**勒索病毒应急处理须知**

因勒索病毒在互联网和公安网大面积蔓延，影响到所有联网电脑用户的文件，为避免和减少损失，请所有人员认真查看此须知！！！

一、病毒**影响范围**

MS17-010漏洞主要影响以下操作系统：Windows 2000，Windows 2003，Windows2008，Windows2012，Windows XP，Windows Vista，Windows7，Windows8，Windows10。

二、应急解决方案

**对于未开机或未被感染的计算机：**

第一步：断开网络（拔掉网线）；

第二步：使用U盘或光盘自带的PE系统启动电脑，将计算机中所有重要文件（尤其文档、图片、照片、压缩包、音频、视频等）备份到移动存储设备上。

第三步：开启系统防火墙，并利用系统防火墙高级设置阻止向445端口进行连接。

第四步：对系统进行ms17010、ms10061、ms14068、ms08067、ms09050补丁更新。

三、启动防火墙及阻止445端口处理流程

**Win7、Win8、Win10的处理流程：**

1、打开控制面板-系统与安全-Windows防火墙，点击左侧启动或关闭Windows防火墙。 

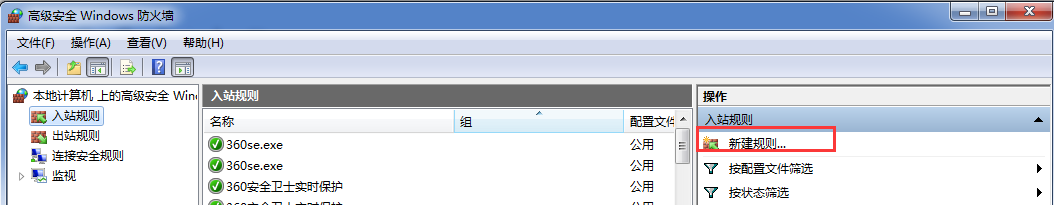
2、选择启动防火墙，并点击确定。



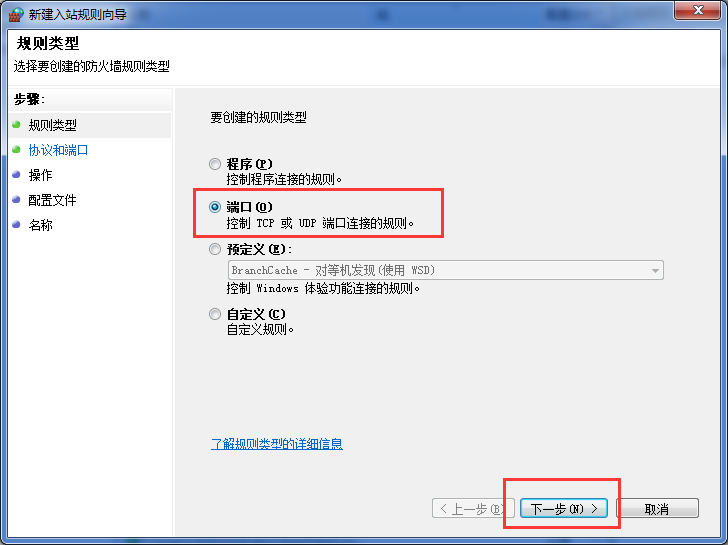
3、点击高级设置。



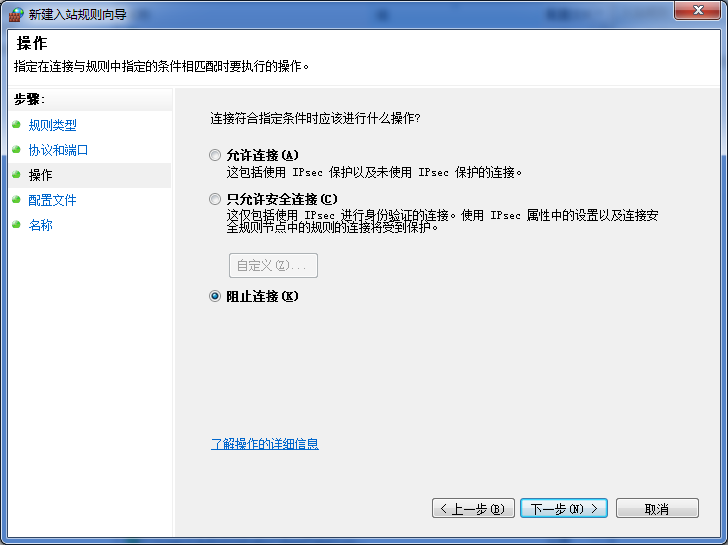
4、点击入、出站规则，新建规则。



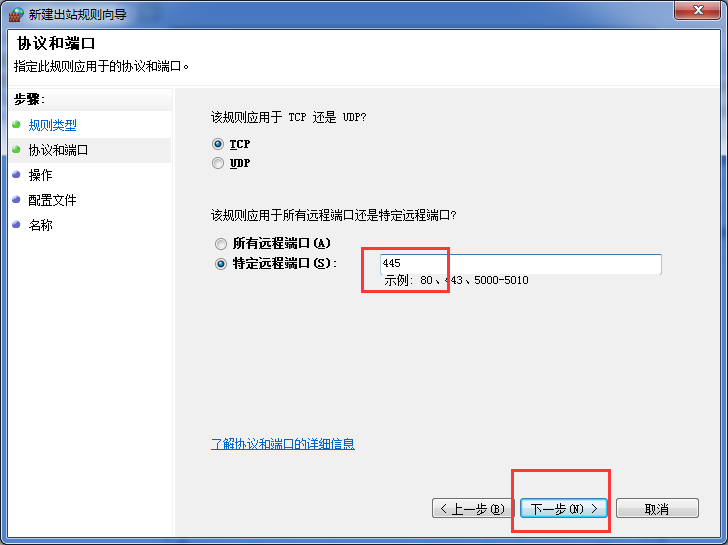
5、选择端口，下一步。



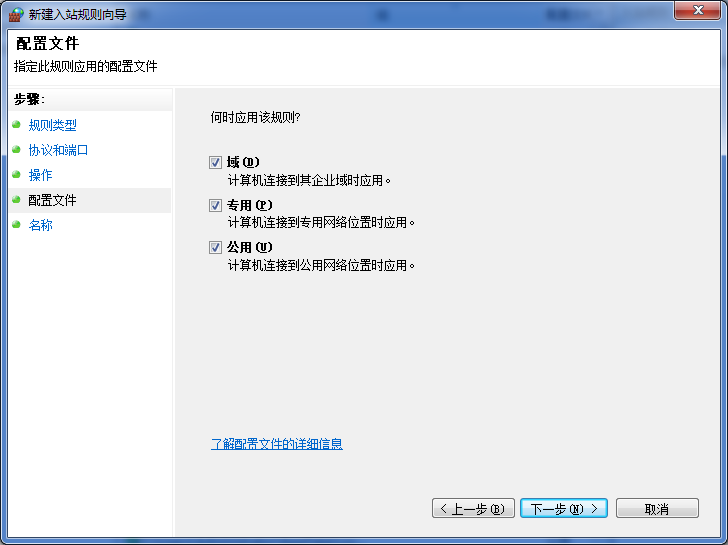
6、选择阻止连接，下一步。



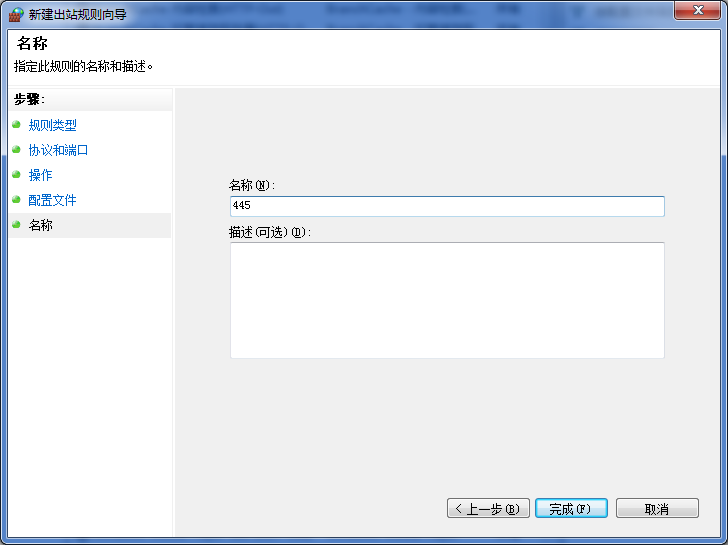
7、特定本地端口，输入445，下一步。



8、配置文件，全选，下一步。



9、名称，可以任意输入，完成即可。



**XP系统的处理流程：**

1、依次打开控制面板，安全中心，Windows防火墙，选择启用



2、点击开始，运行，输入cmd，确定执行下面三条命令

net  stop rdr

net  stop srv

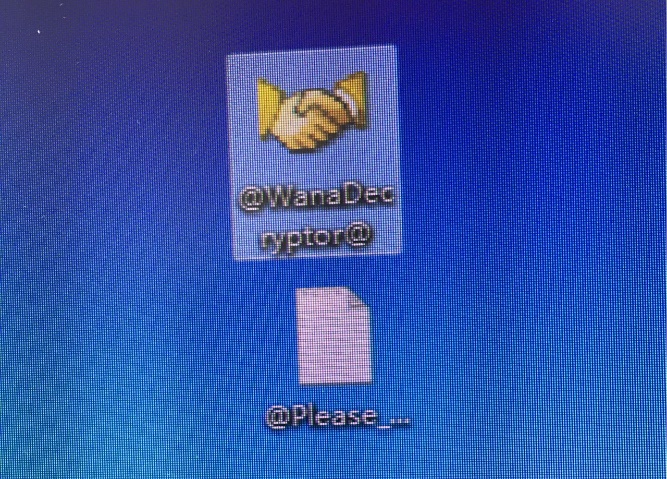
net  stop netbt

**四、如何分辨是否中毒：**

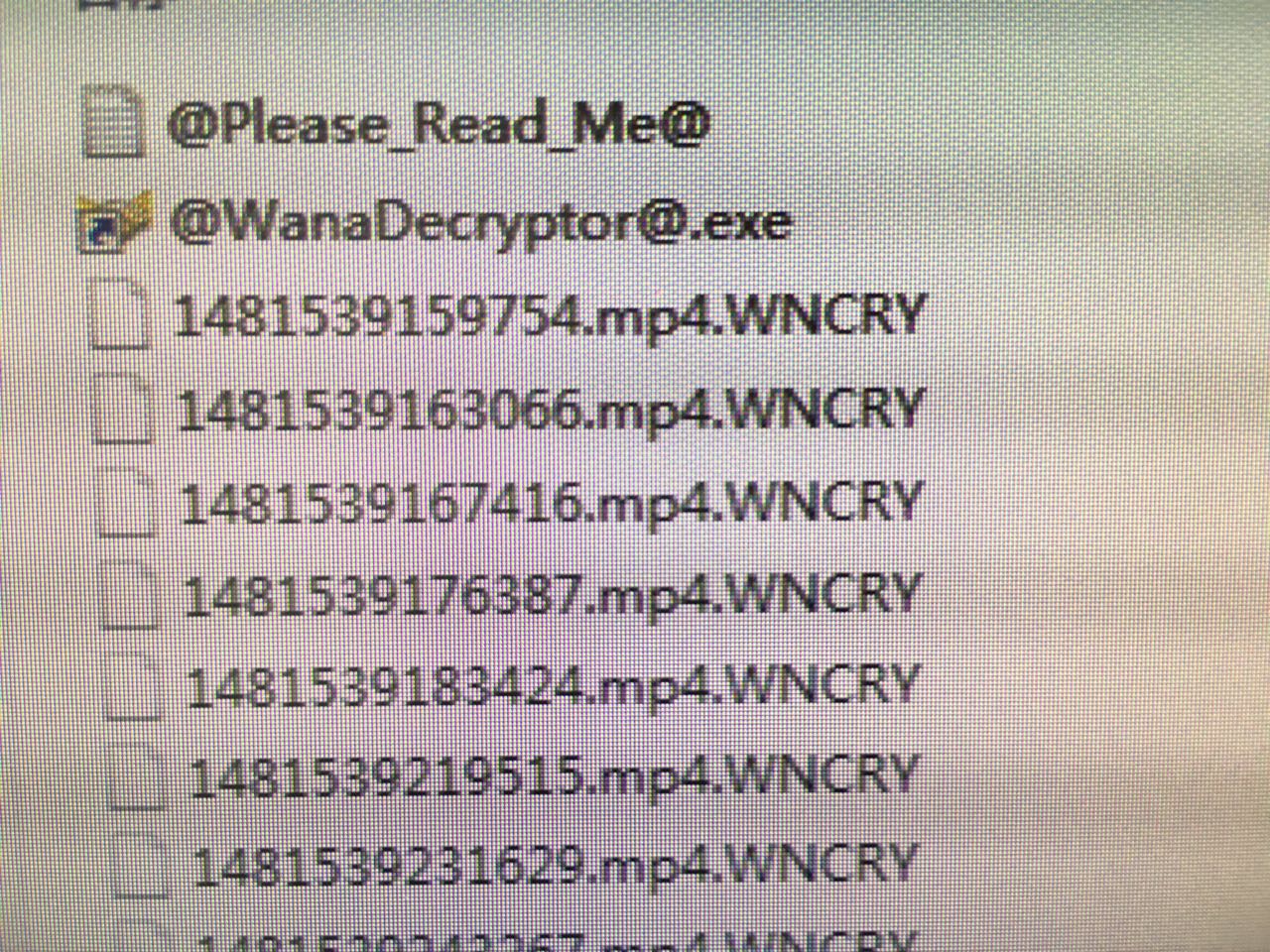
当系统被该勒索软件入侵后，会弹出勒索对话框：



或在桌面及各个文件夹内出现以下文件：



所有被感染文件以“.WNCRY”或者“.ONION”为后缀：



该病毒目前没有专杀工具，加密文件无法暴力破解。如不幸感染病毒，系统中有重要文件的请等待解密工具，没有重要文件的可以选择格式化全盘并重做系统。

该勒索软件采用包括英语、简体中文、繁体中文等28种语言进行“本地化”。会将自身复制到每个文件夹下，并重命名为“@WanaDecryptor@.exe”。同时衍生大量语言配置等文件，该勒索软件AES和RSA加密算法，加密的文件以“WANACRY!”开头，加密如下后缀名的文件：

