上网终端计算机防范勒索病毒技巧

一、仅使用Windows操作系统的电脑用户可以执行下面操作。

1. 断开网络开机

拔掉网线，开机启动电脑。如果Windows启动后自动连接了无线网络，请第一时间断开无线网络连接。

1. 检查是否已感染病毒

依次检查C盘、D盘、“我的文档”文件夹和其他保存重要文件的文件夹，查看是否有文件名末尾带有“.onion”、“.wannacry”字样或近似字样。如果有说明您的电脑已感染病毒，后续处理方法见“已感染病毒Windows系统重装操作步骤”。如果没感染病毒，请继续下面步骤。

1. 备份重要文件数据

插入U盘/移动硬盘等存储介质（最好是空白的或不含重要文件的），将电脑中的重要文件拷贝到U盘/移动硬盘上。拷贝完后拔下U盘/移动硬盘。

1. 临时禁用445端口

以管理员身份运行cmd命令行程序("C:\命令提示符"程序)(适合win7/8/10系统)，在DOS提示符后执行下面命令：

***netsh advfirewall firewall add rule name="deny445" dir=in protocol=tcp localport=445 action=block***

执行成功会显示“确定。”

1. 插好网线，恢复网络连接
2. 打windows系统补丁

手工执行windows自带的“windows update”打补丁。

**离线补丁下载链接**

**winxp特别补丁KB4012598**

winxp3 32位 Security Update for Windows XP SP3 (KB4012598)

http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-chs\_dca9b5adddad778cfd4b7349ff54b51677f36775.exe

winxp2 64位 Security Update for Windows XP SP2 for x64-based Systems (KB4012598)

http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-enu\_f24d8723f246145524b9030e4752c96430981211.exe

**win2003特别补丁KB4012598**

2003SP2 32位 Security Update for Windows Server 2003 (KB4012598)

http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x86-custom-chs\_b45d2d8c83583053d37b20edf5f041ecede54b80.exe

2003SP2 64位 Security Update for Windows Server 2003 for x64-based Systems (KB4012598)

http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-chs\_68a2895db36e911af59c2ee133baee8de11316b9.exe

**win2008R2补丁 KB4012212、KB4012215**

March, 2017 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB4012212)

http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64\_2decefaa02e2058dcd965702509a992d8c4e92b3.msu

March, 2017 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4012215)

http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows6.1-kb4012215-x64\_a777b8c251dcd8378ecdafa81aefbe7f9009c72b.msu

**win7补丁 KB4012212、KB4012215**

win7 32位

March, 2017 Security Only Quality Update for Windows 7 (KB4012212)

http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x86\_6bb04d3971bb58ae4bac44219e7169812914df3f.msu

March, 2017 Security Monthly Quality Rollup for Windows 7 (KB4012215)

http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/03/windows6.1-kb4012215-x86\_e5918381cef63f171a74418f12143dabe5561a66.msu

win7 64位

March, 2017 Security Only Quality Update for Windows 7 for x64-based Systems (KB4012212)

http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64\_2decefaa02e2058dcd965702509a992d8c4e92b3.msu

March, 2017 Security Monthly Quality Rollup for Windows 7 for x64-based Systems (KB4012215)

http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows6.1-kb4012215-x64\_a777b8c251dcd8378ecdafa81aefbe7f9009c72b.msu

**win10 1607补丁 KB4013429**

win10 1607 32位

Cumulative Update for Windows 10 Version 1607 (KB4013429)

http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4013429-x86\_8b376e3d0bff862d803404902c4191587afbf065.msu

win10 1607 64位

Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB4013429)

http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/03/windows10.0-kb4013429-x64\_ddc8596f88577ab739cade1d365956a74598e710.msu

**win2012R2补丁 KB4012213、KB4012216**

March, 2017 Security Only Quality Update for Windows Server 2012 R2 (KB4012213)

http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8.1-kb4012213-x64\_5b24b9ca5a123a844ed793e0f2be974148520349.msu

March, 2017 Security Monthly Quality Rollup for Windows Server 2012 R2 (KB4012216)

http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/03/windows8.1-kb4012216-x64\_cd5e0a62e602176f0078778548796e2d47cfa15b.msu

**win2016补丁 KB4013429**

Cumulative Update for Windows Server 2016 for x64-based Systems (KB4013429)

http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/03/windows10.0-kb4013429-x64\_ddc8596f88577ab739cade1d365956a74598e710.msu

1. 启用445端口

（如果您从来不用“文件和打印机共享”、“网上邻居”等功能，建议省略本步操作，一直禁用445端口。）

以管理员身份运行cmd命令行程序("C:\命令提示符"程序)(适合win7/8/10系统)，在DOS提示符后执行下面命令：

***netsh advfirewall firewall delete rule name="deny445" dir=in protocol=tcp localport=445***

执行成功会显示“已删除1规则。确定。”

特别提醒：个别电脑打完windows系统补丁后可能会出现蓝屏无法启动的情况，这是windows补丁程序兼容性的问题。

二：各类操作系统防火墙规则启用方法

Windows XP操作系统防火墙规则启用方法：

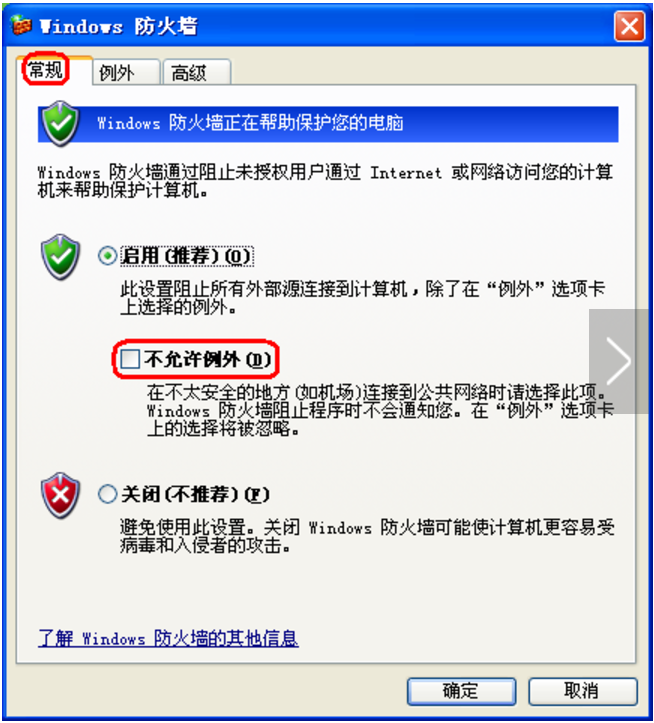
1. 点击 开始-控制面板-安全中心



1. 点击 Windows防火墙



1. 点击【常规】选项卡

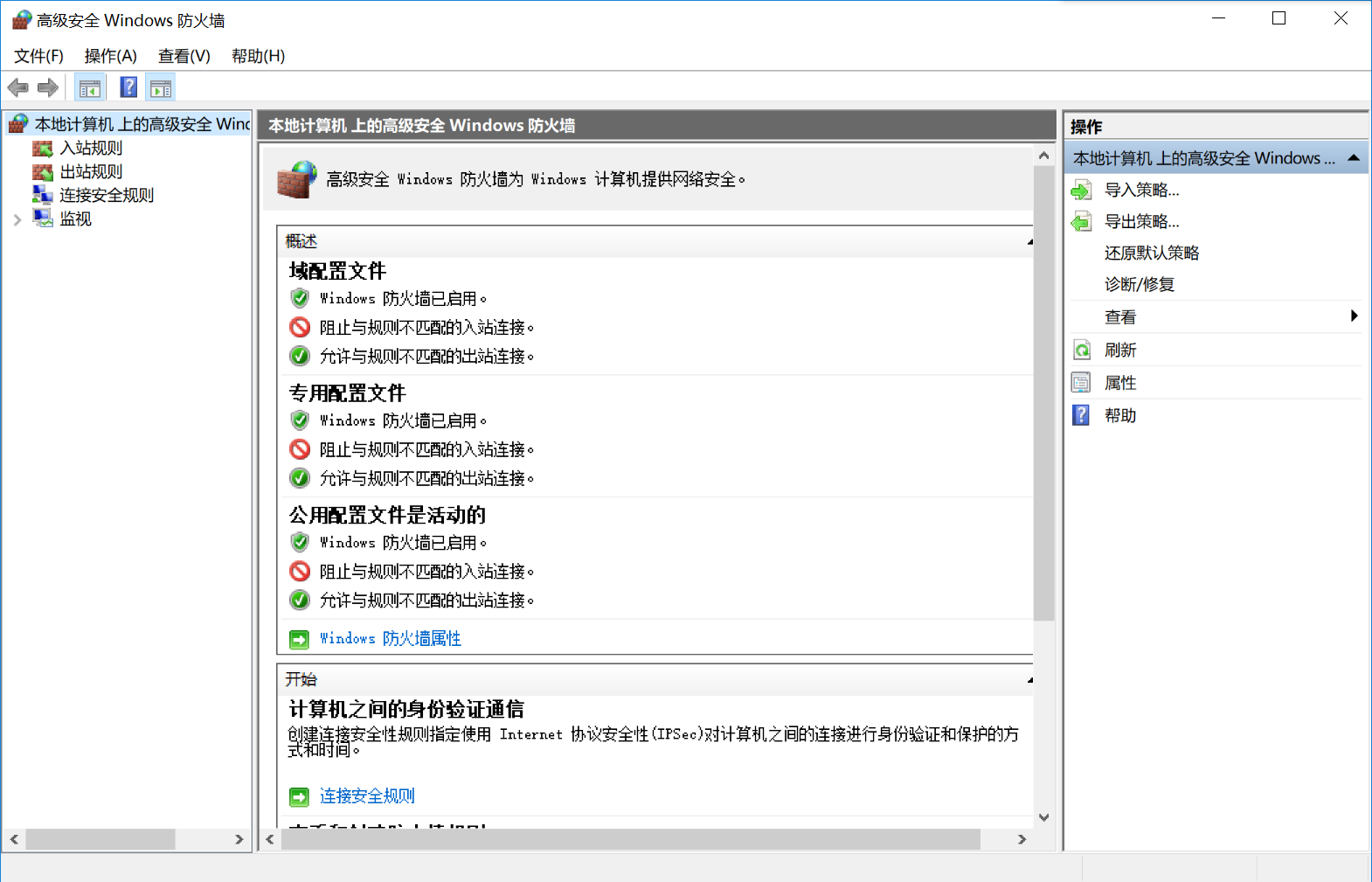


1. 点击【例外】选项卡，取消【文件和打印机共享】

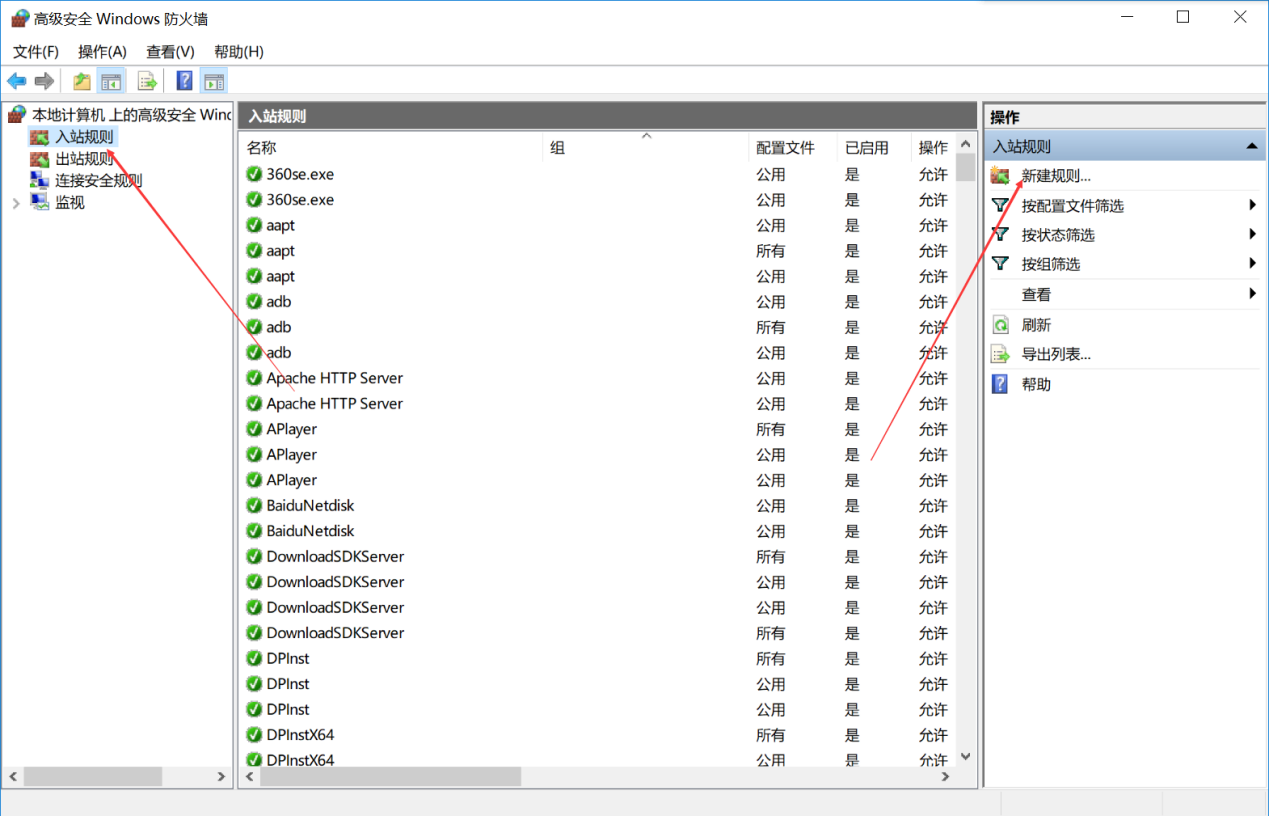


Windows 7以上版本操作系统

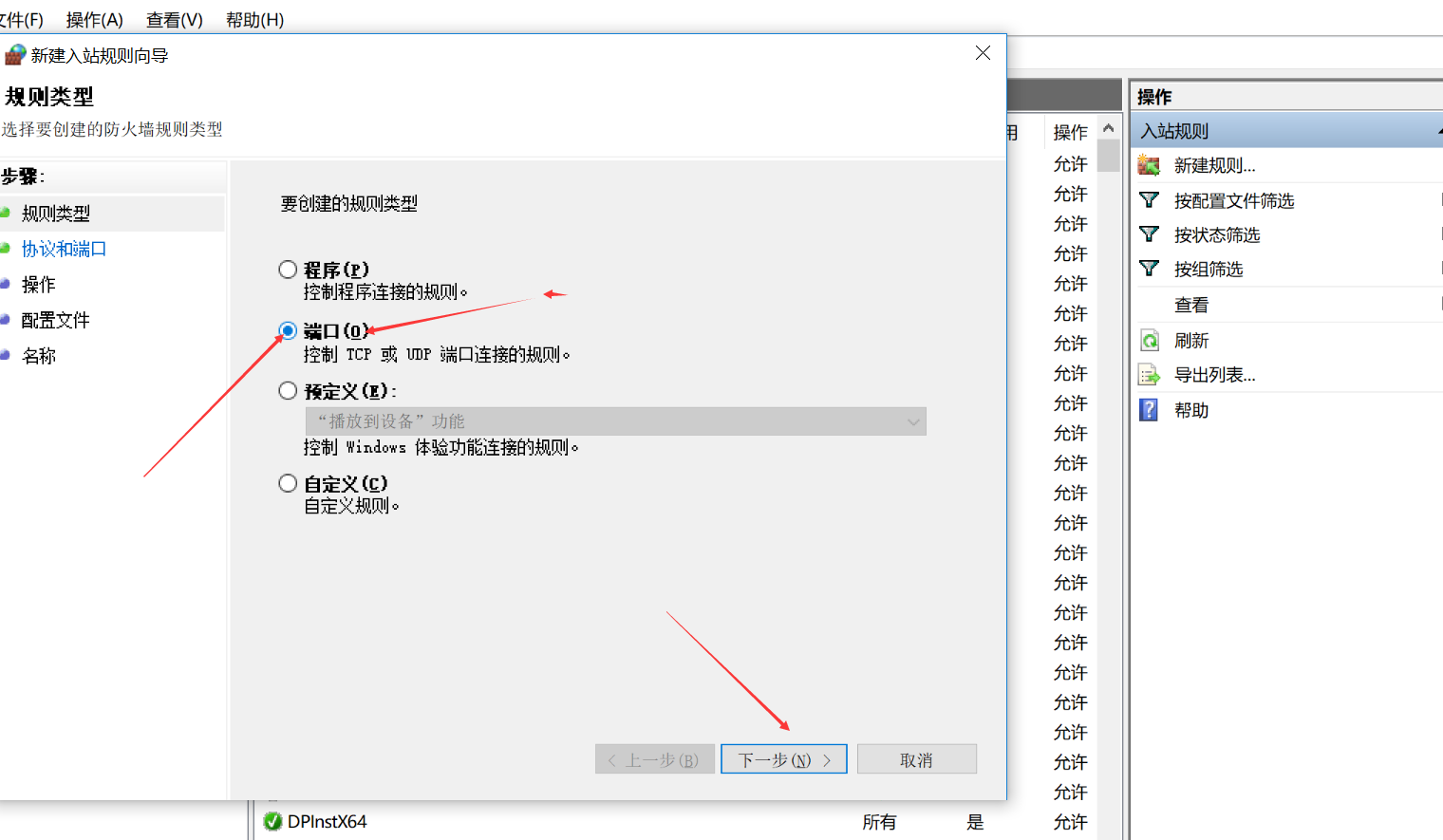
第一步：进入防火墙-》高级设置



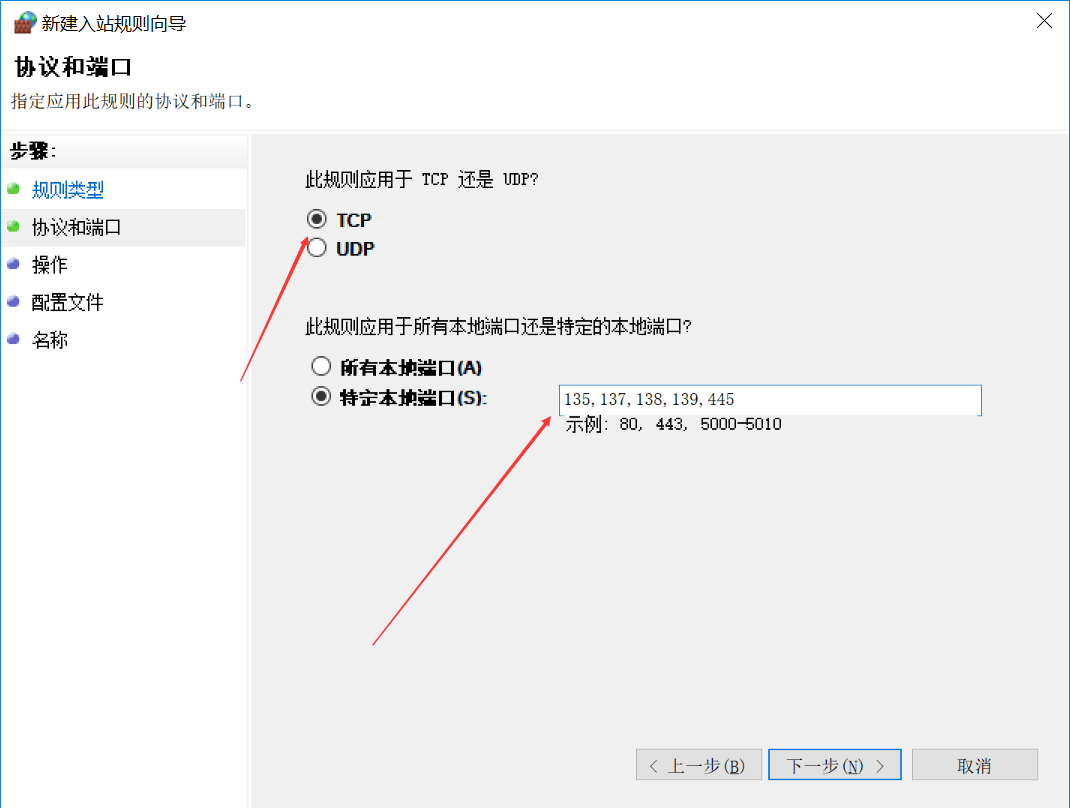
第二步：点击入站-》新建规则



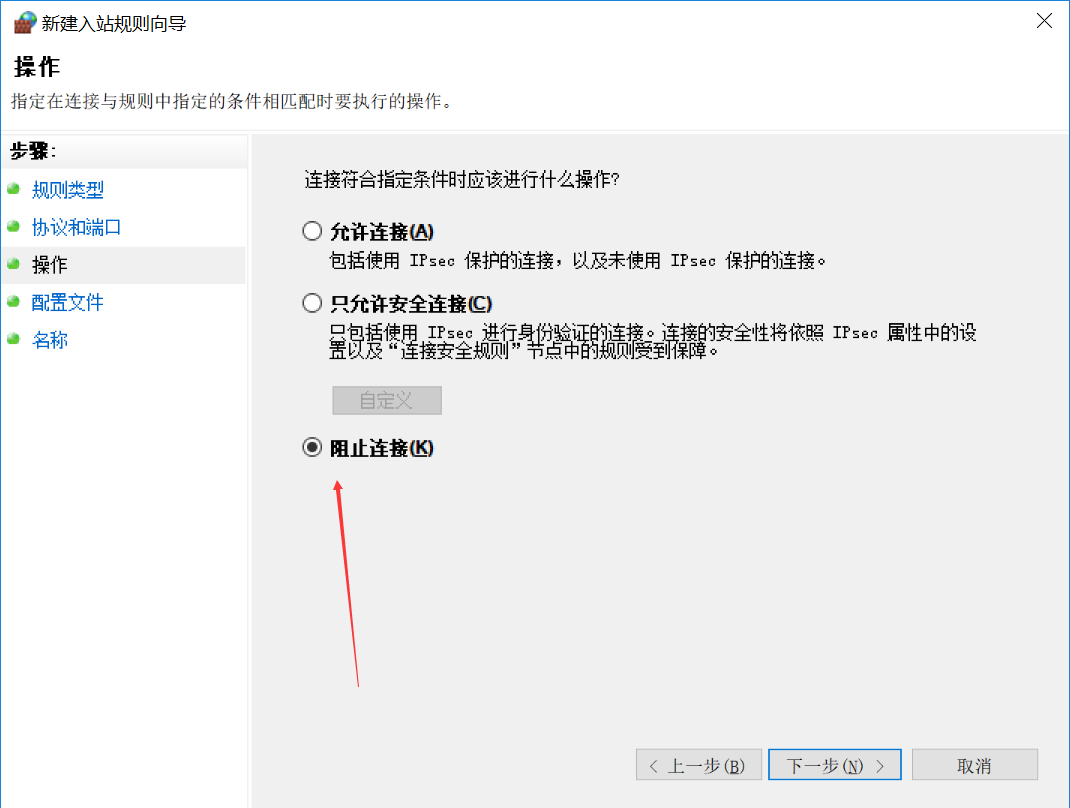
第三步：选端口-》下一步



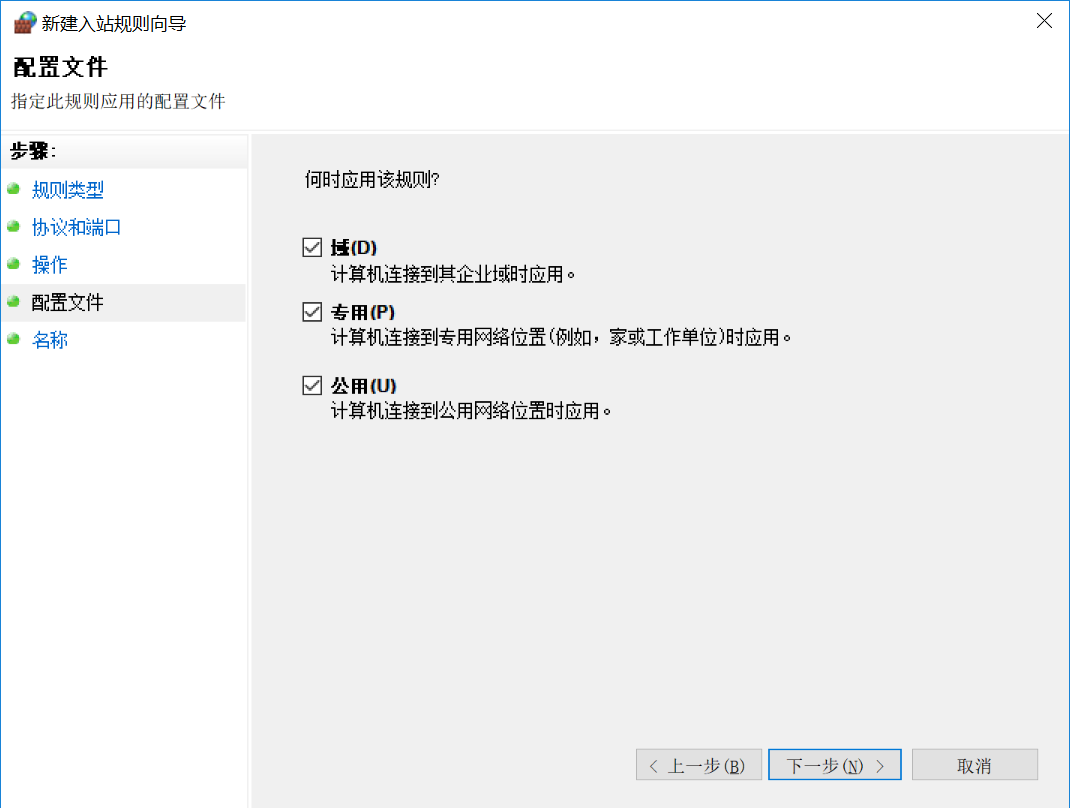
第四步：选TCP-》特定端口（135,137,138,139,445）



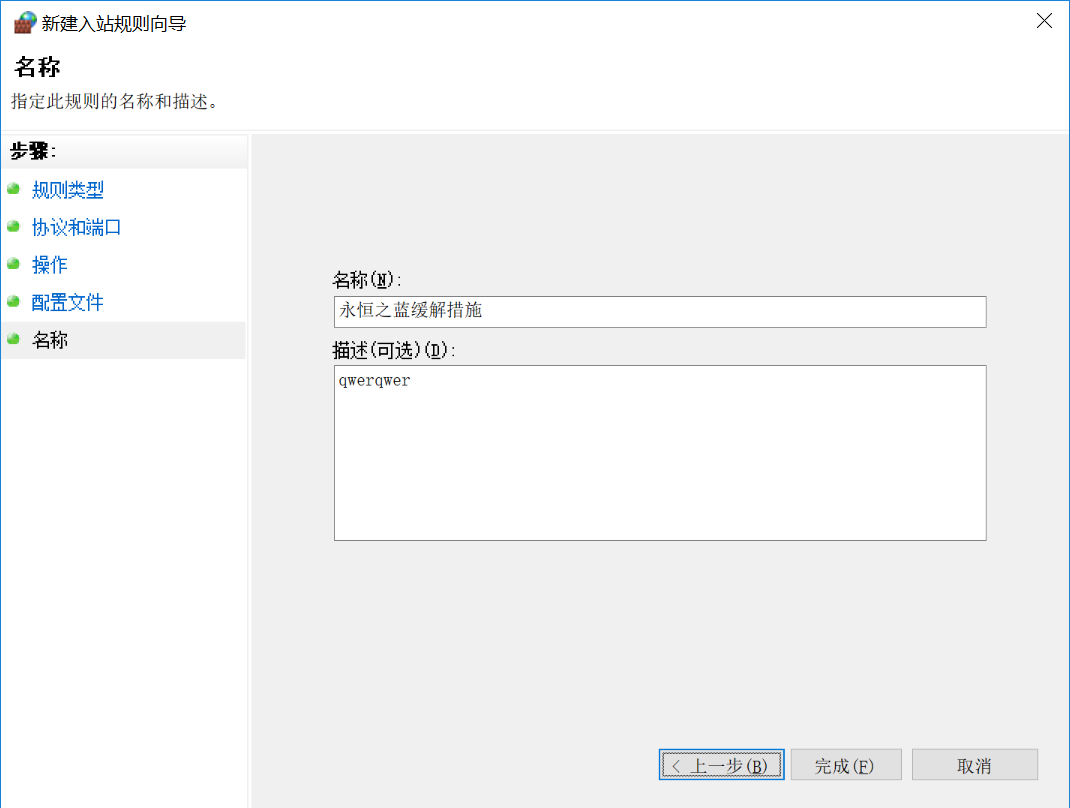
第五步：阻止连接-》下一步

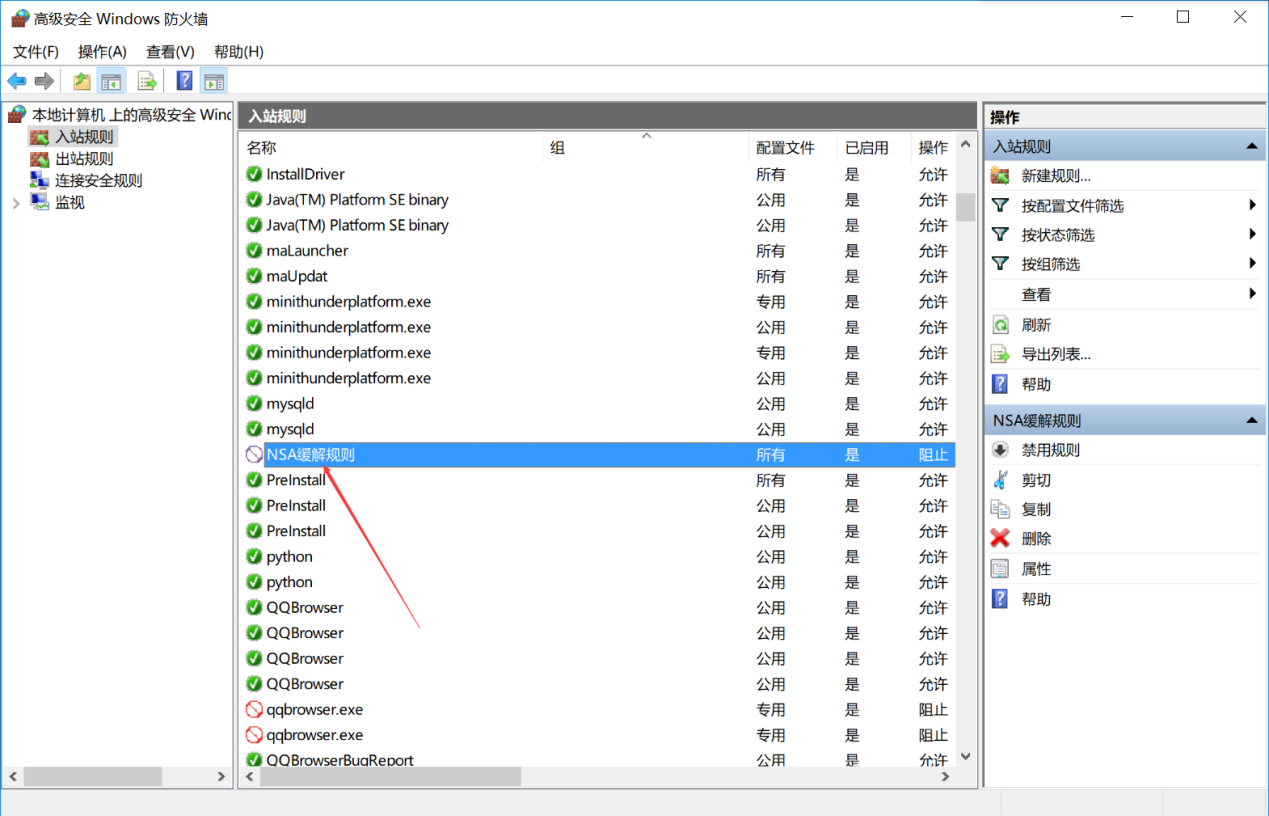


第六步：



第七步：名字随便取-》完成





## 三、终端侧应急解决方案（启明星辰信息安全技术）

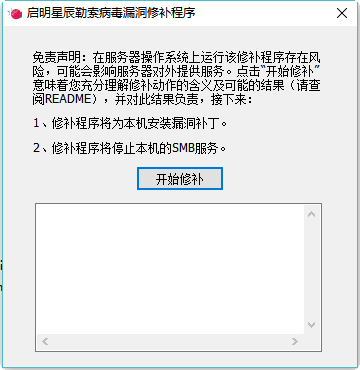
对于WinXP及以上版本的系统确认是否安装了MS07-010补丁，如没有安装则受威胁影响。



### 一键补丁加固

建议使用一键补丁加固工具进行补丁安装。（包含WinVista、WinXP、server2003、 server2008、server2008R2、win7、win8.1离线补丁）

链接: https://pan.baidu.com/s/1i5n6fY1 密码: n24f



### 一键加固工具

如果遇到打补丁失败的情况下,可使用一键加固工具进行服务器加固(此加固方式是关闭相应的共享服务，可能会影响文件共享、打印机共享)：

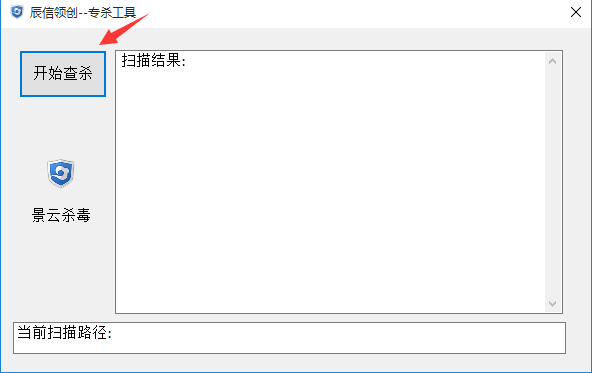
链接: https://pan.baidu.com/s/1dFkWzst 密码: dk8y



### 一键清除病毒

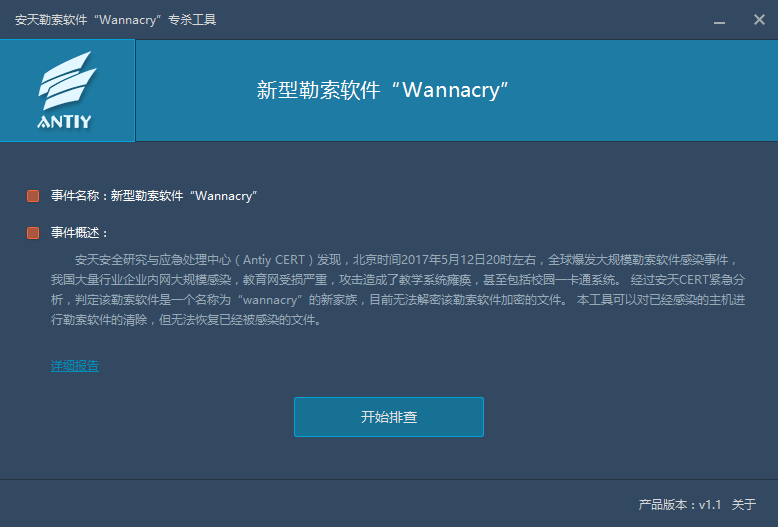
如果设备已经受到感染，可以使用一下工具清除勒索病毒文件，但是无法恢复受到感染的文件。

链接:http://pan.baidu.com/s/1b60VRS



## 已经感染设备应急解决方案

* 断开网络连接，阻止进一步扩散。使用专杀工具对病毒进行查杀（链接：链接: https://pan.baidu.com/s/1bpq0jG7 密码: y4dd此查杀工具只可查杀主机病毒，但无法恢复文件）。



* 已经感染终端，根据终端数据类型决定处置方式，如果重新安装系统则建议完全格式化硬盘、使用新操作系统、完善操作系统补丁、通过检查确认无相关漏洞后再恢复网络连接。