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_ti2020/140/2021_2022_Windows_E7_B3_BB_c100_140541.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 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