



**火绒安全**  
HUORONG SECURITY

# 火绒使用中常见问题处理

---

2020/07/06



公 司：北京火绒网络科技有限公司

地 址：北京市朝阳区红军营南路 15 号瑞普大厦 D 座 3 层

网 址：<https://www.huorong.cn>

电 话：400-998-3555

## 版权声明

本文件所有内容受中国著作权法等有关知识产权法保护，为北京火绒网络科技有限公司（以下简称“火绒安全”）所有，任何个人、机构未经“火绒安全”书面授权许可，均不得通过任何方式引用、复制。另外，“火绒安全”拥有随时修改本文件内容的权利。

如有修改，恕不另行通知。您可以咨询火绒官方、代理商等售后，获得最新文件。

## 目录

病毒问题 .....	4
勒索病毒 .....	4
感染型病毒 .....	5
挖矿病毒 .....	7
黑客工具 .....	8
广告程序 .....	9
非病毒问题 .....	10
漏洞扫描 .....	10
软件冲突 .....	13
其他问题 .....	13
蓝屏 .....	13
恶意网址拦截 .....	16
提交问题 .....	18

# 病毒问题

使用火绒进行查杀后，可能会发现以下企业内常见病毒，此节内容主要介绍此类常见病毒的传播、危害、识别方式。

## 勒索病毒

勒索病毒主要通过 RDP、钓鱼邮件、漏洞攻击等方式进行传播。勒索病毒成功运行后，会根据病毒内的规则，加密所有符合条件的文件。因勒索病毒多使用非对称加密算法，在没有获取到密钥的情况下无法解密，中毒后损失较大。

此类病毒被火绒查杀时，报毒名称为 Ransom/病毒名。

需要注意的是以 RDP 弱口令为主要传播方式的勒索病毒，黑客在获取到 Windows 账户的密码后，通过“远程桌面”登录到企业内，在成功登陆后，会寻找高价值服务器(文件服务器、OA、业务服务器、数据库)，加密其中文件进行勒索。

火绒企业版对该传播方式有额外的防护措施，但除了部署安全软件，您也可以按照我们提供的《部署火绒后的安全加固建议》文档，对火绒和 Windows 进行有针对性的配置，以提高安全性。



## 感染型病毒

感染型病毒是企业内常见病毒，此类病毒多会感染可执行文件，导致在用户在使用被感染的软件时，病毒会先运行，以达到在系统内常驻的目的，并会通过可移动设备，文件共享等渠道传播。

此类病毒被火绒查杀时，报毒名称为“Virus/病毒名”，例如“Virus/Ramnit”、“Virus/Sality”等。

发现此类病毒后，需要进行全盘查杀，查杀前修改火绒扫描时机(监控级别)，全盘扫描时尽量不要运行其他程序。



在处理病毒时，如该文件为被感染程序，火绒会清除文件内的病毒代码，修复该文件，如文件是病毒本体、被感染导致文件损坏、无法写入等情况，火绒会删除该文件(文件在 C:\windows 目录下，如文件无法清除需要删除，为了保持系统稳定，火绒不会主动删除文件该文件，日志内会显示处理失败)，如不确认是否可以清除，可与我们联系帮您进行判定。



## 挖矿病毒

挖矿病毒已经是企业内最常见的病毒之一，此类病毒运行时大量占用系统资源，影响企业内的业务，妨碍员工办公。挖矿病毒的传播方式较多，企业内常见的传播方式有内网横向传播、软件安装包携带、黑客入侵投放等。

火绒查杀到此类病毒时，报毒名称多为“Trojan/挖矿程序名”，例如“Trojan/CoinMiner”、“Trojan/JS.CoinMiner”。正常情况下，电脑内发现此类病毒只需要用火绒终端扫描查杀即可，在查杀结束后需要重启。

因挖矿病毒多会携带其他模块，例如利用永恒之蓝进行传播的模块等，所以在查杀挖矿病毒时，除了挖矿组件外，还可能会查杀到报毒名为“Exploit/EquationDrug”或“HackTool/EquationDrug”的其他功能模块。





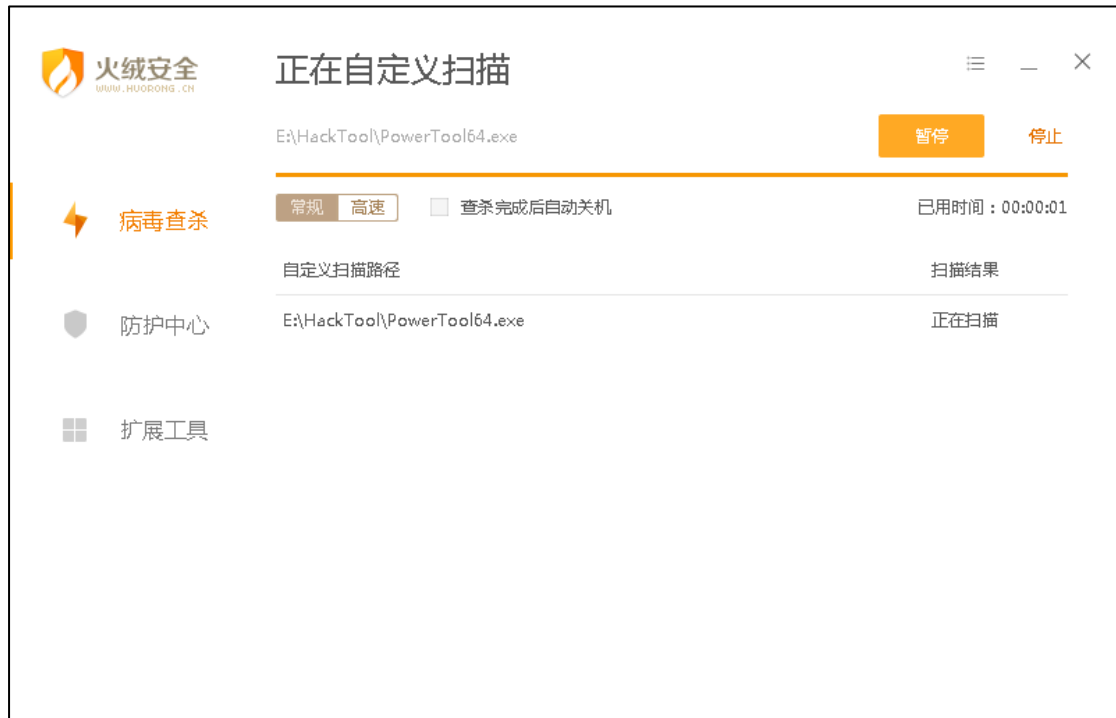
## 黑客工具

火绒对黑客工具的定义为“可以被黑客利用, 用来控制用户计算机或发起网络攻击的工具程序”, 包括挖矿工具、端口扫描工具、ARK 工具、远程控制工具等。

在查杀到此类程序时, 火绒的报毒名称多为“ HackTool/ 工具名”, 例如“ HackTool/PowerTool.a”、“ HackTool/PortScan.a”等, 在企业环境内, 发现此类工具多是遭受攻击, 黑客试图使用此类工具继续对内网进行渗透时被火绒拦截。

在企业内查杀到此类工具, 如并非为企业内常用工具或运维人员所用工具, 需及时进行排查, 对所查杀工具的来源与作用进行确认。也可直接与火绒安全进行联系, 协助您进行排查。





## 广告程序

广告程序会通过多种途径进入系统，多为未经用户允许便进行安装(捆绑安装携带、软件自身的广告组件等)。

运行时多会通过弹出式广告、劫持浏览器主页、暗刷等方式盈利，对用户日常的电脑使用，办公等造成影响。此类程序被火绒查杀时，报毒名称为“ Adware/名称”，例如“ Adware/FakeAV.ks”、“ Adware/PuddingZip.g”等。火绒在查杀此类程序时，只会处理该程序的广告模块，不会影响该程序的正常使用，但是会出现该软件升级时，将广告模块恢复的情况，会导致火绒对此文件频繁查杀。出现此类情况时，如该软件需要继续使用，建议您将相关文件添加到白名单，如此程序并非您主动安装(捆绑)，或不需要使用，建议您进行卸载。

对于软件的弹窗广告，火绒提供了安全工具“ 弹窗拦截”，可阻止此类窗口出现。



## 非病毒问题

### 漏洞扫描

使用火绒“漏洞修复”功能，扫描并修复 Windows 漏洞时，可能因为多种原因导致补丁下载或安装失败，该小节内容为常见的“漏洞修复”问题与处理办法。

#### 1、火绒“漏洞修复”扫描出的补丁数量，与“Windows Update”提供的补丁数量不一致

火绒默认不推送部分功能性补丁，例如 IE 跨版本升级(如 IE10 升级到 IE11)、.Net 跨版本升级、语言包等，除减少了功能性补丁外，微软提供的补丁部分存在包含与替代关系，火绒会根据测试后的情况，调整规则库，在高危漏洞全部安装的情况下，调整被替代的补丁推送，所以会比系统推送的补丁数量少。

#### 2、补丁“下载失败”



此问题多为网络环境异常导致，如需要安装补丁的电脑可以访问网络，可以尝试 ping 以下地址：

download.windowsupdate.com

download.microsoft.com

如无法 ping 通，需要排查网络是否存在故障，若网络环境无异常依旧下载失败，可联系火绒协助您排查该问题。

需要修复漏洞的电脑是内网，无法于微软服务器下载补丁，此时需要检查“火绒中心”是否能够连接互联网。

在火绒中心可以访问网络的情况下，需要修改“火绒中心->漏洞修复”功能设置，勾选从中心下载补丁。





火绒中心也部署在内网的情况下，需要使用“离线升级工具”，相关使用方法可以查看使用文档。



### 3、补丁“安装失败”

出现补丁“安装失败”的情况，多为系统环境内，更新相关环境、组件、服务出现异常。

当您出现此类问题时,可与我们联系,帮您找到补丁安装失败的原因,并提供解决方案。

## 软件冲突

### a).透明加密软件

企业内在使用透明加密软件(防泄密程序)时,常会遇到宏病毒在扫描时不报毒,打开文件时火绒提示存在宏病毒。

出现此问题的原因为,安装防泄密软件后,被保护的文档内容被加密,只有使用防泄密软件允许的打开程序(Office Word、WPS 等)该文件,或事先使用该软件解密文件内容后,文档内容才可以被其他软件正常访问。

当您遇到此类问题时,如该防泄密软件有白名单功能,可先将火绒目录下的可执行程序添加到白名单(HipsDaemon.exe\HipsMain.exe\HipsTray.exe)后,再次扫描查看问题是否解决。

如该防泄密程序没有白名单功能,或添加白名单后依旧无法正常进行扫描,可联系防泄密程序厂商与火绒安全,共同解决此问题。

## 其他问题

### 蓝屏

火绒使用过程中出现蓝屏问题时,需要提取该电脑上的蓝屏 dump 并上传,我们会帮您分析

#### 蓝屏原因

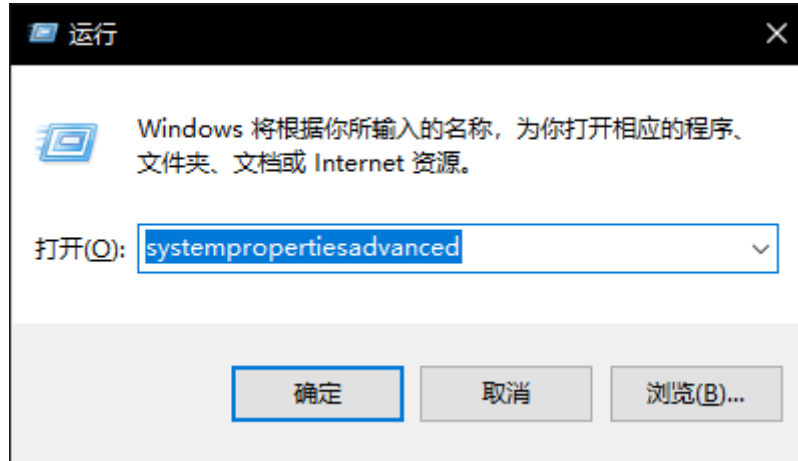
dump 文件位置:

%SystemRoot%\Memory.dmp

%SystemRoot%\Minidump\*.dmp(根据日期命名)

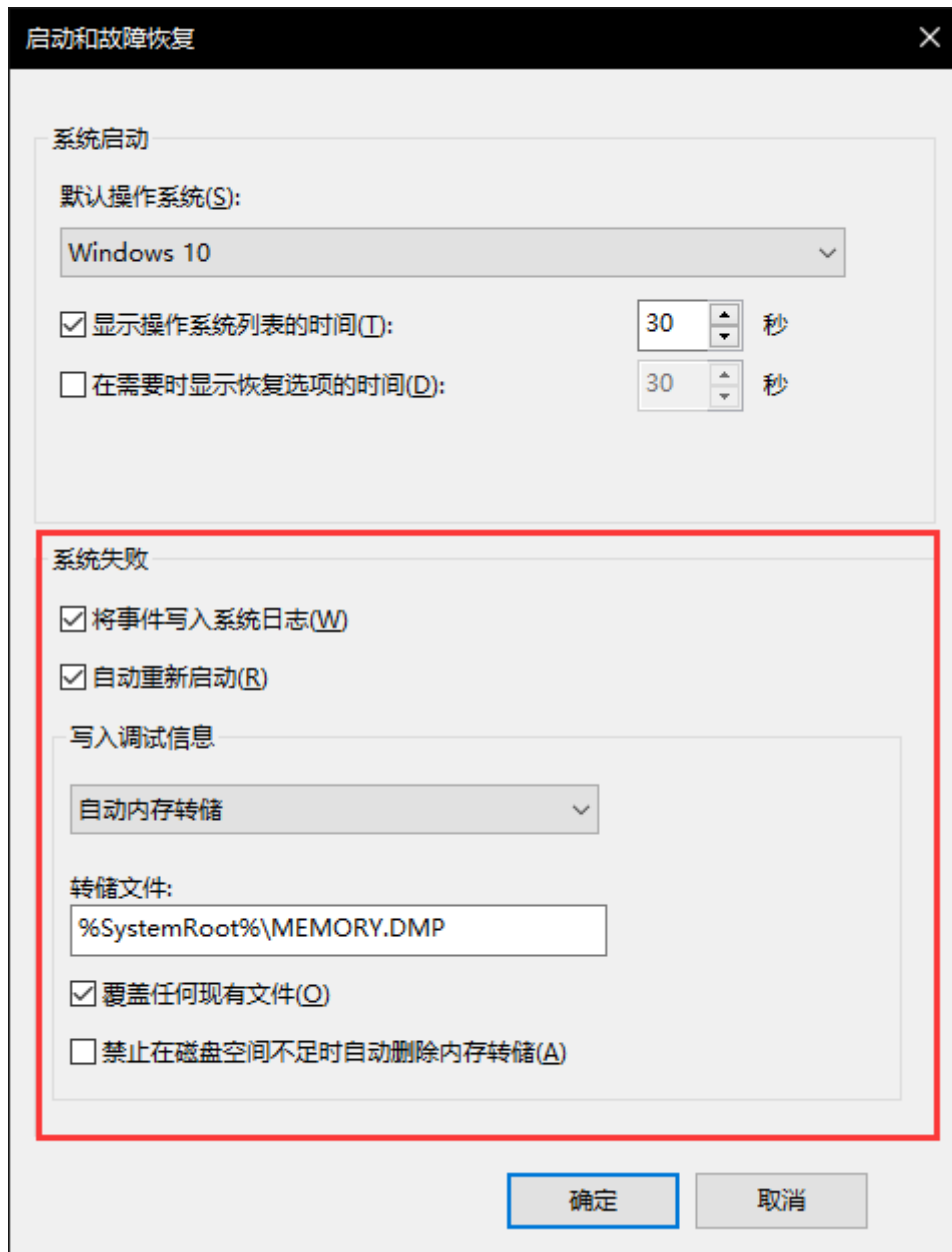
如此目录下没有发现相关文件,可以检查以下设置。

打开运行,输入“systempropertiesadvanced”,打开“高级系统设置”。



点击“高级->启动和故障恢复->设置”，按照图片进行设置。如没有“自动内存转储”选项，可根据需求选择“核心内存转储(推荐)”、“最小内存转储”、“完全内存转储”。





## 恶意网址拦截

火绒终端部署后，根据局域网内状况不同，可能会出现大量“恶意网址拦截日志”，此小节列出企业内较常见的被拦截网址，并提供解决方案。

- kuaizip.com
- kpzip.com

出现以上网址的拦截，是因您电脑中安装了快压导致，可根据您的需求选择是否继续使用或



卸载该软件。

相关报告:[知名压缩软件“快压”传播病毒和多款流氓软件 劫持流量](#)

- down.sgshurufa.com
- down.znshuru.com
- downsrfeastday.com
- d.wn51.com
- down.shusw.com
- chlbiz.com

出现以上网址的拦截，是因您电脑中安装了布丁系软件导致。

- Clover
- 东方浏览器
- 东方输入法
- 东方头条
- 万能浏览器
- 万能看图
- 万能五笔
- 智能云五笔输入法
- 智能云输入法
- 补丁压缩
- 补丁桌面
- 水果输入法

可根据您的需求选择是否继续使用或卸载该软件，此类软件在卸载后有残留服务访问以上

网址，重新安装软件的行为，如您电脑上未发现此系列软件但依旧存在“恶意网址拦截”日志，可联系我们帮您进行排查。

相关报告:[灰色产业链成病毒传播最大渠道 流量生意或迎来最后的疯狂](#)

- haqo.net
- beahh.com
- abbny.com
- zer2.com
- ackng.com
- awcna.com
- amxy.com

出现以上网址的拦截，是因您电脑中存在 DTStealer 木马导致，除了拦截网址访问，可能会同时出现“隐藏执行 PowerShell”等拦截日志，关于此病毒只需使用火绒全盘查杀，重启即可。

相关报告: [“驱动人生”利用高危漏洞传播病毒 12月14日半天感染数万台电脑](#)

## 提交问题

如果您遇到以下情况:

- 网络内发现可疑文件，想要提供给我们进行分析。
- 系统出现异常，但是不方便我们远程进行协助。

您可以按照以下方式提交相关信息，我们会根据您的信息与提供的信息做出相应解决方案。

病毒问题

需要您提交以下信息:

- 问题详情

- 火绒中心日志(包括《病毒防御日志》《系统防御日志》《网络防御日志》, 时间为 30 天)。
- 报毒终端日志。
- 报毒终端版本、病毒库版本。
- 需要我们进行分析的样本、隔离区内提取的样本。