Windows系统及应用技巧（4） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/225/2021_2022_Windows_E7_B3_BB_c100_225218.htm 如何判断自己是遇到了恶意网站的攻击，症状多种多样： 1. 开机自动登录网站。 2. 启动IE，自动登录网站，无法修复主页设置。 3. IE不断打开窗口。 4. 修改[主页]按钮和[搜索]按钮。 5. 修改右键菜单，甚至屏蔽右键菜单。 6. 更改收藏夹的内容。 7. 安装自动拨号程序。 8. 自动安装木马程序。 9. 自动格式化硬盘或删除某个文件夹中的所有文件。 10. 更新文件关联和锁死EXE程序。 11. 锁死注册表。 ★对症下药 了解了症状，就要对症下药了！ 一、备份 建议使用“ 超级兔子魔法设置 ”中的“ 注册表优化 ”进行备份，软件能将Classes.dat、System.dat、System.ini、User.dat、Win.ini等文件全部备份下来，上面提到的前五种恶意网站无非就是通过修改这些文件来达到其目的的。 二、弃用IE 大部分的攻击目标都是IE。如果我们用MyIE2（强烈建议使用Ver 0.8.220这一版本）代替IE浏览器，恶意网站就无的放矢了。MyIE2在启动时能够绕开主页直接打开空白页，而且还能保护主页不被修改。如果开机就自动运行IE，要先用超级兔子魔法设置中的“ 自动运行 ”功能将网址删除，再用MyIE2代替IE。 注意：这两个功能在默认状态下是关闭的，您要在[选项]→[MyIE2选项]→[常规]中和“ 启动时 ”中将其打开。由于MyIE2使用IE的内核，所以请勿删除IE。 三、解救被封死的收藏夹 某些恶意网站会对收藏夹进行修改，大多是通过修改“ C:\ Windows/Favorites ”中的“ Desktop.ini ”文件来实现的，所以只要删除这个文件就可以了。如果根本

就无法打开“ C:\ Windows\Favorites ”文件夹，就到DOS下进行删除（要先用“ attrib -r -s -h ”后才能将其删除）。另外，“ 收藏夹 ”中的内容并没有被删除，只是放入了另一个文件夹中，名称和“ Favorites ”差不多（如“ Favorites2 ”等），如果想恢复原来的“ 收藏夹 ”，只要剪切一下就可以了。 如果是将系统默认的“ 收藏夹 ”路径设置成指定的目录（如“ C:\ Windows\Favorites2 ”等），只要恢复正常的“ 注册表 ”就一切OK了。 四、定期还原正常的注册表 如果遇到安装自动拨号程序的情况，你可要小心啦，小心惊人的国际长话费。对付它，最好是定期还原正常的注册表！这样做虽然不能彻底删除此类恶意程序，但却能让其完全禁止运行，因为这类程序是通过修改注册表来达到随机运行的目的的（只有极少数是在“ 开始 ”菜单的“ 启动 ”项内做文章），只不过我们无法通过手工删除干净。 这个方法对于自动安装木马程序的情况也同样适用。 五、防止硬盘被格式化 对于自动格式化硬盘的恶意网站，要把“ C:\Windows\COMMAND ”文件夹中的format.com、Fdisk.exe、Deltree.exe这三个程序文件删除或进行改名，因为这些恶意代码是需要这些程序才能够发挥“ 威力 ”的，只要让这些恶意代码找不到它们，您的电脑也就安全了！ 六、打开“ 锁死 ”的程序 对于被锁死的EXE程序，只要事先已将“ C:\Windows ”目录下正常的Classes.dat、System.dat、User.dat、System.ini、Win.ini这五个文件备份下来，在“ 中招 ”后用正常的文件覆盖一下并重新启动就OK了（注：Windows 95和98中可能没有Classes.dat文件，而且Windows 97以下版本的操作系统用此方法无效！甚至会使整个系统瘫痪。）。如果连复制都被禁止了的话，您可用启

动盘到DOS下进行覆盖复制。 七、“ 防 ”要胜于“ 治 ” 通常恶意网站都披着具有“ 诱惑力 ”的外衣，设下诱人的陷阱让您“ 中招 ”。所以一定要意志坚强，抵制住诱惑。只要您能做到“ 任你花言巧语，我自岿然不动 ”。那么，什么样的陷阱也奈何不了您。 另外，现在有很多恶意网站开始通过即时通讯软件来传播了，比如QQ、ICQ等，方式虽然多种多样，但通常是在对方网友的话后面又发来了一个网站信息，有的会附有一些带有“ 诱惑性 ”的话（如：“ 看看我的样子 ”等），有的只是一个有着诱人域名的网址，对于这样的网站，原则也同样就是不上当！ 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com