

# 银狐病毒查杀全教程

全盘查杀 + 专杀工具，手把手教你彻底清除

最近很多人电脑"越用越卡"、杀毒软件突然打不开、微信/QQ莫名自动发消息——很可能是中了"银狐"木马。它伪装成钉钉、WPS、微信、向日葵等常用软件的安装包，一旦运行就被远程控制、盗取账号密码，甚至成为勒索攻击的"跳板"。别慌！这篇教程按"先排查 → 再全盘杀 → 后专杀清底"的顺序，跟着点鼠标就能操作。

## 一、一分钟认识银狐木马

它怎么进你电脑的？记住三个常见入口：

- 1.仿冒软件官网：搜索"钉钉/WPS/微信下载"，点进了高仿钓鱼下载站；
- 2.群文件 / 陌生链接：微信、QQ 群里突然出现的"发票""通知""报税"文件；
- 3.钓鱼邮件附件：伪装成财税、工资单的可执行文件。

中招之后会发生什么？电脑被远程控制、浏览器和聊天软件账号密码被盗、屏幕被监控，木马还会继续"拉同伙"下载更多病毒。它的变种更新快、会把自己藏进系统进程，普通杀毒软件杀一遍经常杀不干净——可以按下面的流程来，杀毒更彻底。

## 二、第一步：快速排查（脚本扫描）

先用工具 **SilverFox-Scanner** 给电脑"把把脉"，专查银狐的典型痕迹：恶意进程、注册表/计划任务/服务等持久化项、杀毒软件被做的"排除项"、可疑网络连接。

工具下载：<https://pan.njfu.edu.cn/share/a139e138cc717f588914584c53>（仅作安全检测使用）

**Windows 用户三步走（不需要装任何软件）：**

**第 1 步：**右键点击“开始菜单”→选择“Windows PowerShell(管理员)”；

**第 2 步：**粘贴下面这行命令并回车（首次运行需要，允许脚本运行）：输入 Y 后回车

`Set-ExecutionPolicy RemoteSigned -Scope CurrentUser`

**第 3 步：**进入脚本所在目录，运行 `.\windows_scanner.ps1`，等待扫描完成。

**跑不起来？两个最常见的坑（实测都有）：**

**坑 1：**提示“未对文件进行数字签名”——GitHub 下载的本脚本自带“网络下载”标记，解除即可。在 PowerShell 里执行：

`Unblock-File .\windows_scanner.ps1`

**坑 2：**报一堆乱码语法错误——脚本是 UTF-8 编码，老版 PowerShell 按 GBK 误读导致。最简单的办法：改用 PowerShell 7 运行，或用记事本打开脚本 → 另存为时把编码选成“带 BOM 的 UTF-8”再运行。

**怎么看结果？**扫描结果里如果出现红色  标记的可疑项，说明有风险，继续按下面第二、三步处置；没有可疑项也不能大意，建议仍然做一次全盘杀毒兜底。

（正常项说明：系统自带的“SCM Event Log Filter”WMI 过滤器、Realtek 声卡启动项等都是正常组件，见到不必紧张；装了第

三方杀毒软件的电脑，最后一步查 Defender 排除项时会报 0x800106ba 错误，属杀软共存的正常现象。)

### 三、第二步：全盘杀毒

动手前，先做这 3 件事（很重要）：

1.先联网更新病毒库：把杀毒软件升级到最新，更新完立即断网（拔网线 / 关 Wi-Fi）。银狐是远控木马，断网才能掐断它的"遥控器"；

2.备份重要文件：文档资料复制到 U 盘 / 移动硬盘等离线介质，备份盘先杀毒再用；

3.一台电脑只留一款杀毒软件：多款杀软互相拦截反而杀不干净。已有 EDR 的学校电脑，用"EDR + 一款杀软"组合即可。

#### 方案 A：360 安全卫士

只从官网下载，不要用搜索结果里的第三方下载站——高仿下载站正是银狐的传播途径！

1.打开 360 → "木马查杀" → 先"快速扫描"，再"全盘扫描"；

2.扫描完成后点"立即处理"，到隔离区确认处理结果；

3.杀不掉的顽固木马：用 **360 系统急救箱**（官网下载）→ "全面扫描" → 勾选"强力模式"，必要时重启进安全模式再跑一次；

4.处理完重启电脑，再全盘扫一遍确认没有"复发"。

## 方案 B：火绒安全软件

官网下载。

1. 打开火绒主页 → 点"快速查杀"右侧的下拉箭头 → 选"全盘查杀";
2. 全盘查杀耗时较长，耐心等它跑完;
3. 对检出威胁点"处理"（清除 / 隔离），然后重启电脑;
4. 怀疑有残留：用"安全工具"里的安全分析工具排查进程、启动项和网络连接，再配合下面的专杀工具清底。

## 方案 C：学校 EDR 终端

1. 在 EDR 控制台对终端进行"全盘扫描"任务（我校终端：edr.njfu.edu.cn）;
2. 重点核实这几类告警：白加黑加载（合法程序带陌生 DLL）、svchost.exe 被注入、异常外联地址、可疑服务 / 注册表 / 计划任务;
3. 攻击还在持续时，先让把终端网络隔离，再溯源查其他受影响的电脑。

【学校 EDR】<https://mp.weixin.qq.com/s/YLVxxoI2FixocoOXNX4wsA>

## 四、第三步：银狐专杀工具深度清底

为什么全盘杀毒之后还要跑专杀？银狐变种更新太快，通用杀毒软件对最新变种和"母体"经常漏检。专杀工具专门针对银狐的行为特征，能把藏得更深的残留挖出来。两款任选或都跑一遍，双保险。

## 火绒银狐专杀 (HrKill)

●下载地址：<https://pan.njfu.edu.cn/share/4268df29acc5604a83cff80d05>

●用法：双击运行 → 一键扫描 → 按提示处理即可，无需安装。

## 深信服银狐专杀 (SFAKiller)

●下载地址：<https://pan.njfu.edu.cn/share/f5050b786daee01b968edd842e>

●用法：右键"以管理员身份运行" → 扫描 → 处理检出项

小提示：专杀工具偶尔会误报正常的安全软件组件，处理前看一眼文件路径和数字签名，别把杀软本体删了。下载专杀工具认准上面的官方地址。

## 五、收尾检查：别让木马"复活"

专杀跑完 ≠ 万事大吉，最后花 5 分钟做这几项检查：

1.重启 + 复扫：重启电脑后再用杀毒软件全盘扫一次，确认没有复发；

2.查启动项：按 Ctrl+Shift+Esc 打开任务管理器 → "启动"选项卡，把陌生条目禁用；再看看计划任务、系统服务里有没有不认识的项；

3.翻可疑目录：检查 C:\Users\你的用户名\AppData\Roaming、ProgramData、Temp 里的陌生程序；

4.看浏览器：主页、桌面快捷方式有没有被篡改；

5.改密码：用其他干净设备，重置微信、QQ、邮箱、网银

等重要账号密码；

6.通知同伴：检查接收过同一批文件的其他电脑，中毒期间在群里发过的消息要向群里说明；

7.终极方案：杀毒软件被木马专门关掉 / 卸载、怎么杀都杀不掉时，先用杀软官方急救箱处理；对抗性太强的样本，备份数据后重装系统最彻底。

## 六、日常防护：不给银狐留后门

- 不开来源不明的邮件附件、压缩包和可执行文件；
- 不点陌生链接、不扫来历不明的二维码；
- 关闭 Office 默认宏功能，打开陌生文档前先确认安全；
- 系统和杀毒软件病毒库保持最新；
- 服务器不用弱密码，关闭不必要的对外端口；
- 重要文件定期备份，记住 **3-2-1** 原则：3 份备份、2 种介质、1 份离线。

一句话总结：断网备份 → 开源脚本排查 → 杀软全盘杀 → 专杀工具清底 → 重启复扫改密码。五步走完，银狐无处遁形。