看它的属性和修改日期，有的是往往是发生病毒情况的那一天的，很容易就发现它是病毒，直接封杀！有的更“牛”一点，在父文件夹里还带着一些广告网站的 .ini 文本文件和其它文件夹，这个没事，你打开看看那些文件夹里都是啥，有时候你能发现这些 .ini 文件里就写着骚扰你的恶意网站或者其它广告网站的地址。发现了就好，然后再看看这个文件夹的修改时间，如果是发生病毒时候的，还等什么？整个这个异常文件夹一下子删除！就这样，你可以通过进程扫描，寻根求底的方法，找到隐藏的系统文件下，通过查阅文件夹以及异常文件属性等，直接手工删除！

第 15 招：主动出击：根除残留病毒有时候，某些病毒并不是在运行，而是在你打 IE 之后的某个时间或者激发了某些事件，它们才会运行。有的还是某些 .DLL 文件，隐藏在系统文件夹下，很难发现，而且往往误认为是系统文件而不敢查杀。这些成为最顽固的病毒，不用怕。这些也都可以通过第三招而杀除。最常用的方法是根据文件夹和文件修改创建时间。首先你把文件夹属性调整为查阅所有文件，包括隐藏文件和系统文件。然后右键，再通过查看文件方式选择为查看详细信息，则会出现详细信息列表，你可以通过选择最近时间排列，而看到最新创建的一些文件夹和一些文件。如果你记得你病毒发作的那第一天时间，直接可以发现那些异常文件夹的创建时间和病毒发作时大概相同，直接进去查看，有时候往往发现这些文件夹里果然包含着广告网站的信息等或者其它异常内容。不管有没有，直接删除这些文件夹吧！有的如果是你最近装过的软件的话，你自己也会清楚，如果不是的，那就是病毒创建的文件夹了。删除这些新创建的对你系统运行也没有损失。

第 16 招：用插件管理来定位流氓软件的位置。第一步：打开“IE”- 工具- internet 选项- 程序- 管理加载项然后会列出很多 IE 插件，我们要做的只是观察插件的发行者，如果看到发行者前面有个“未验证”的话，我推荐别管它起什么作用，禁用，然后把不是 microsoft 的都禁用了，不用担心会关闭某些有用的插件，比方说播放网页中 flash 的插件，就算我们关闭了，以后 IE 会提示你。在状态栏上有个齿轮的符号，双击打开，然后它会提示你需要哪个插件，你到时候再恢复也不迟。第二步：记录下刚才被基本怀疑为流氓软件的插件(Dll 文件)的名字，然后到搜索中对系统进行搜索，一般来说，大部分流氓软件都会安装到 x:\ProgramFiles\下面，找到流氓软件安装的文件夹，先尝试删除，应该是没办法删除的，系统会跳出个窗口——“某文件正在被使用”，那么说明你刚才光在 IE 里清除是不够的，因为流氓软件已经将其自己加载到 rundll32.exe 进程中了。第三步：我们要使用 icesword 进行操作了。打开 icesword，然后选进程，找到 rundll32.exe（有时候可能会有几个，如果有多个的话，一个一个操作），点右键选择“模块信息”，在模块里找到你刚才没办法删除的 dll 文件，现在强行结束这个 rundll32.exe 进程，然后回到 ProgramFiles 下，先别急着删除。现在打开 regedit.exe 开始搜索 dll 插件（就是你刚才在 rundll32 模块里找到的那个流氓软件的插件），找到一处就点右键删除注册键值，然后按 F3 继续搜索，直到跳出个窗口说搜索完毕了，那就说明你已经很干净地清除了流氓软件，删除刚才找到的文件夹，重新启动电脑吧！

注册表的操作有几个注意点：

- 1、不要乱删键值，如果不小心删除了某个重要的数据，电脑可能会发生问题的。
- 2、regedit.exe 里搜索时候，先点最顶端的我的电脑（注意：是注册表编辑器里的“我的电脑”），这样注册表搜索能搜索得最彻底。

注意：流氓软件有时候会同时用两个或以上的 dll 文件对 IE 进行捆绑，所以要把刚才

的步骤做几次，一个一个的解除 dll 文件对 IE 的捆绑。

第 17 招：如果是自己运行的服务器被别人入侵攻击后挂马，最直接的方法就是重新覆盖网站所有代码，更新系统补丁和帐号密码等信息；其次，可以查看编写程序代码缺陷，如果利用网站自动生成系统，查看该系统的补丁程序；另外，可以配置 WebGuard 网页防篡改保护系统进行网站保护，该系统可以实时检测网页文件变化，即刻恢复到原始状态，并发现哪些文件被修改。

第 18 招：采用掘马网页木马检测系统，该系统除了可以进行网页木马定位，可以定位到某一行代码，帮助网管人员在数以万计的代码中查找出隐藏的木马，还可以做文件更新对比发现，可以发现哪些文件做了更新，这可以迅速定位到某个文件。

第 19 招：如果您是局域网的网络管理人员，可以对局域网部署 SUS 系统，或者桌面管理系统，该系统可以帮助大家进行补丁实时更新。当然了特别要关注浏览器更新内容，建议大家使用 firefox 或者 maxthon 等浏览器，并配置浏览器禁用脚本，如果能禁用图片或动画文件那也是比较安全的做法。

第 20 招：时刻警惕：不要浏览陌生人发的网站链接或具有诱惑性的网站链接！