勒索病毒防范紧急处置手册（Win7）

（2017-5-14 版本 1.1）

信息中心信息安全事件 7x24 小时帮助热线

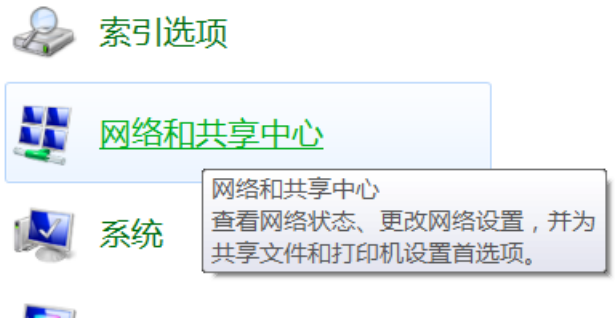
6011050，3176928(明向)

处置流程

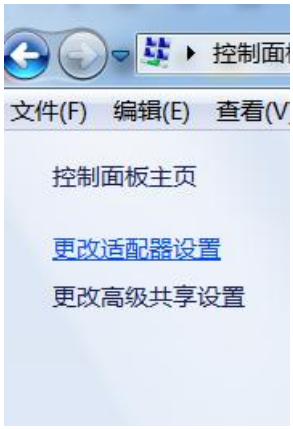
1. 在开机之前，严禁接入网络。首先拔掉网线，笔记本电脑关闭无线网络开关。
2. 加电启动 Windows 系统。
3. 关闭文件与打印机共享服务。操作步骤如下：

点击“控制面板”

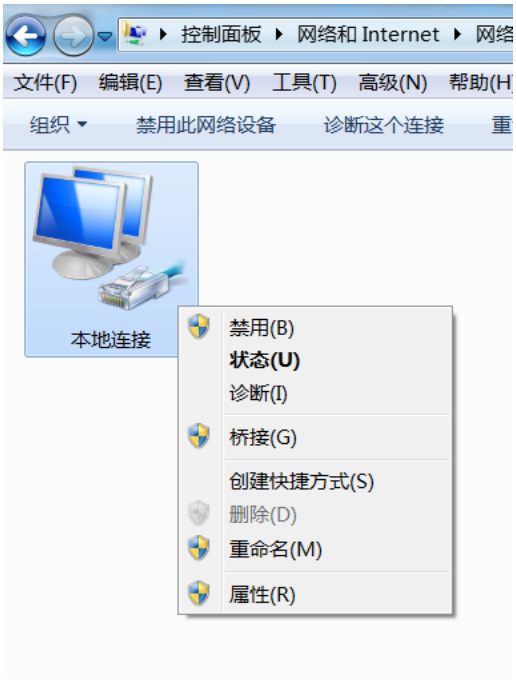
选择“大图标”



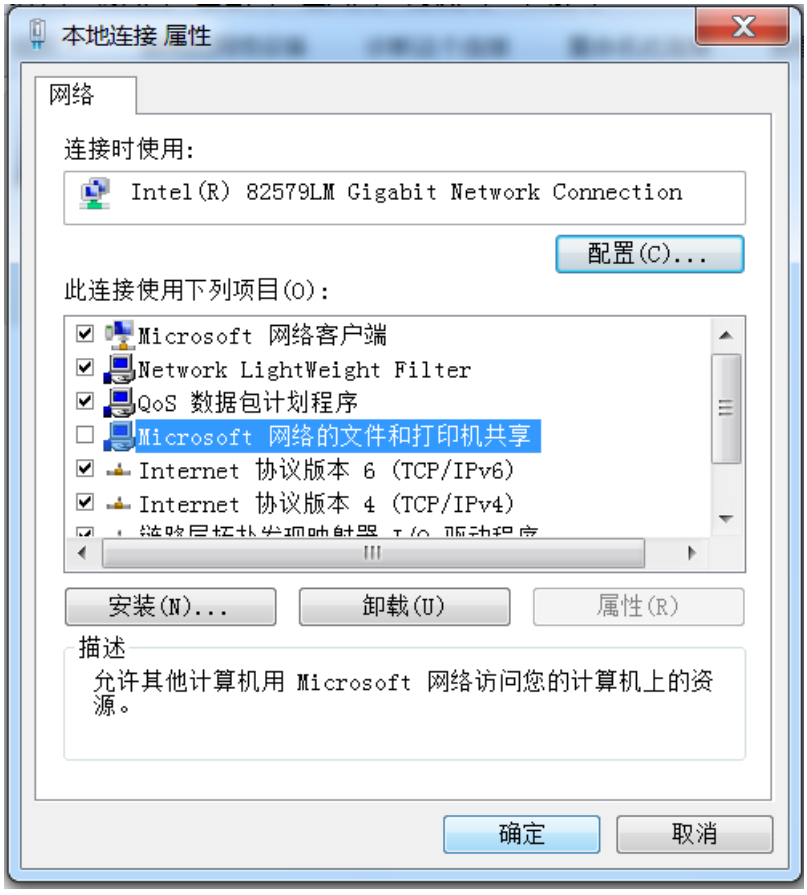
点击“网络与共享中心”



点击“更改适配器设置”



在“本地连接”上点击右键，选择“属性”



取消“Mircosoft 网络的文件与打印机共享”前面的对勾，然后点击“确定”。

4. 启用防火墙并关闭 445 端口。操作步骤如下：

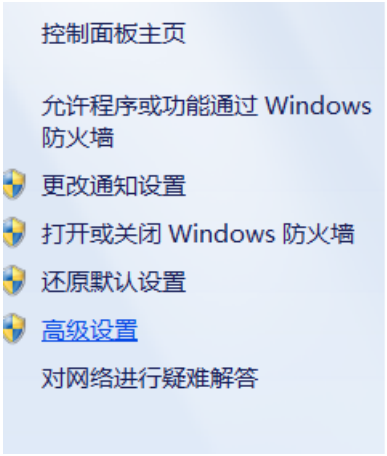
点击“控制面板”

选择“大图标”

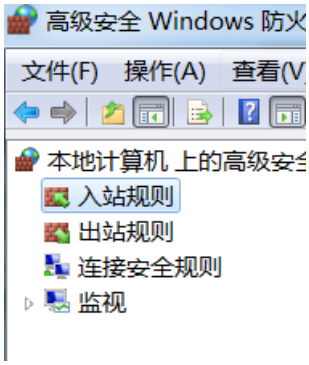
点击“Windows 防火墙”

选择“打开或关闭 Windows 防护墙”

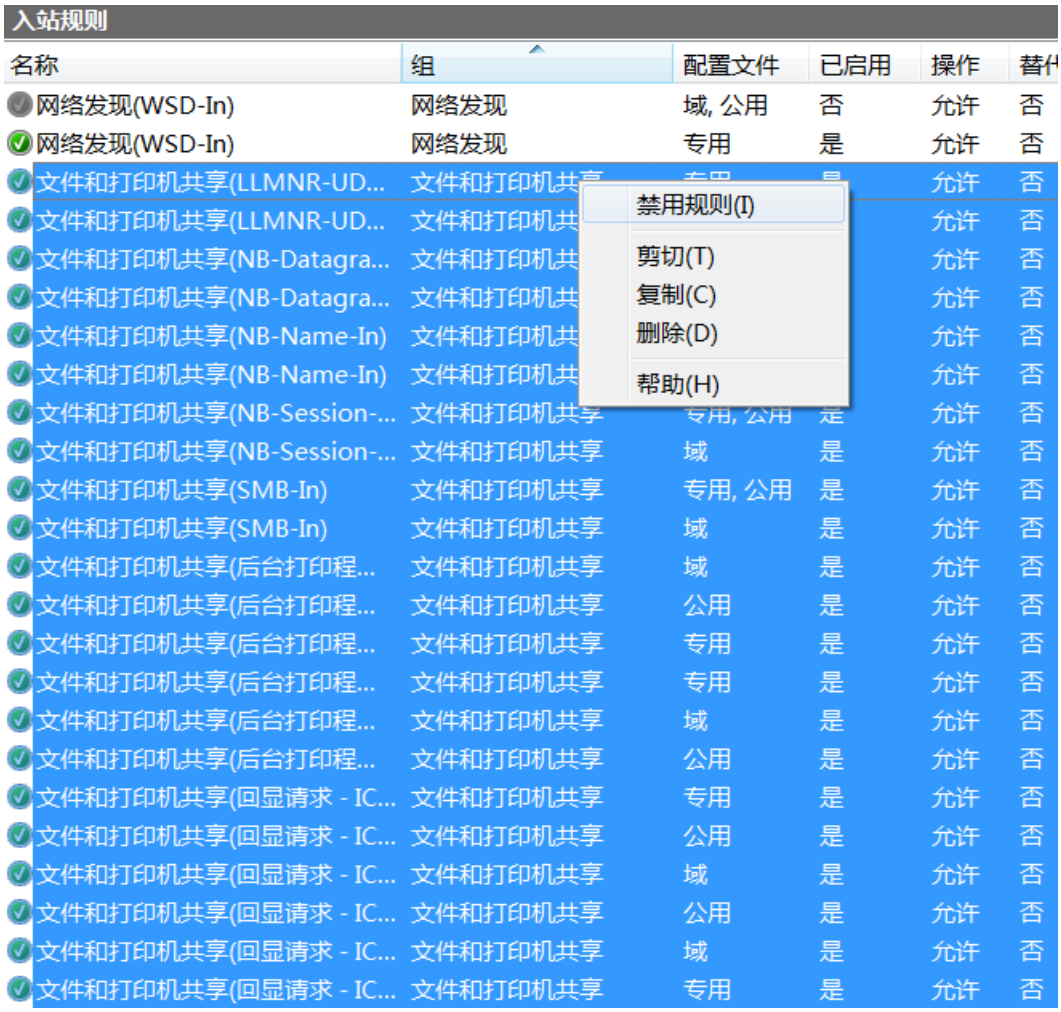
选择“启用 windows 防火墙”，点击“确定”



点击“高级设置”



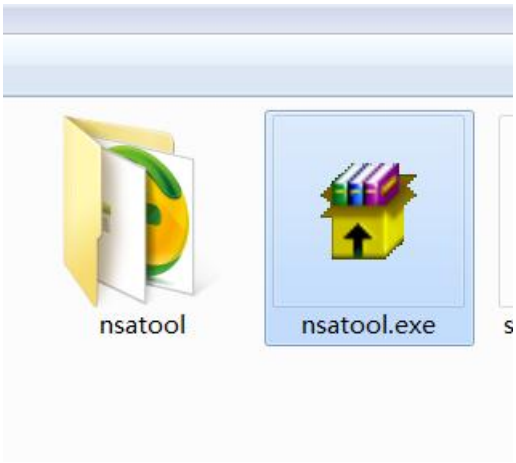
点击“入站规则”



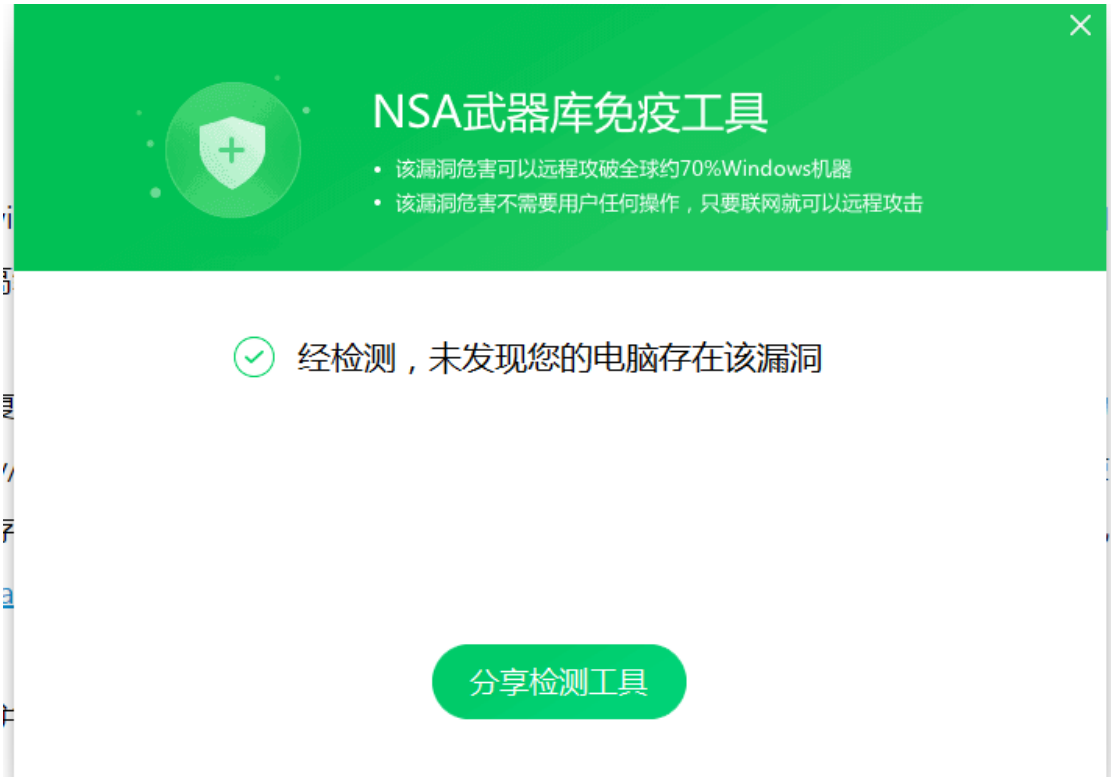
在右侧的列表中找到所有的“文件和打印机共享”,按 shift 键，选择所有的“文件和打印机共享”，在上面点击右键选择“禁用规则”，使规则前的图标变为灰色。

5. 插入网线或者连接无线网络。

6. 下载并安装补丁。从 http://dl.360safe.com/nsa/nsatool.exe （120MB 左右）下载补丁并安装，安装完后，重新启动计算机，待补丁生效。



下载后运行补丁文件为 nsatool.exe，双击运行该文件。



大约 10~15 分钟后，补丁安装完成。重新启动计算机，待补丁生效。

6. 处置完成，可以使用计算机和网络。