**防范勒索病毒个人计算机安全防护指南**

**系统加固流程：**

1、开机前拔掉网线，保持计算机断网状态。

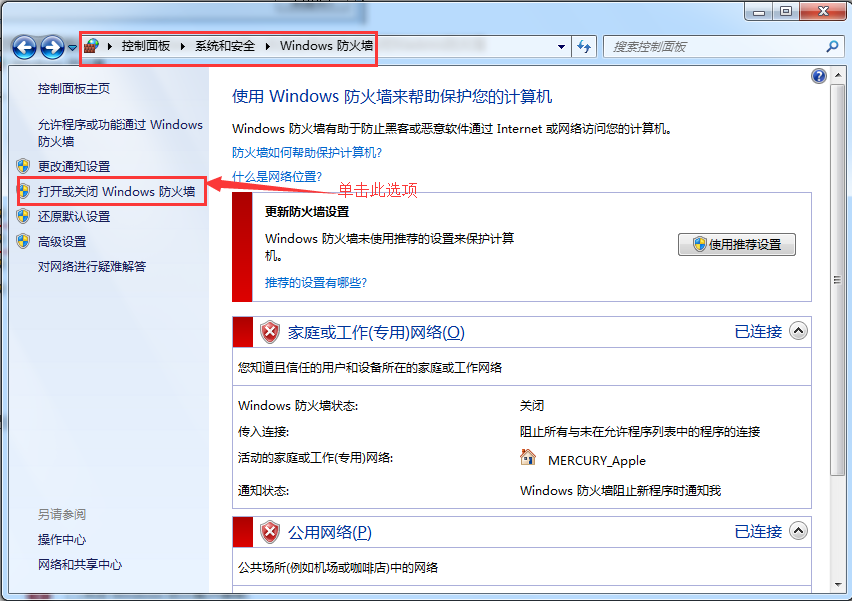
2、准备移动U盘或光盘在断网状态下，对计算机内的重要资料进行数据备份。

3、依照以下步骤对计算机进行安全策略加固。

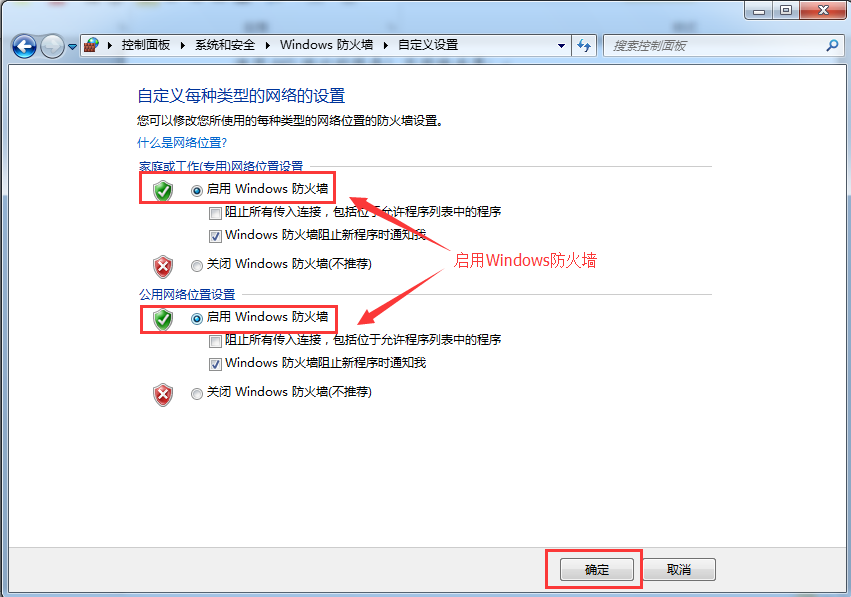
**（1）Win7、Win8、Win10的处理流程：**

①拔掉网线保持计算机断网状态。

②打开控制面板-系统与安全-Windows防火墙，点击左侧打开或关闭Windows防火墙。

****

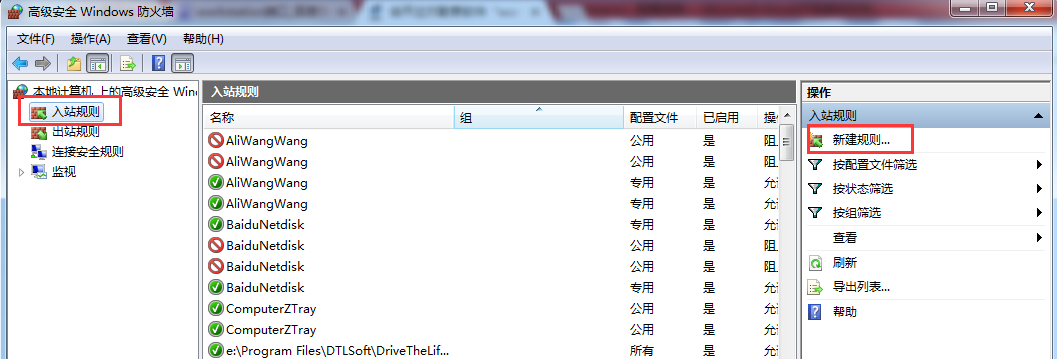
③选择启动防火墙，并点击确定

****

④点击高级设置

****

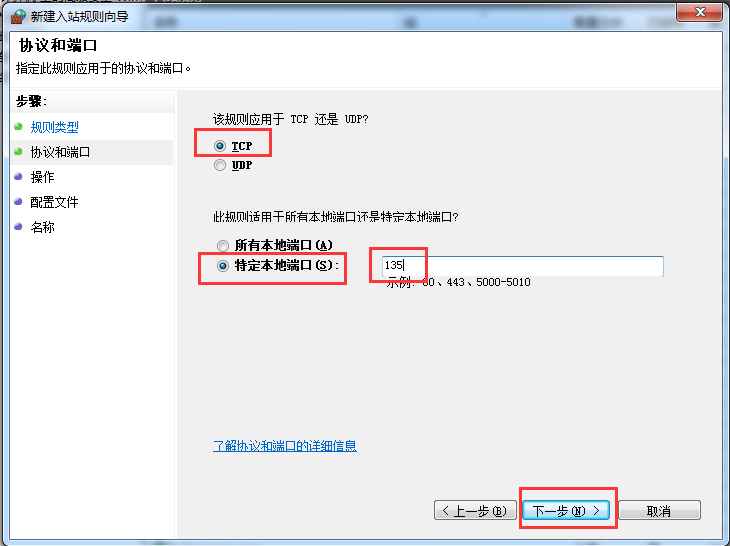
⑤点击入站规则，新建规则，以135端口为例

****

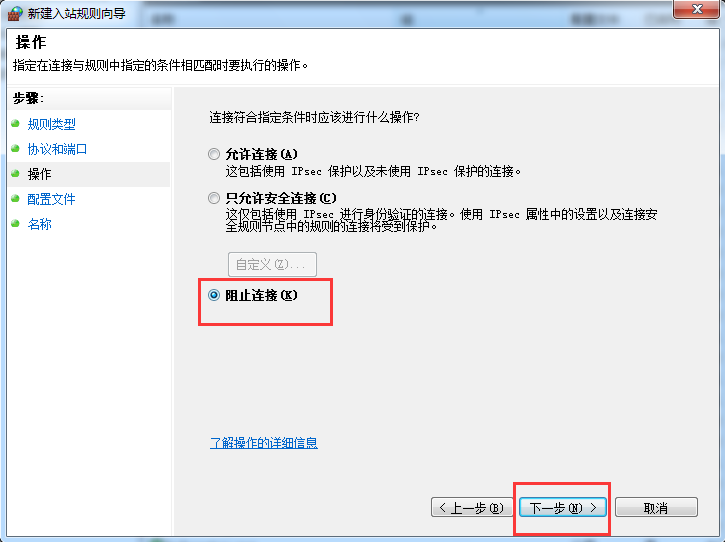
⑥选择端口、下一步

****

⑦选择特定本地端口，选择TCP协议，端口输入135，下一步

****

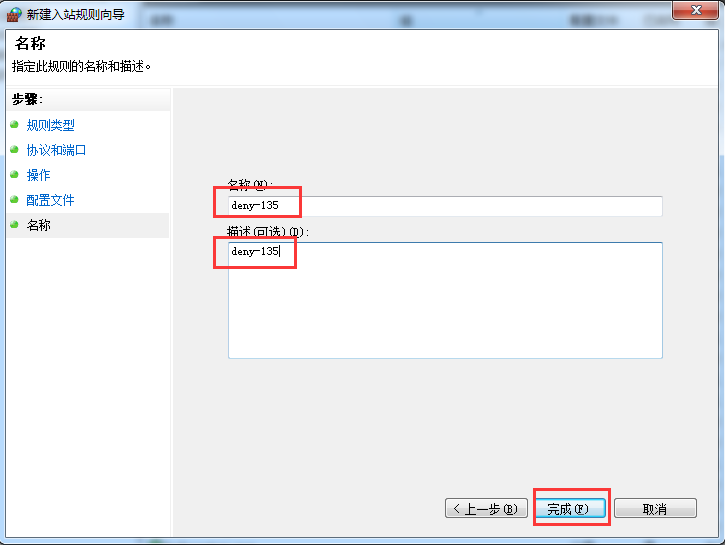
⑧选择阻止连接，下一步

****

⑨配置文件，全选，下一步

****

⑩名称，可以任意输入，完成即可

****

⑪仿照步骤4）～10）也可以新建一个135端口的UDP协议的封堵规则（也可以不建）

⑫准备移动U盘或者光盘，下载专杀工具和免疫工具

地址如下：

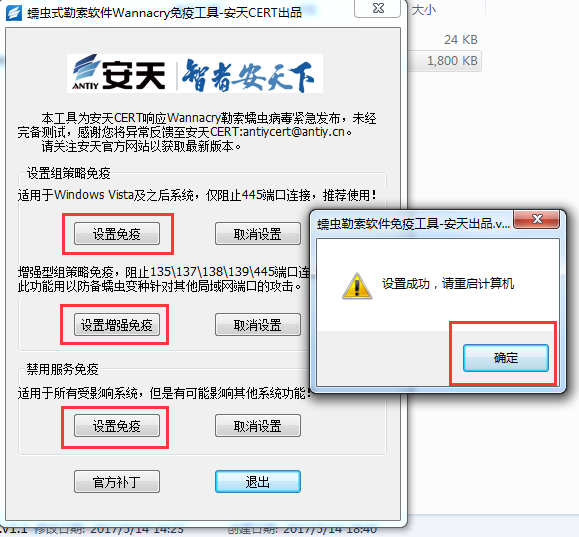
**A．蠕虫勒索软件专杀工具（WannaCry）：**

<http://www.antiy.com/response/wannacry/ATScanner.zip>

**B．蠕虫勒索软件免疫工具（WannaCry）：**

<http://www.antiy.com/response/wannacry/Vaccine_for_wannacry.zip>

⑬使用蠕虫勒索软件免疫工具（WannaCry）（本工具提供禁用系统服务、设置ipsec本地组策略等功能，能阻断通过SMB漏洞MS17-010向本机传播WannaCry勒索软件，但不能阻断WannaCry在本机上的运行）。需要三项免疫策略全部点击（包括设置策略免疫两项与禁止服务免疫）

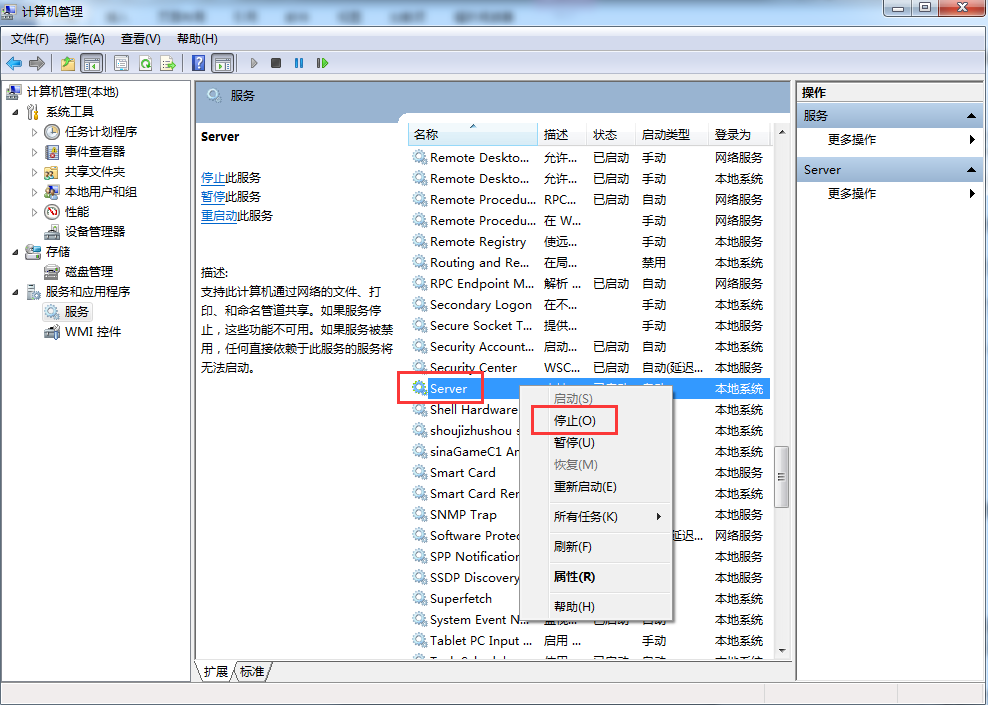
****

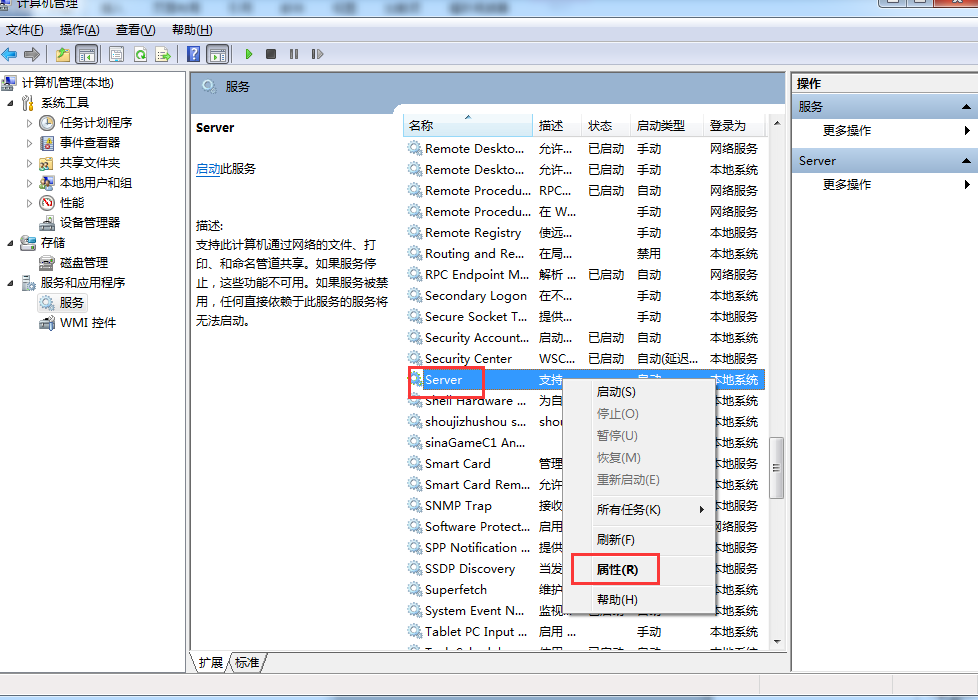
⑭关闭Windows Server服务。

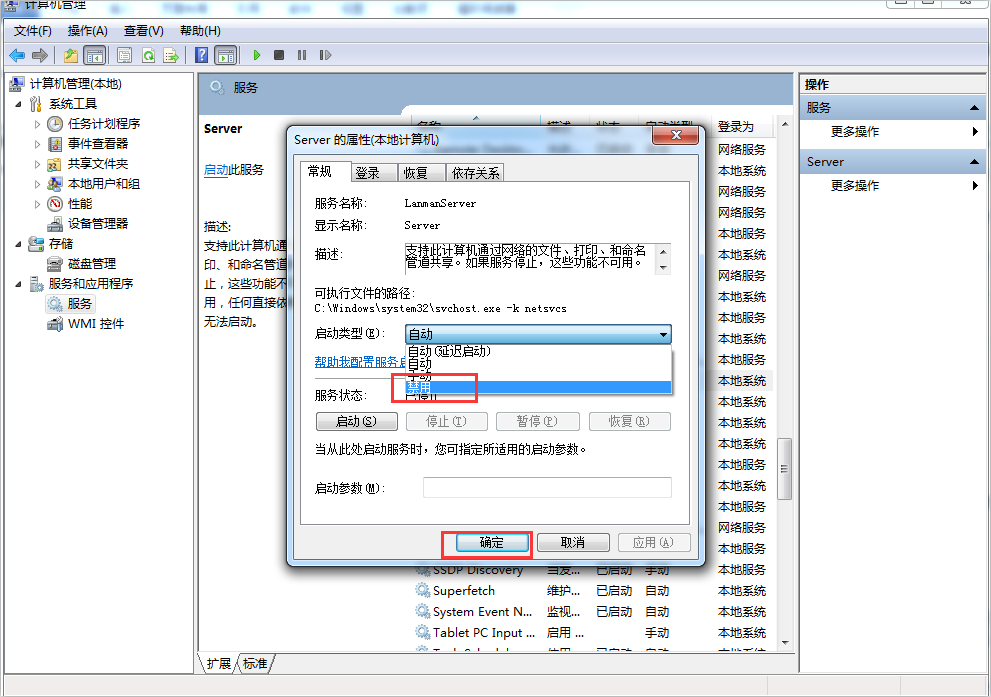
此步骤的目的是从根上彻底关闭445端口的服务，比通过策略管理拦截比较方便操作。

步骤如下：

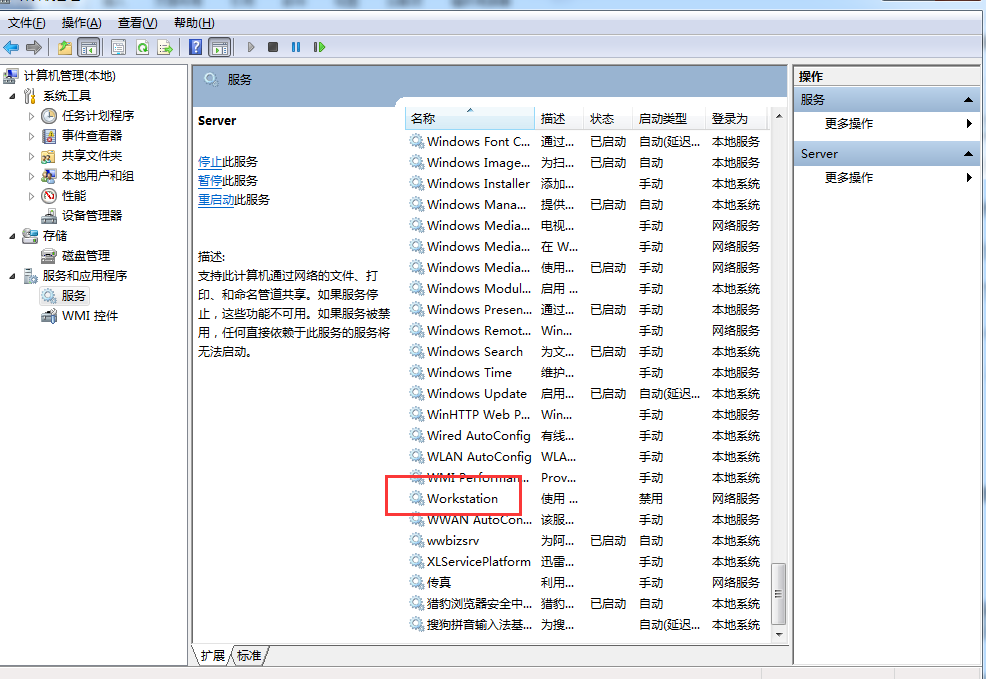
计算机->管理->配置->服务->找到右侧的Server服务，右击，停止，再右击，属性，并将启动类型改为禁用，点击确定。







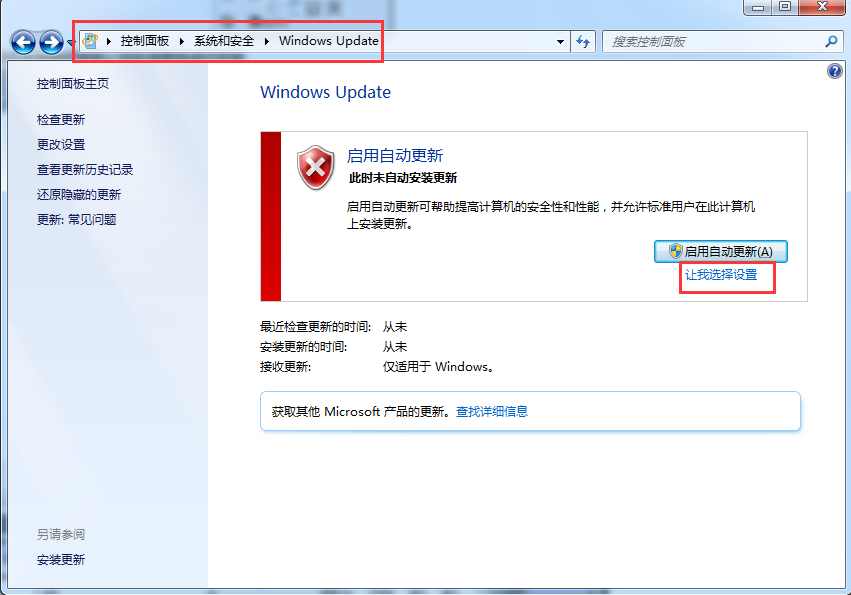
⑮关闭Workstation服务，参考（1）中步骤⑭

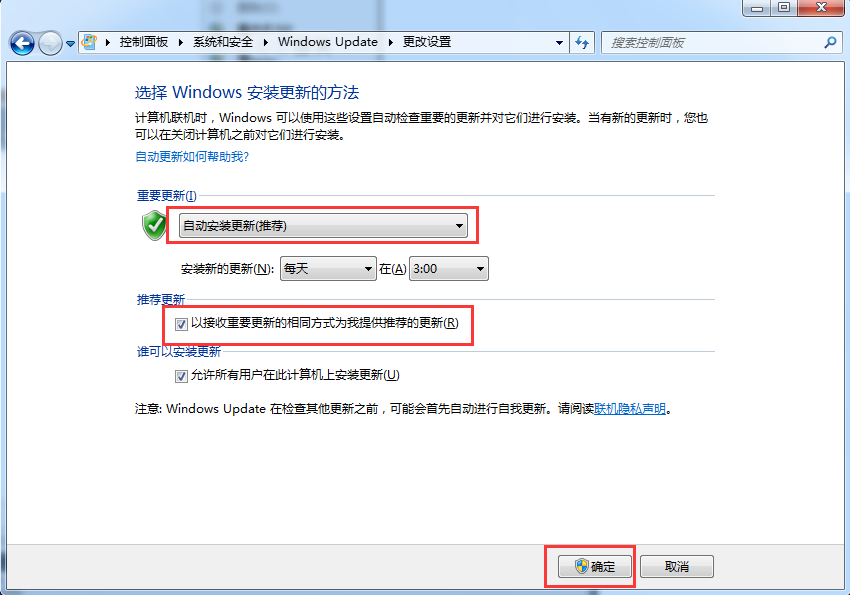


⑯恢复网络（连接网线并启用本地连接）

****

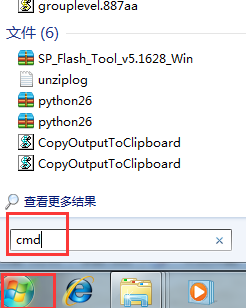
⑰开启系统自动更新，并检测更新进行安装

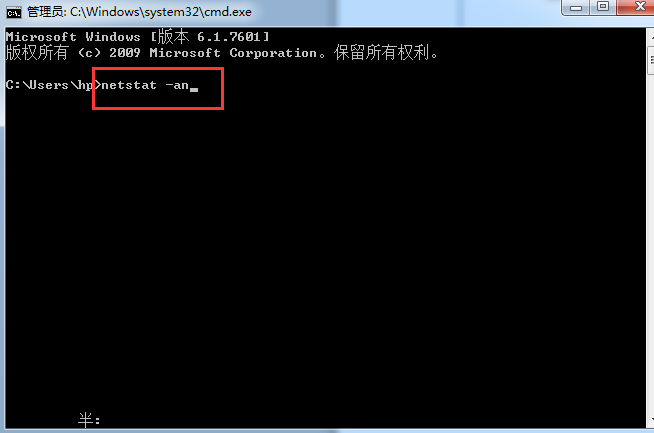
****

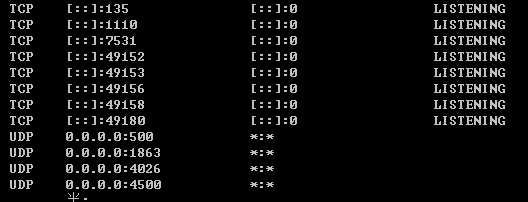
****

⑱最后重启计算机

⑲重启之后在开始菜单输入cmd，输入命令netstat–an，如下图：



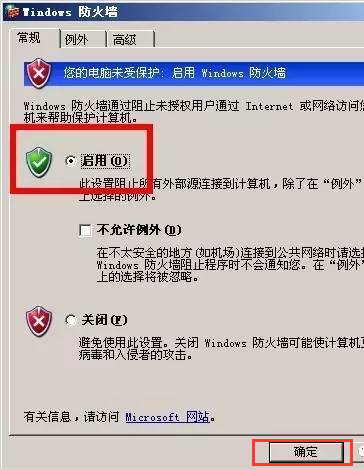




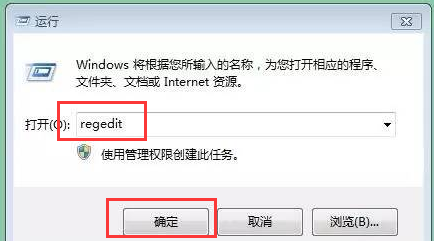
此时已经看不到445监听端口，注意135端口是无法停止，经测试Windows的一些应用需要用到135，所以135只通过阻止外网访问方式访问（参考步骤4～11），而不直接停止服务及其监听。

**（2）WinXP的处理流程：**

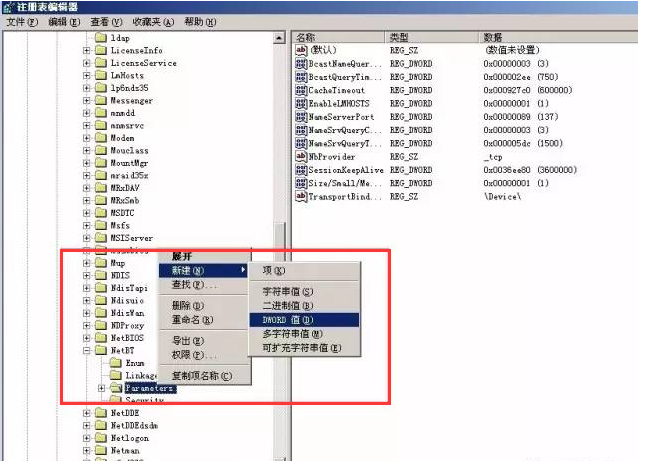
①依次打开控制面板，安全中心，Windows防火墙，选择启用



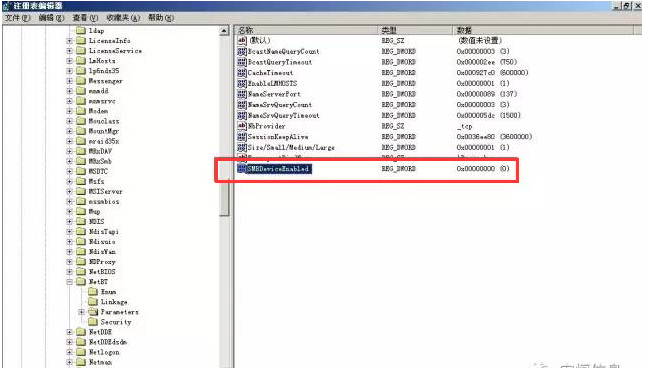
②通过注册表关闭445端口，单击“开始”——“运行”，输入“regedit”，单击“确定”按钮，打开注册表。



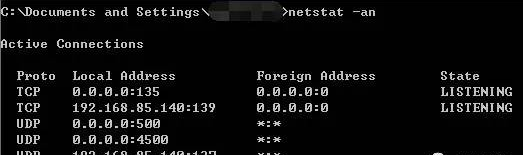
③找到HKEY\_LOCAL\_MACHINE\System\Controlset\Services\NetBT\Parameters，选择“Parameters”项，右键单击，选择“新建”——“DWORD值”



1. 将DWORD值命名为“SMBDeviceEnabled”，值修改为0

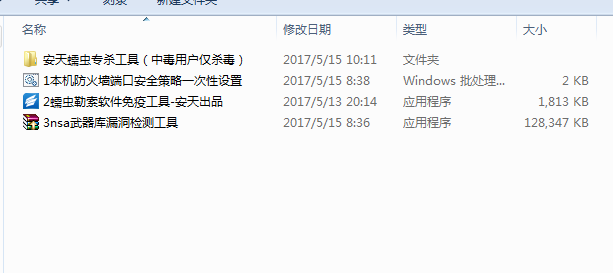


1. 重启机器，查看445端口连接已经没有了

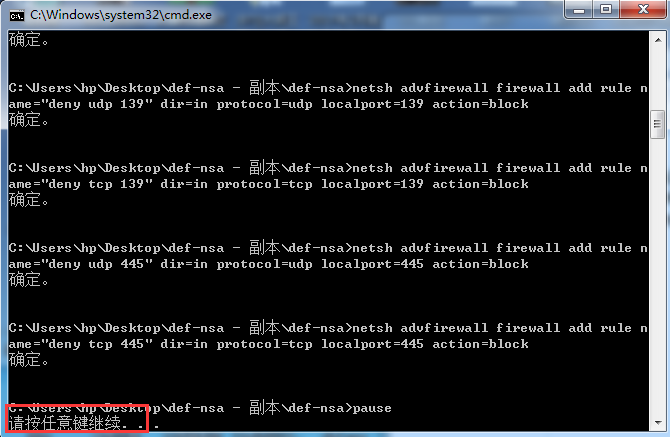


鉴于本次Wannacry蠕虫事件的影响巨大，微软总部决定对已停服的XP和部分服务器版本发布特别补丁，微软公告详情<https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>，经安全厂商验证，XP系统补丁有效。

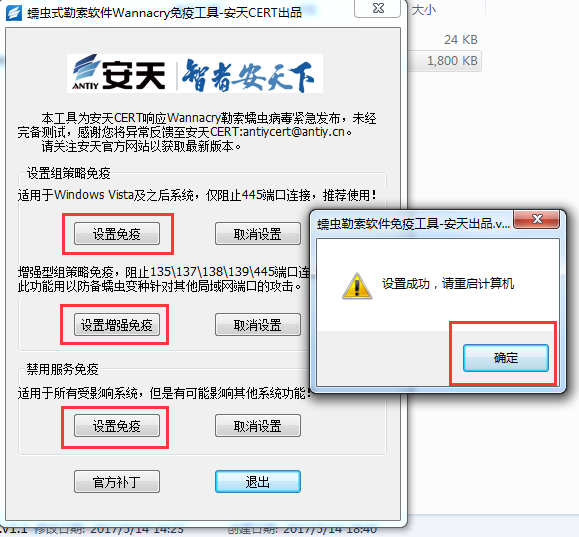
**（3）对于已经联网，并未出现感染病毒的用户**建议使用附件2中的处理工具：



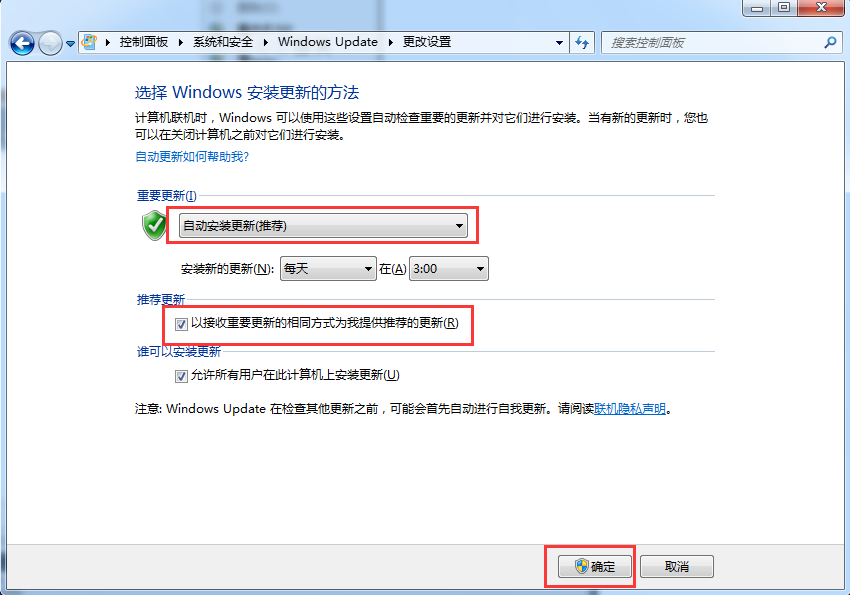
1. 首先双击运行序号为1的软件 ，运行结束后按回车



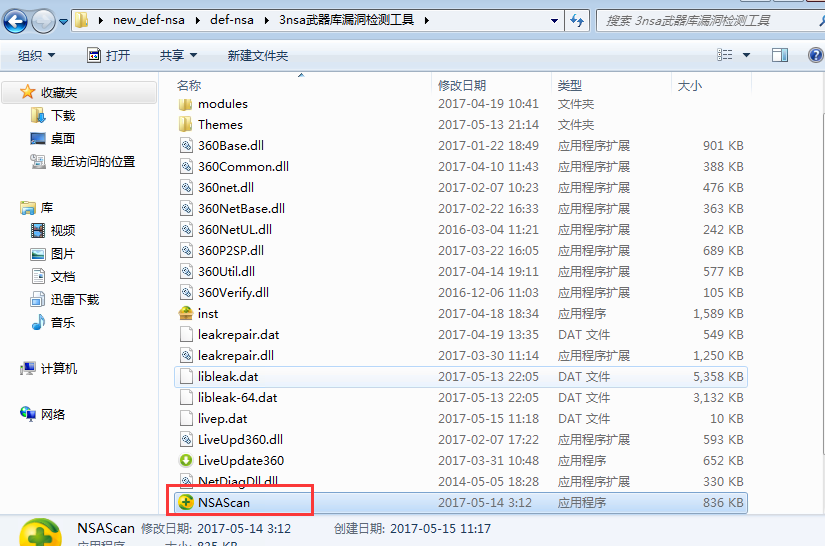
1. 运行序号为2的软件，参考（1）中步骤⑬

****

1. 检测系统安装更新，参考（1）中步骤⑰

****

1. 重启计算机后，解压序号为3的检测工具，并运行“NSAScan”检测



1. 检测安全后，则可以正常使用了

