Windows系统及应用技巧（1） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/223/2021_2022_Windows_E7_B3_BB_c100_223195.htm 几天一些恶意网站的恶意代码闹得挺凶，像是www.58q.com www.qq230.com 这样欠黑的网站，一打开这些网页就中了恶意脚本，而且一般的IE修复和杀毒软件都不能比较彻底清除。 典型症状： 1. IE 首页被改为恶意网站，默认主页，起始页，甚至搜索页全部被更改 2. C盘下生成文件夹：$NtUninstallQxxxxxxx$（x代表数字） 从名字上看企图冒充微软更新补丁的卸载文件夹，并且在Win2000/XP下拥有系统文件级隐藏属性，比较隐蔽。文件夹中包含了恶意脚本文件winsys.vbs、winsys.cer 3. 随机启动项被添加3项： 4. 如用杀毒软件查杀，可以查到名为Harm.Reg.WebImport.g 的病毒，但若是清除不彻底，只是删除了文件夹，开机将会出现提示： 清除方法小结： 1. 删除启动项： 建议通过msconfig、优化软件禁用或注册表手动删除以上3项启动项 HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Run 删除：regedit -s C:\$NtUninstallQxxxxxxx$\WINSYS.cer HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce 删除：Sys32，值为：C:\$NtUninstallQxxxxxxx$\WINSYS.vbs

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 删除：Sys32，值为：regedit -s C:\$NtUninstallQxxxxxxx$\WINSYS.cer 删除：internat.exe，值为：internat.exe 2. 删除文件夹： 文件夹选项设置 然后删除整个$NtUninstallQxxxxxxx$ 目录 3. 清理注册表： 记下恶意网站的域名，以它为关键字搜索注册表或用注册表清理工具，因为恶意网站的名字会替换注册表中所有IE 默认起始页、默认搜索页、默认主页等键值。 一旦通过这种方式再次打开恶意网站，以上做的就白费了，所以清理完以前暂时不要打开IE，如需要访问某些网站，可以通过运行输入网址或收藏夹等方式访问。 根据恶意代码的内容，附上被修改的注册表键值，供参考：

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchURL

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Search\SearchAssistant

HKEY_USERS\.Default\Software\Microsoft\Internet Explorer\SearchURL

HKEY_USERS\.Default\Software\Microsoft\Internet Explorer\Main\Search Page

HKEY_USERS\.Default\Software\Microsoft\Internet Explorer\Main\Default_Search_URL

HKEY_USERS\.Default\Software\Microsoft\Internet Explorer\Main\Search Bar

HKEY_USERS\.Default\Software\Microsoft\Internet Explorer\Search\SearchAssistant

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search\SearchAssistant
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\First Home Page
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Default_Search_URL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Search Page
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Search Bar
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Local Page
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\Default_Page_URL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\SearchURL 4. 清理完成后： 建议屏蔽此类网站，具体方法可以搜索以前的讨论，建议试试通过Hosts 屏蔽，嘿嘿 另外对WinXP或安装文字服务的系统，清除恶意代码后，任务栏上的输入法指示器可能消失，无法使用输入法 偶个人试验一下，在开始>运行中输入：ctfmon.exe，启动输入法指示器并加入随机启动组，一般可以解决这个问题，如果问题依旧，请开新帖讨论 补充说明： 系统文件夹（\WINNT或\Windows）下出现的如$NtUninstallQ823980$、$NtUninstallQ814033$ 这类文件夹是Windows Update 或安装

微软补丁程序留下的卸载信息，用来卸载已安装的补丁，按补丁的编号如Q823980、Q814033 可以在微软的网站查到相应的说明。请注意与恶意代码建立的文件夹区分 。 如果不打算卸载已经安装的补丁，这些文件夹也是可以安全删除的 。