

《“挖矿”木马检测及处置参考手册》

虚拟货币“挖矿”活动指通过计算机设备获取虚拟货币的过程，需借助设备高速运转，消耗大量电力和算力资源。国家已经明确其为高耗能的淘汰类产业，虚拟货币相关业务活动属于非法金融活动。虚拟货币活动常伴随安全问题，不法分子通过大量植入“挖矿”木马病毒，控制受害者计算机进行虚拟货币“挖矿”牟利，对计算机及网络安全构成严重威胁。

挖矿木马病毒具备传播性，可在内网电脑之间传播，会对未及时更新操作系统补丁及未安装安全软件的电脑造成危害。出现计算机CPU利用率飙高（时间段可能是非工作时间）、网速明显变慢等现象，需要引起高度重视，及时进行病毒查杀。

● 下载并安装病毒防护软件或“挖矿病毒巡检工具”进行查杀

在计算机中安装病毒查杀软件（如金山毒霸 www.iijinshan.com、360 安全卫士 www.360.cn、火绒安全 www.huorong.cn 等），并及时更新病毒查杀软件的病毒库，还需做好定时全盘查杀病毒。如果计算机中有存在挖矿木马的样本程序，杀毒软件一般情况下是可以查杀的。

“挖矿病毒巡检工具”：

https://edr.sangfor.com.cn/#/introduction/all_tools

- 日常安全防护：关闭 Windows 共享服务，远程桌面控制等不必要的服务，关闭高危端口(135、136、137、138、139、445、3333、4444、5555、8220)，参考以下方法：

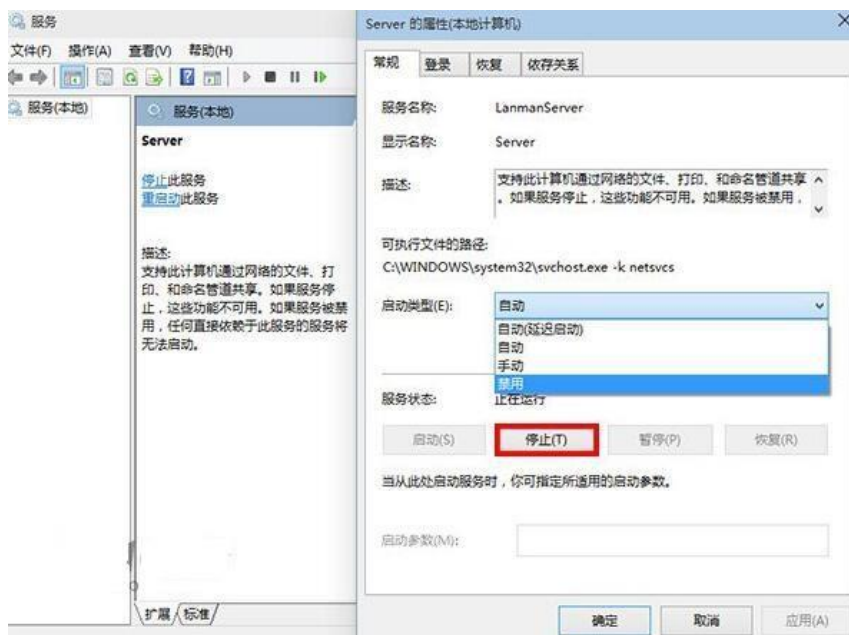
【关闭共享 Server 服务】

方法 1：在 Windows 服务中关闭

①在运行、任务管理器或 Cortana 搜索栏（Win10）/开始菜单搜索栏（Win7）/开始屏幕搜索栏（Win8.1）输入 services.msc 后回车，打开“服务”。

②找到 Server，双击打开。

③在“启动类型”中选择“禁用”，然后在“服务状态”点击“停止”后确定。



这种方法能够关闭管理共享，不过对于需要开启打印和传真等共享和某些文件共享的用户来说，这种方式有些“矫枉过正”。后面方式更适合这部分用户。

方法 2：在注册表中关闭“管理共享”

虽然是在注册表中操作，但这种方法其实并不费事，不过最好在修改前备份一下注册表，以防修改错误导致不必要的麻烦。具体方法如下：

①在运行、任务管理器或 Cortana 搜索栏（Win10）/开始菜单搜索栏（Win7）/开始屏幕搜索栏（Win8.1）输入 regedit 后回车，打开注册表编辑器。

②定位到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

③新建 DWORD（32 位）值，重命名为 AutoShareWks，并将其数值数据设置为“0”确定。

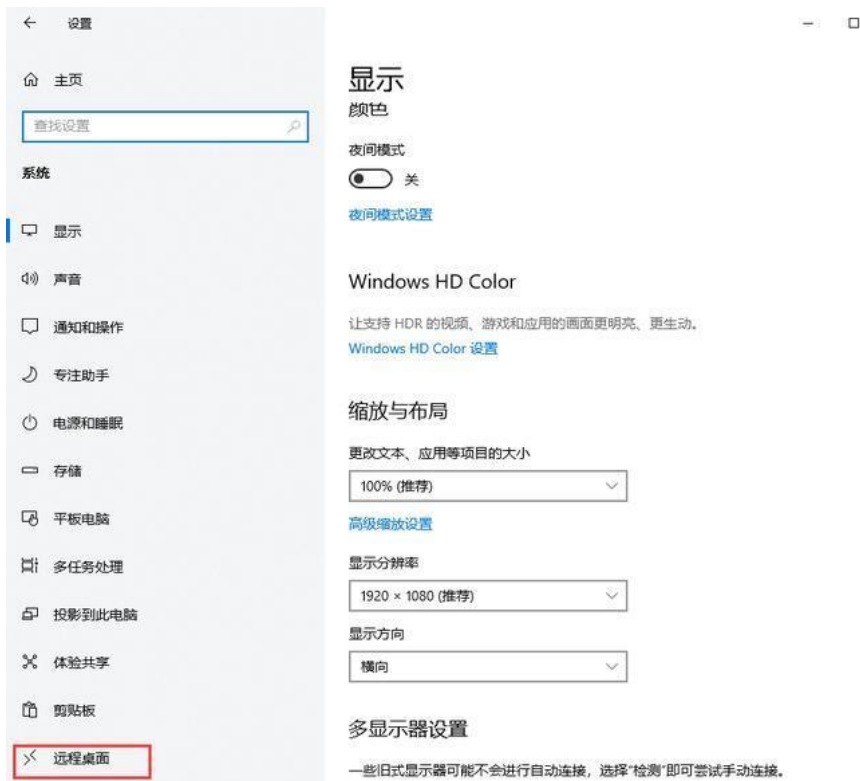
【关闭远程桌面】

①在 Windows 电脑左下角点击开始菜单，进入设置控制面板。

②在 Windows 设置内找到【系统】并进入。



③在系统设置内找到【远程桌面】并进入。



④进入远程桌面后，将已开启允许启用远程桌面的功能关闭。



⑤关闭远程桌面后，将禁止其他设备远程连接这台电脑。

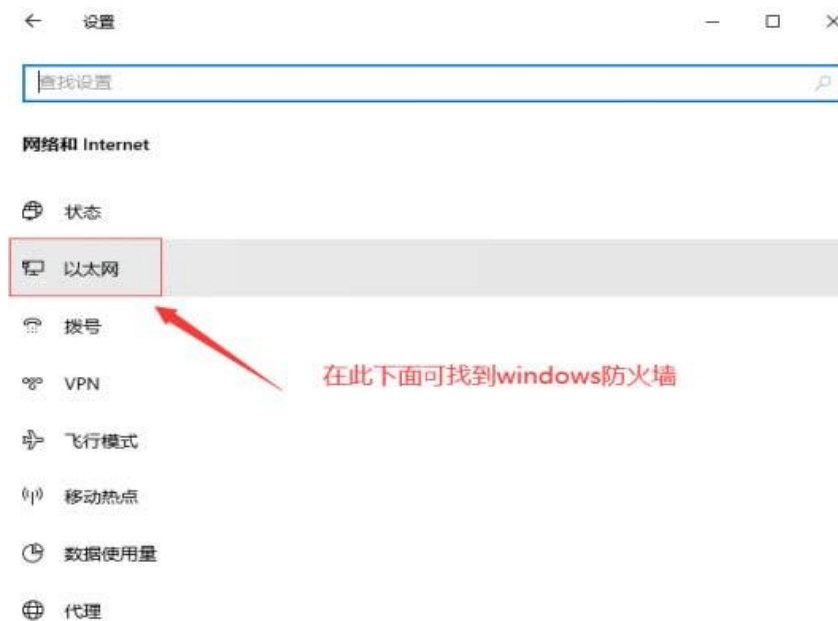
【关闭高危恶意端口】

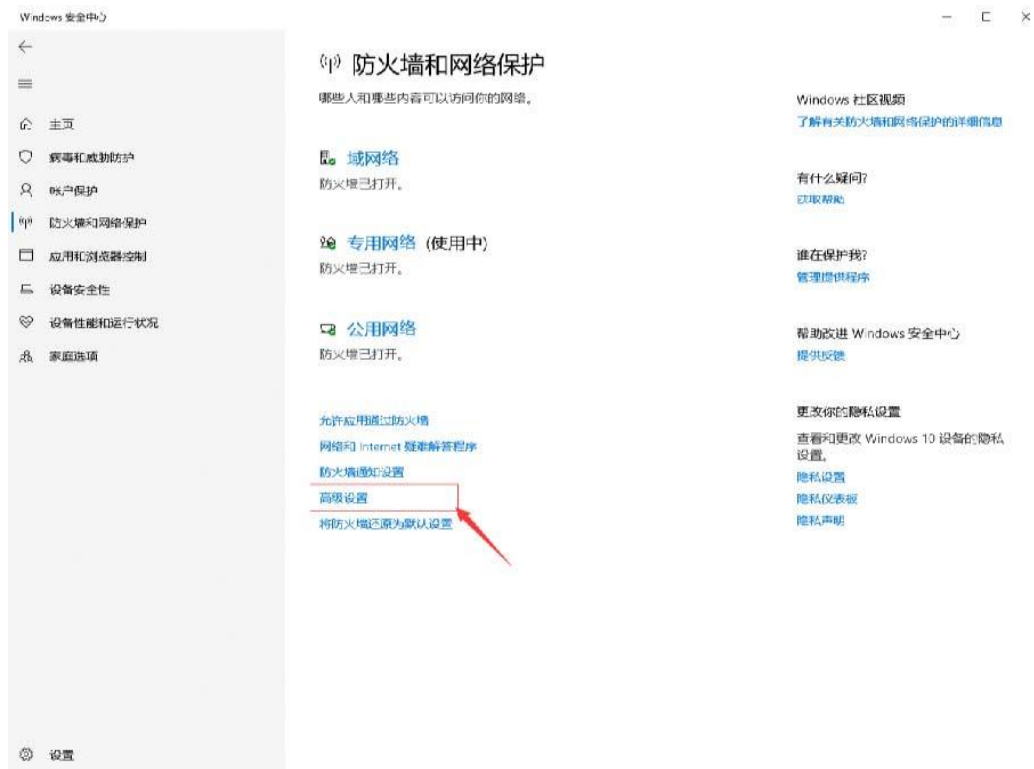
①在 Windows 电脑左下角点击开始菜单，进入设置控制面板。

②在 Windows 设置内找到【网络和 Internet】并进入。

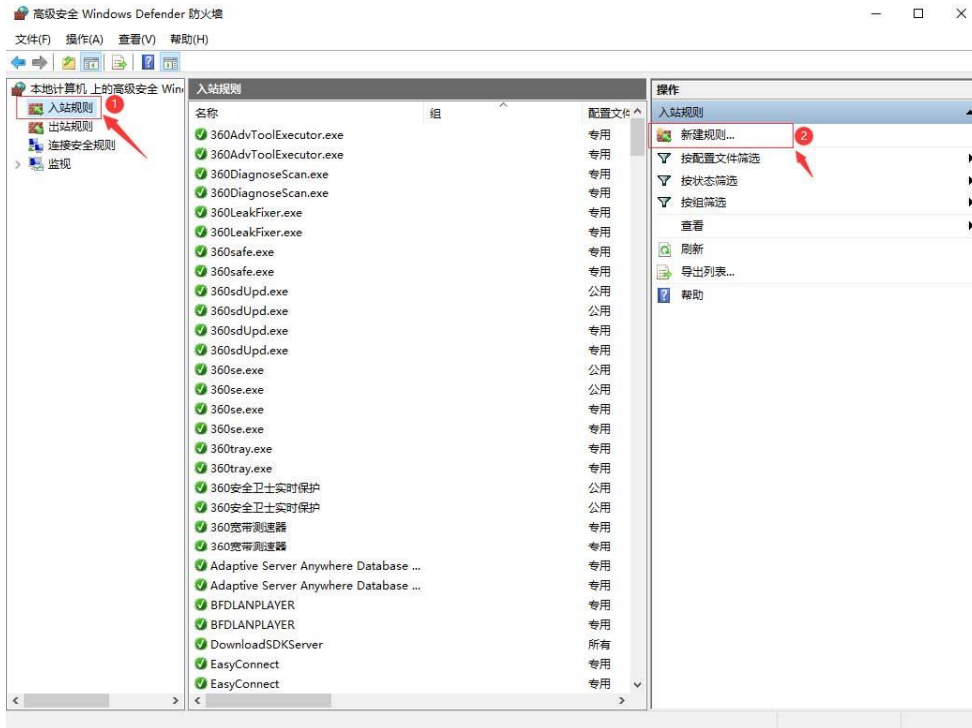


③找到【Windows 防火墙】，进入高级设置。





④点击进站规则，新建规则。



⑤关闭高危端口(135、136、137、138、139、445、3333、4444、5555、8220)。

协议和端口

指定应用此规则的协议和端口。

步骤:

- 规则类型
- 协议和端口
- 操作
- 配置文件
- 名称

此规则应用于 TCP 还是 UDP?

- TCP
- UDP

此规则应用于所有本地端口还是特定的本地端口?

- 所有本地端口(A)
- 特定本地端口(S): 135-139, 445, 3333, 4444, 5555, 8220
示例: 80, 443, 5000-5010

135-139,445,3333,4444,5555,8220

< 上一步(B) 下一步(N) > 取消

操作

指定在连接与规则中指定的条件相匹配时要执行的操作。

步骤:

- 规则类型
- 协议和端口
- 操作
- 配置文件
- 名称

连接符合指定条件时应该进行什么操作?

- 允许连接(A)
包括使用 IPsec 保护的连接, 以及未使用 IPsec 保护的连接。
- 只允许安全连接(C)
只包括使用 IPsec 进行身份验证的连接。连接的安全性将依照 IPsec 属性中的设置以及“连接安全规则”节点中的规则受到保障。

自定义

- 阻止连接(K)

< 上一步(B) 下一步(N) > 取消



高级安全 Windows Defender 防火墙

文件(F) 操作(A) 查看(V) 帮助(H)

本地计算机上的高级安全 Windows Defender 防火墙

入站规则

名称	组	配置文件	已启用	操作	替代
高危端口		所有	是	阻止	否
360AdvToolExecutor.exe		专用	是	允许	否
360AdvToolExecutor.exe		专用	是	允许	否
360DiagnoseScan.exe		专用	是	允许	否
360DiagnoseScan.exe		专用	是	允许	否
360LeakFixer.exe		专用	是	允许	否
360LeakFixer.exe		专用	是	允许	否
360safe.exe		专用	是	允许	否
360safe.exe		专用	是	允许	否
360sdUpd.exe		公用	是	允许	否
360sdUpd.exe		公用	是	允许	否
360sdUpd.exe		专用	是	允许	否
360sdUpd.exe		专用	是	允许	否
360se.exe		公用	是	允许	否
360se.exe		公用	是	允许	否
360se.exe		专用	是	允许	否
360se.exe		专用	是	允许	否
360tray.exe		专用	是	允许	否
360tray.exe		专用	是	允许	否
360安全卫士实时保护		公用	是	允许	否
360安全卫士实时保护		公用	是	允许	否
360宽带测速器		专用	是	允许	否
360宽带测速器		专用	是	允许	否
Adaptive Server Anywhere Database ...		专用	是	允许	否
Adaptive Server Anywhere Database ...		专用	是	允许	否
BFDLANPLAYER		专用	是	允许	否
BFDLANPLAYER		专用	是	允许	否
DownloadSDKServer		所有	是	允许	否
EasyConnect		专用	是	允许	否

操作

- 入站规则
- 新建规则...
- 按配置文件筛选
- 按状态筛选
- 按组筛选
- 查看
- 刷新
- 导出列表...
- 帮助
- 高危端口
- 禁用规则
- 剪切
- 复制
- 删除
- 属性
- 帮助