

浏览器主页被篡改的背后，有你想不到的赚钱方式（附解决方法）

原创 安哥拉 效率工具指南

收录于话题

#效率工具 94 #2021 93 #浏览器劫持 1 #Windows 16 #浏览器 9



配图：来自 Unsplash

Hello 大家好，我是安哥。

今天来聊一聊「**电脑浏览器主页被流氓软件劫持**」的话题，这里的「**劫持**」是指，每次打开浏览器，它都会**自动打开你从未设置为浏览器主页的网站**，这些网站可能是：

- 2345 导航页
- hao 123 导航页
- 360 导航网站

劫持之所以长期存在，还是因为**利益**的驱动，流氓软件可以供你免费下载、免费使用，但你需要付出相应的代价：**你被当成流量**，卖给各类需要用户的导航网站。



导航网站上会有花样繁多的网站，提供各类服务，不要以为导航网站就是慈善家，排在导航网站显眼位置的服务，大多都是向导航网站花了钱「优化」过的。

这条产业链大致的思路就是：**流量的倒买倒卖**，把从浏览器主页劫持获取的用户，转手卖给导航网站上的其他产品或服务。



流氓软件频繁广告弹窗就算了，还要被当成流量卖给导航网站，这情况有点像是「被别人卖了，还在帮人数

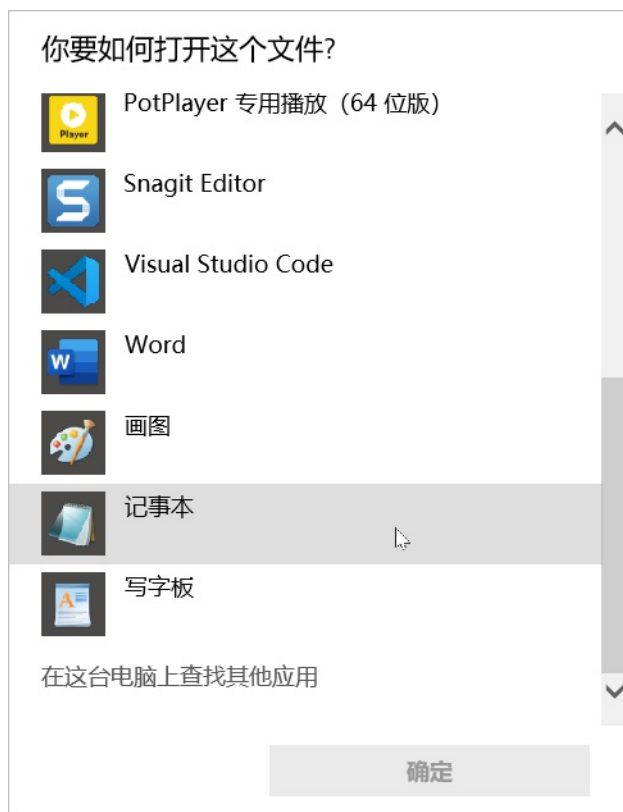
钱」，实在是太让人看不过去了。

因此，今天的这篇文章，我想给大家介绍 4 种解决浏览器主页劫持的方法，希望对遇到同样问题的朋友有帮助。

01. 屏蔽导航网站

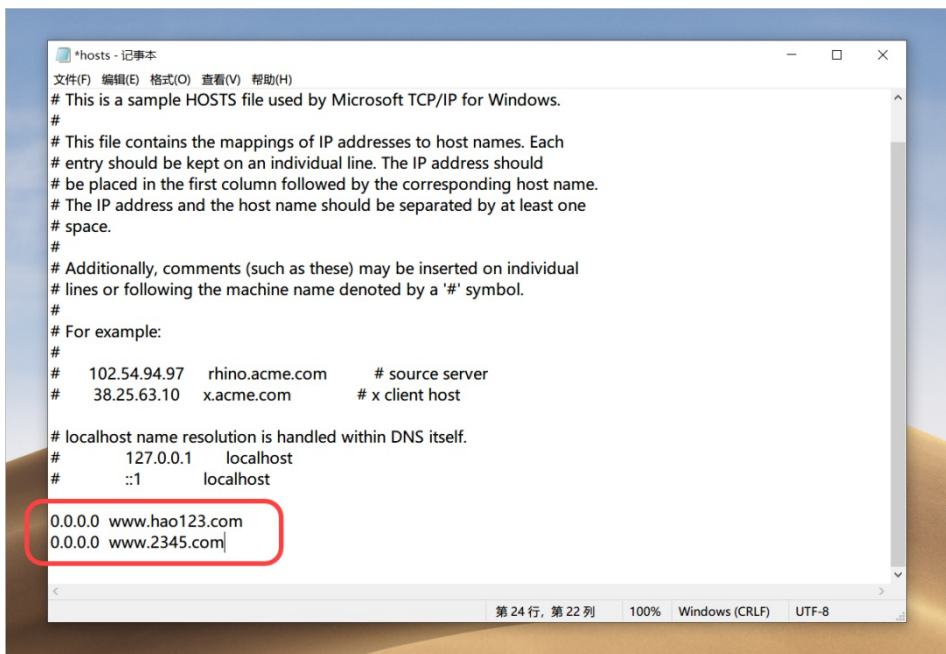
屏蔽导航网站，需要先按照路径 **C:\Windows\System32\drivers\etc** 打开存放 **hosts** 的文件夹。

双击 hosts 文件，系统会询问「如何打开这个文件」，这里我们选择以「记事本」的方式打开。

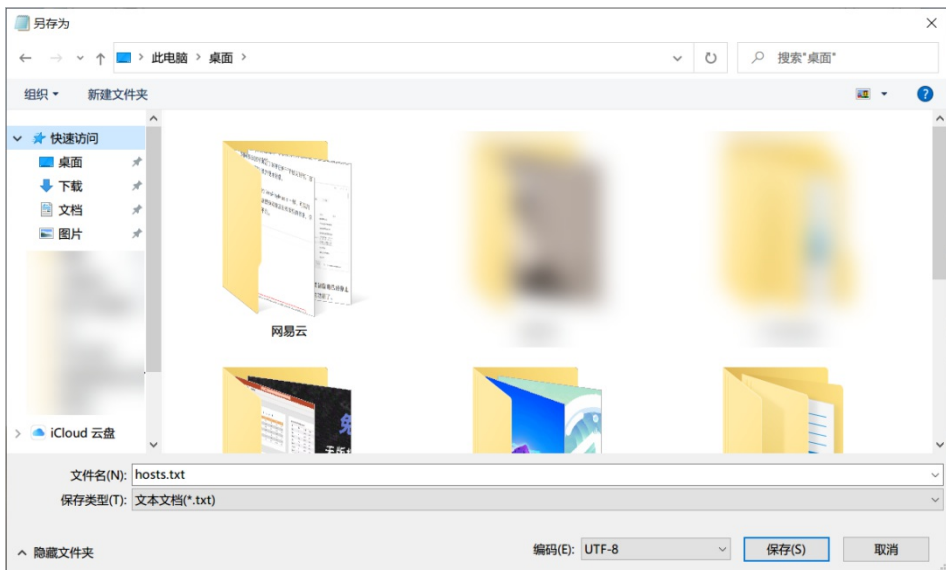


打开 hosts 文件后，在文件末尾添加你想屏蔽的网站，写法如下：

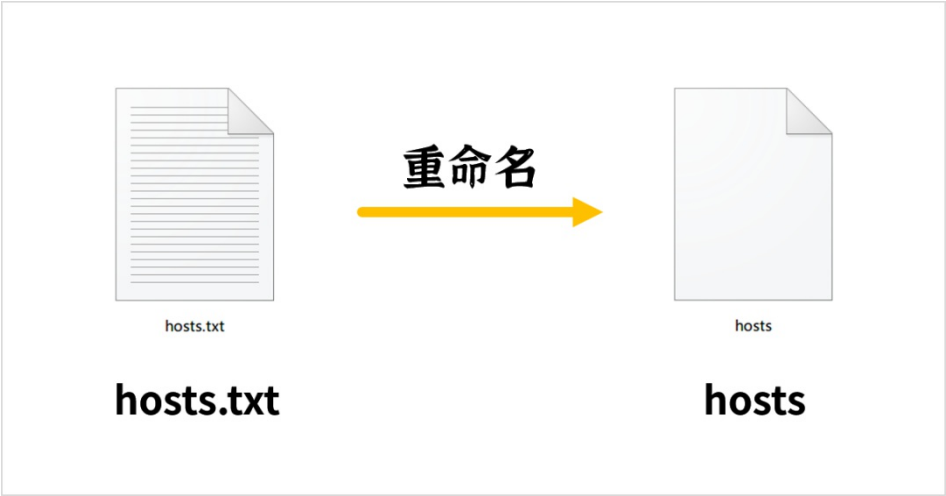
0.0.0.0 + 空格 + 想屏蔽的网站（注：0.0.0.0 代表屏蔽）



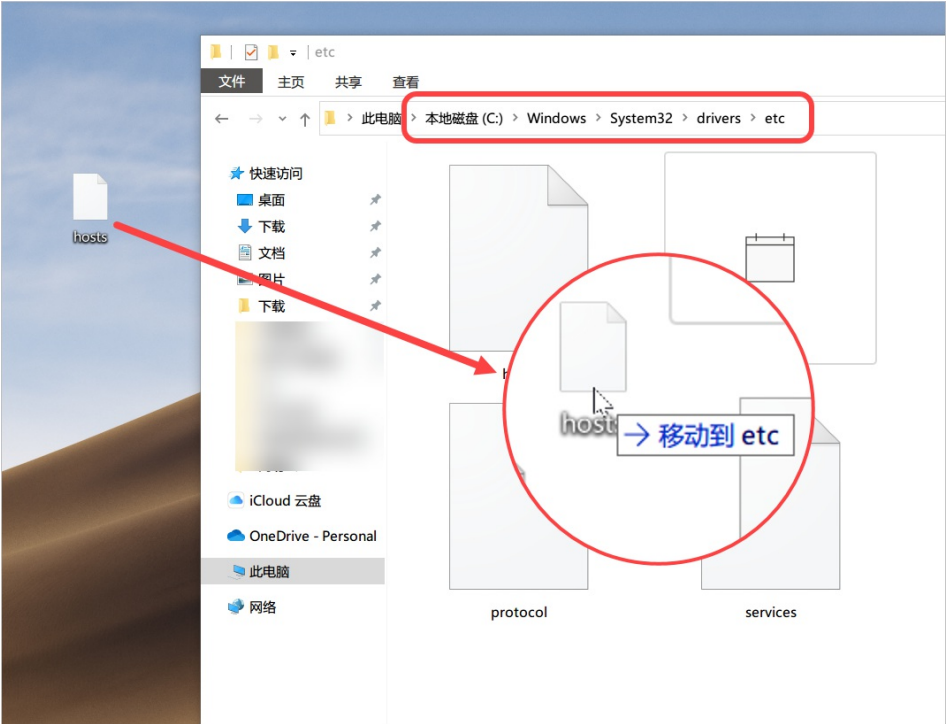
使用快捷键 Ctrl + S 保存编辑好的文件，将文件以 txt 文本的格式保存到桌面。



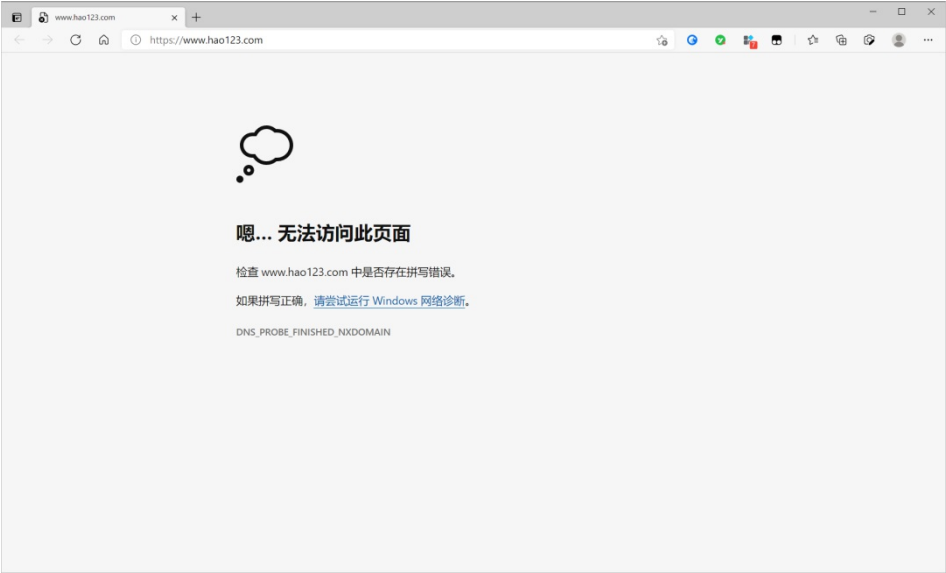
接着对保存得到的 hosts.txt 文件进行**重命名**，去除 .txt 的后缀，得到一份与编辑之前的同名文件 hosts。



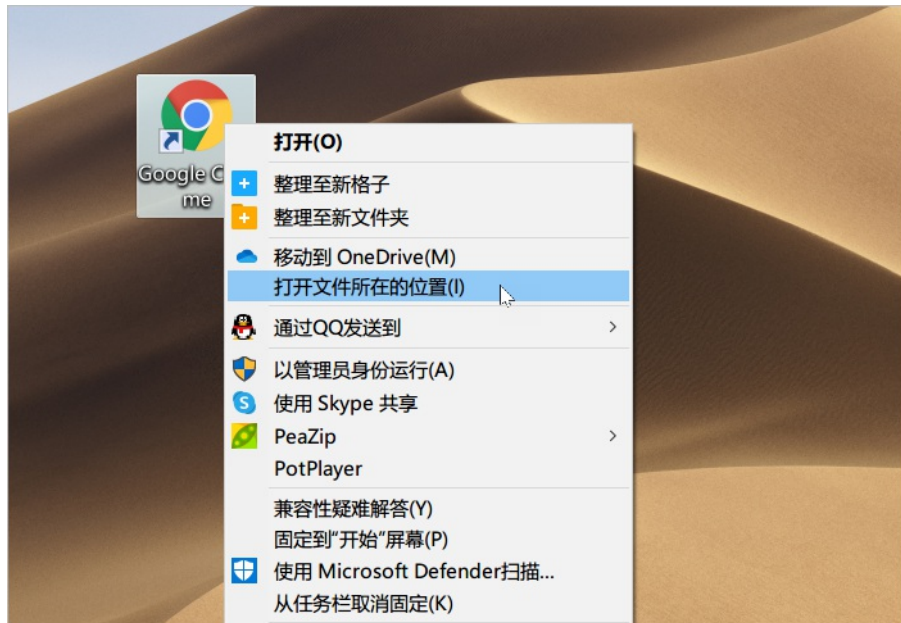
接着将放在桌面的 hosts 文件拖拽到文件夹 `\etc` 下，覆盖原先的 hosts 文件。



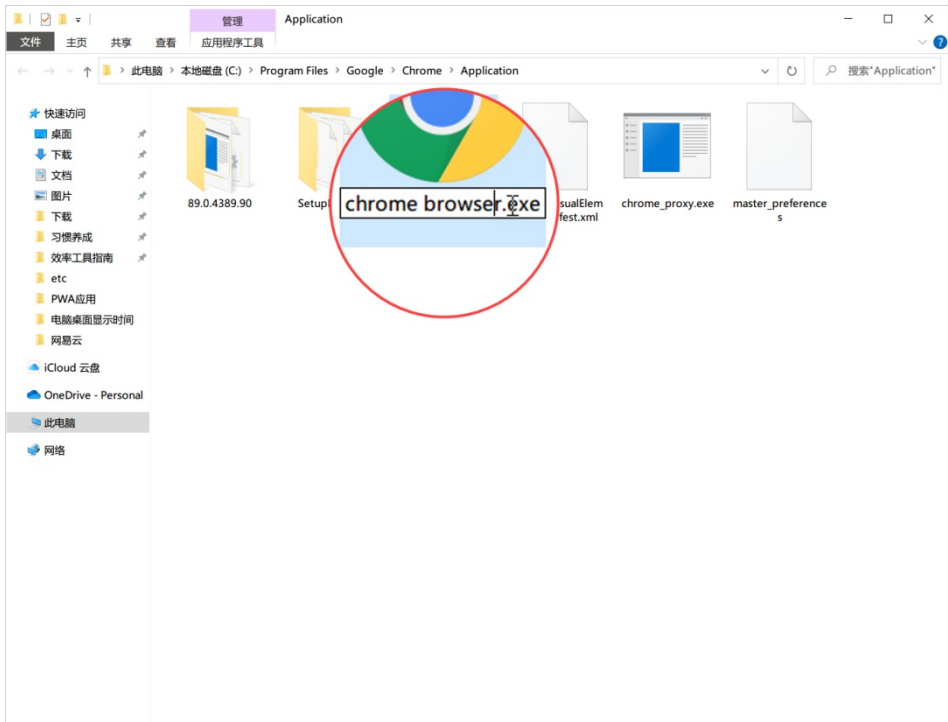
覆盖之后，在浏览器中尝试打开被屏蔽的网站，你会发现网页提示「无法访问此页面」，这样就达到屏蔽网站的目的了。



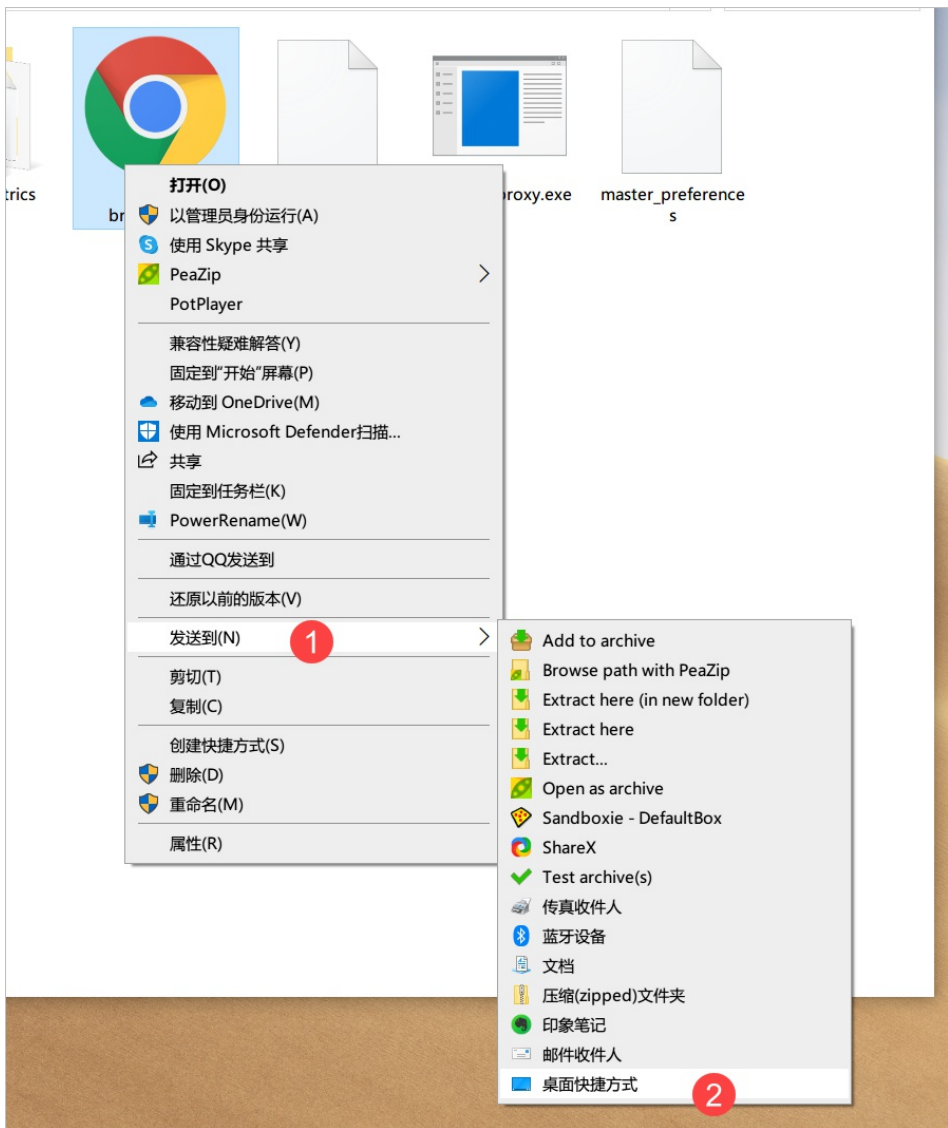
屏蔽导航网站之后，被劫持的浏览器的快捷方式可能无法正常使用，此时我们可以先右击桌面的浏览器快捷方式，选择「打开文件所在的位置」。



在打开的文件夹路径下，**重命名浏览器的 exe 文件**，例如将原先的 `chrome.exe` 更名为 `chrome browser.exe`。

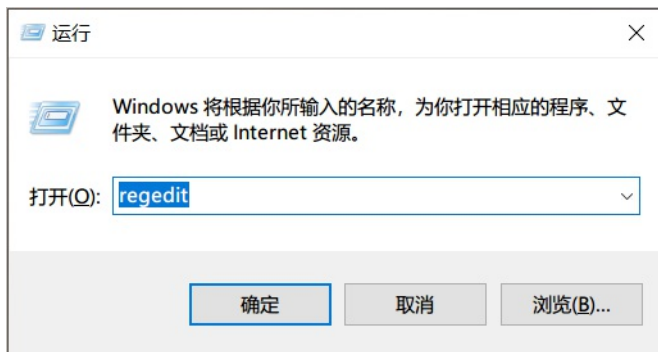


接着右击完成重命名的 exe 应用，选择「发送到 >> 桌面快捷方式」，删除原先失效的快捷方式，使用新的浏览器快捷方式即可。

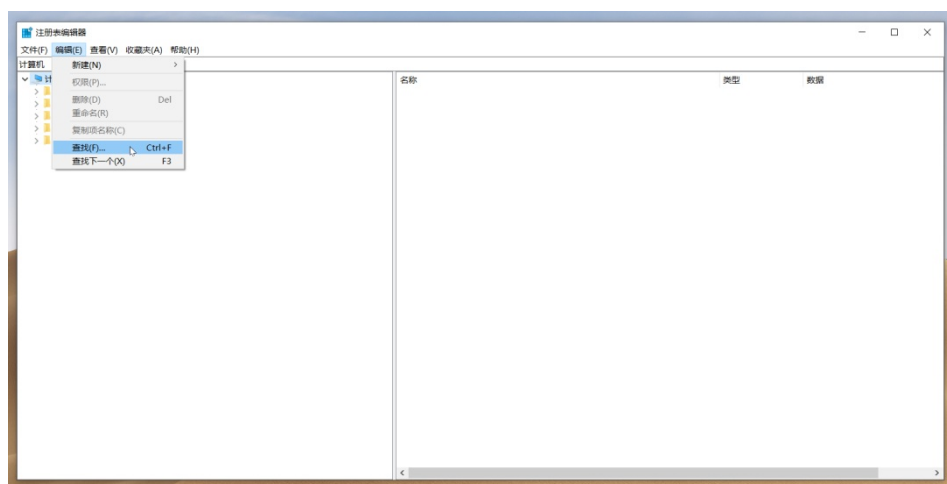


02. 删除注册表

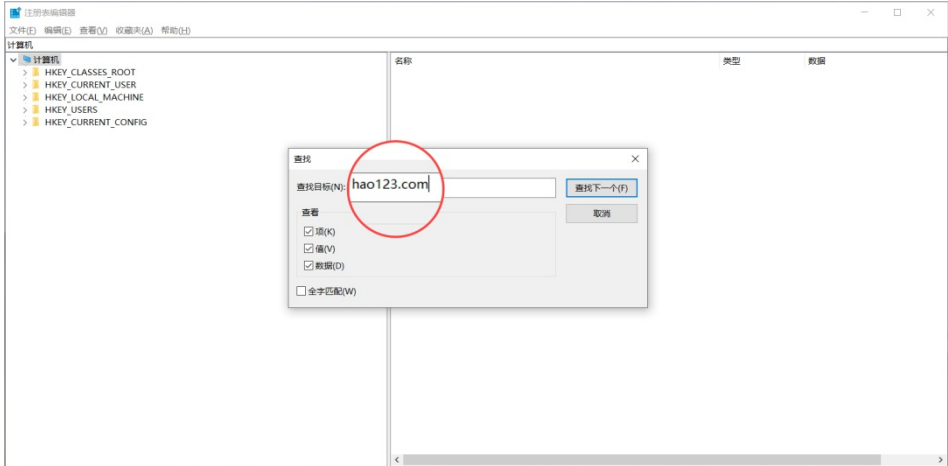
使用 **Win + R** 打开运行窗口，输入 **regedit** 并按下回车键，打开注册表的编辑面板。



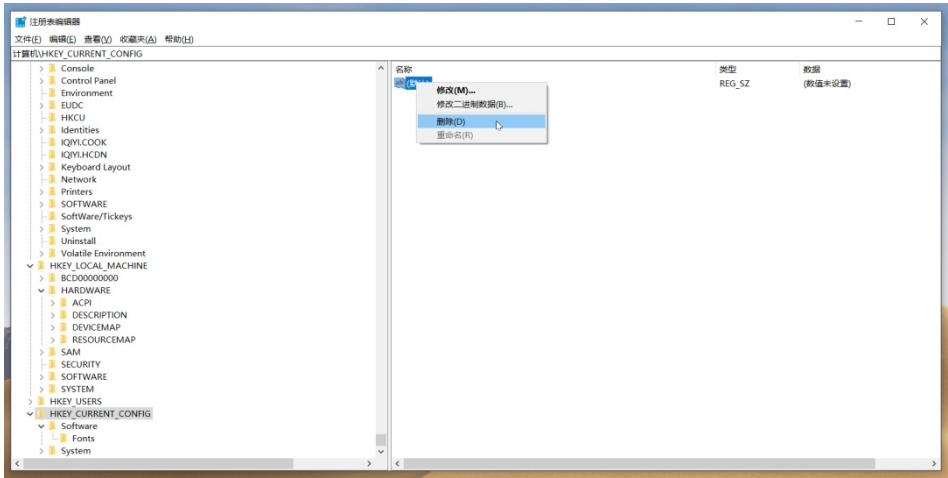
点击顶部的编辑选项卡，选择「查看」，打开注册表搜索面板。



在输入框中输入你想屏蔽的导航网站的网址，例如图中的 `hao123.com`，在注册表中查找与 hao123 相关的注册表。



如果返回的结果中有 hao123 导航页相关的注册表，可以右击右侧的文件，将注册表文件删除。

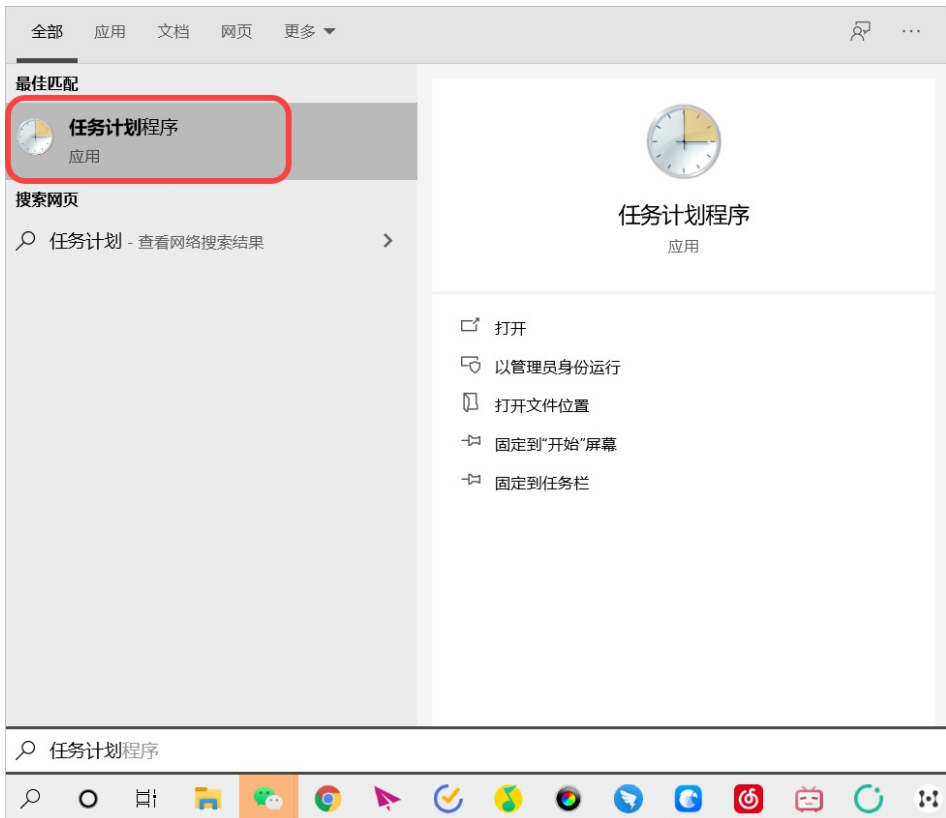


值得一提的是，编辑注册表是一个比较危险的操作，建议和我一样对注册表一窍不通的朋友，不要随意删除或更改注册表中的其他文件。

03. 删除计划任务

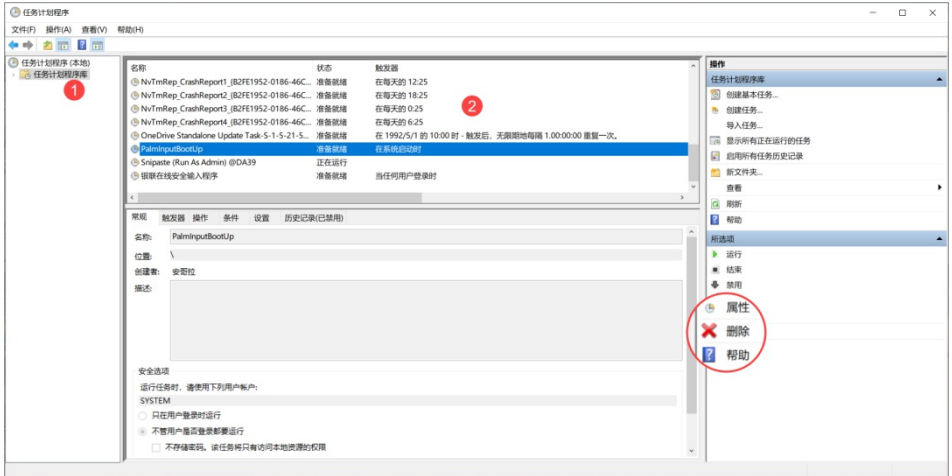
卸载流氓软件之后，有时还是不能将彻底解决浏览器劫持的问题，这是因为卸载后还是会残留一些**启动项**或者**自动触发的任务**。

使用 **Win + S** 打开 Windows 自带的搜索，输入「任务计划」，打开系统自带的「任务计划程序」。



点击页面左侧栏的「任务计划程序库」，中间的窗口会列出系统当前**正在运行**或**准备就绪待运行**的程序。

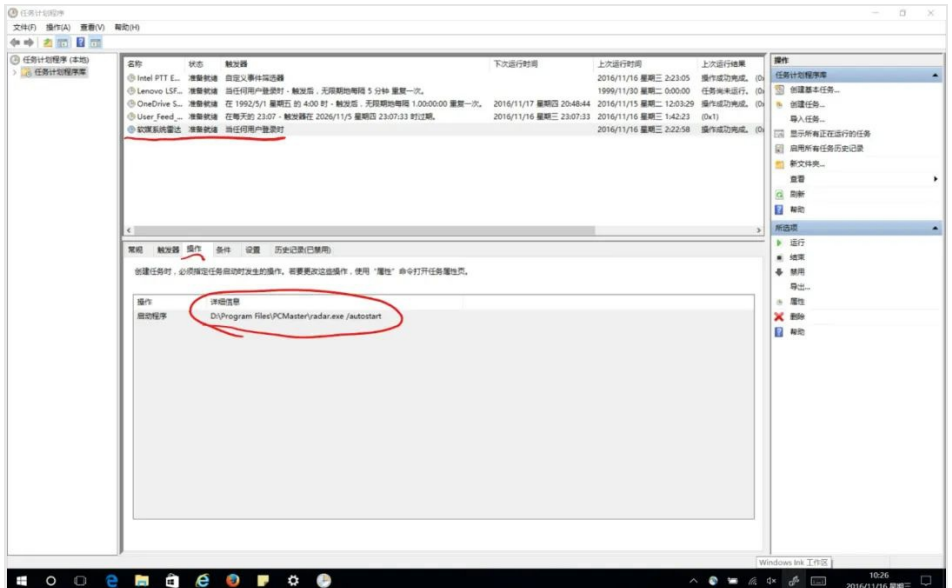
对于那些已经卸载的流氓软件，如果你在列表中还能看到它的名称，可以选中其名称，接着选择右侧的「删除」，就可以清理残留的启动项。



由于我用的电脑还没遇到浏览器劫持的问题，这里暂时不能用自己的情况进行演示。

我从网上找了一个网友提供的图片，他是因为安装了「软媒魔方」而遇到了浏览器劫持，卸载软件之后它还残留了「软媒系统雷达」的启动项。

按照前面的说法，将其从任务计划程序中删除，应该就可以解决浏览器劫持的问题了。



04. 火绒恶性木马专杀工具

如果前面的三种方法都无法解决浏览器劫持的问题，那我只能祭出最后一款工具了。

火绒恶性木马专杀工具，是火绒安全团队推出的另外一款安全产品，专门用来对付电脑病毒和解决浏览器主页劫持的问题，使用起来非常简单。



火绒安全论坛
bbs.huorong.cn

官方网站

登录 | 注册

请输入搜索内容

首页 > 论坛 > 火绒产品 > 火绒安全工具 > 火绒恶性木马专杀工具

火绒安全工具



火绒安全
www.huorong.cn

浪子

[综合讨论] 火绒恶性木马专杀工具  [复制链接]

7310863 773 发表于 2016-12-2 16:42:14 | 只看该作者 | 倒序浏览 | 阅读模式 | 电梯直达

亲爱的火绒用户：

您好，由于内核对抗存在风险，火绒安全软件中不会与Rootkit病毒进行直接对抗。为更好的解决顽固病毒（Rootkit、Bootkit等病毒）问题，火绒安全推出“火绒恶性木马专杀工具”与病毒进行内核对抗，从而快速帮助用户解决所遇到的病毒问题。

主要解决的问题：

1. 顽固病毒木马问题（如：紫狐、ADSafe、MLXG病毒等）

2. 火绒安全服务异常问题（部分火绒安全服务异常也是由于内核级病毒导致）

3. 流量或首页劫持问题等

使用注意事项：

专杀工具在扫描过程中，如果检出了病毒处理项目，则建议在扫描完成后，重启再次使用火绒专杀进行扫描，以确认病毒清除是否成功。

如果重启后再次扫描，在专杀工具中没有病毒项目再被检出，则建议使用火绒安全软件进行全盘扫描，彻底解决病毒问题；

如果重启再次扫描后，专杀工具依然能够检出病毒，则请通过火绒论坛或者其他官方渠道向我们进行反馈。

下载之后双击 exe 应用即可运行，等待软件完成查杀，如果你的电脑存在浏览器劫持的问题，它会检测出来并自动修复。

对了，完成查杀之后，「完成」按钮下方会默认勾选「安装“火绒安全软件”」，即这款工具也会帮着推广它自家的另外一款产品「火绒安全软件」。

如果你不需要的話，先取消下方的勾选，再点击「完成」按钮，软件就不会自动下载并安装另外一款软件。



查杀完成，未发现恶性木马病毒

发现威胁: 0个

成功处理: 0个

完成

☒ 安装“火绒安全软件”，提前防御全面查杀病毒、木马以及流氓软件

当前版本:1.0.0.56

问题反馈

在使用这款工具的过程中，如果你遇到了自己无法解决的问题，可以前往火绒安全的论坛，寻求官方人员的帮助。

火绒安全论坛
bbs.huorong.cn 官方网站

登录 | 注册 | 请输入搜索内容

论坛 | 火绒官方服务 | 主页劫持专项整治

主页劫持专项整治 今日:22 | 主题: 4632 | 排名: 6

全部 | 综合讨论 204 | 病毒木马 212 | 恶意网址 1744 | 流氓软件 17 | 样本误报 1 | 官方公告 18 |

全部主题 | 最新 | 热门 | 精华 | 更多 | 新窗

关于微软签名机制影响火绒使用相关问题回复

huoronganquan | 阅读 272 | 回复 2 | 小多科技于2021-3-15 20:57最后回复

昨天 19:23发布

重要通告: 微软签名机制将影响火绒正常使用, 现提供解...

huoronganquan | 阅读 732 | 回复 9 | abcdcfghi于2021-3-15 18:55最后回复

昨天 09:32发布

5.0.59.0版本升级公告【3月15日】

火绒运营专员 | 阅读 452 | 回复 1 | Dazjka6606于2021-3-15 18:02最后回复

昨天 16:08发布

微软紧急发布多个Exchange高危漏洞 请用尽快修复

huoronganquan | 阅读 1290 | 回复 3 | 晴哈喜欢4.0于2021-3-12 21:52最后回复

2021-3-3发布

【安全快报】ADSafe病毒报毒该如何处理?

火绒运营专员 | 阅读 529 | 回复 2 | 2373924195于2021-3-12 15:09最后回复

4天前发布

2021-03微软漏洞通告

huoronganquan | 阅读 398 | 回复 0 | huoronganquan于2021-3-10 15:48最后回复

6天前发布

关于网传“火绒安全软件存在命令执行0-Day漏洞”的说明

huoronganquan | 阅读 1465 | 回复 5 | @huorong于2021-3-8 19:40最后回复

2021-3-5发布

发布新帖

问题反馈 | 病毒上报

热门版块

火绒安全软件5.0 | 用户规则分享

病毒查杀反馈 | 电脑问题解答

软件版本信息

当前版本 5.0.59.0 | 病毒库日期 2021-03-15

更新公告:

1. 扫描引擎病毒库(PROP)
2. 扫描引擎病毒库(PSET)
3. 扫描引擎病毒库(TRO)

官网下载

火绒小知识

浏览器保护对浏览器的支持(兼容)情况

查看详情

火绒安全论坛地址:

<https://bbs.huorong.cn/forum-62-1.html>

火绒恶性木马专杀工具下载地址:

<https://bbs.huorong.cn/thread-18575-1-1.html>

以上就是本次想和你分享的内容。

看完文章如果觉得对你有帮助的话，别忘了点击底部的「**点赞/在看**」鼓励一下我，谢谢。



微信搜一搜



效率工具指南