WannaCry 勒索蠕虫病毒出现变种

及紧急处置工作通知

各位领导及同事：

国家网络与信息安全通报中心通报，WannaCry 勒索蠕虫病毒出现了变种，该变种的传播速度可能会更快,一旦感染此病毒，可能会造成重要文件被非法加密，从而导致无法打开或丢失。故请全集团各单位部门立即进行关注和处置。

**一、员工应急操作**

1、全集团各员工于2017年5月15日星期一上班时，须率先将各自电脑的网线拔出，然后再开机启动。

2、开机启动后请各自开启操作系统防火墙，阻止445端口进行连接（操作步骤详见第三项）。关闭445端口后可能会影响打印功能，请各位领导及同事理解支持，暂行克服。

3、关闭445端口后，请将各自重要文件、数据利用“自己的”移动设备进行备份操作。

4、备份操作完成后，插入网线利用杀毒软件进行杀毒。

5、在信息部门完成补丁修复工作之前禁止私自打开445端口，并严格禁止将U盘、移动硬盘等移动设备交叉使用。

6、请各位同事务必执行以上操作，以免遭受损失。

**二、各单位信息部门应急工作**

1、由各单位信息部门须立即组织内网检测，查找所有开放445 SMB服务端口的服务器和终端，并对逐一公司内每台电脑及服务器进行补丁MS17-010的修复工作，务必做到每台设备补丁修复后再打开445端口。

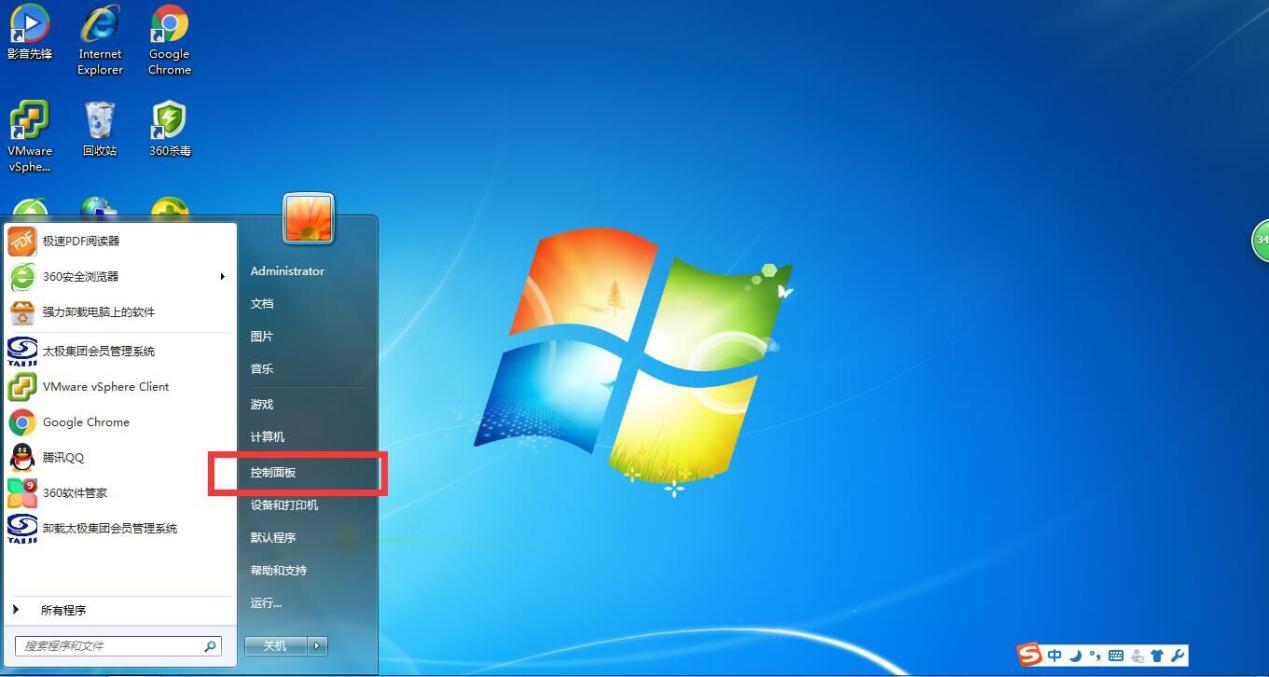
2、一旦发现中毒机器，立即断网处置，目前业内相关专家发现对硬盘格式化可清除病毒。

3、目前微软已发布补丁MS17-010修复了“永恒之蓝”攻击的系统漏洞，请各单位信息部门完成修复工作。网址为：https://technet.microsoft.com/zh-cn/library/security/MS17-010；对于XP、2003等微软已不再提供安全更新的机器，建议升级操作系统版本，或使用360“NSA武器库免疫工具”检测系统是否存在漏洞，并关闭受到漏洞影响的端口，可以避免遭到勒索软件等病毒的侵害。免疫工具下载地址：<http://dl.360safe.com/nsa/nsatool.exe>。

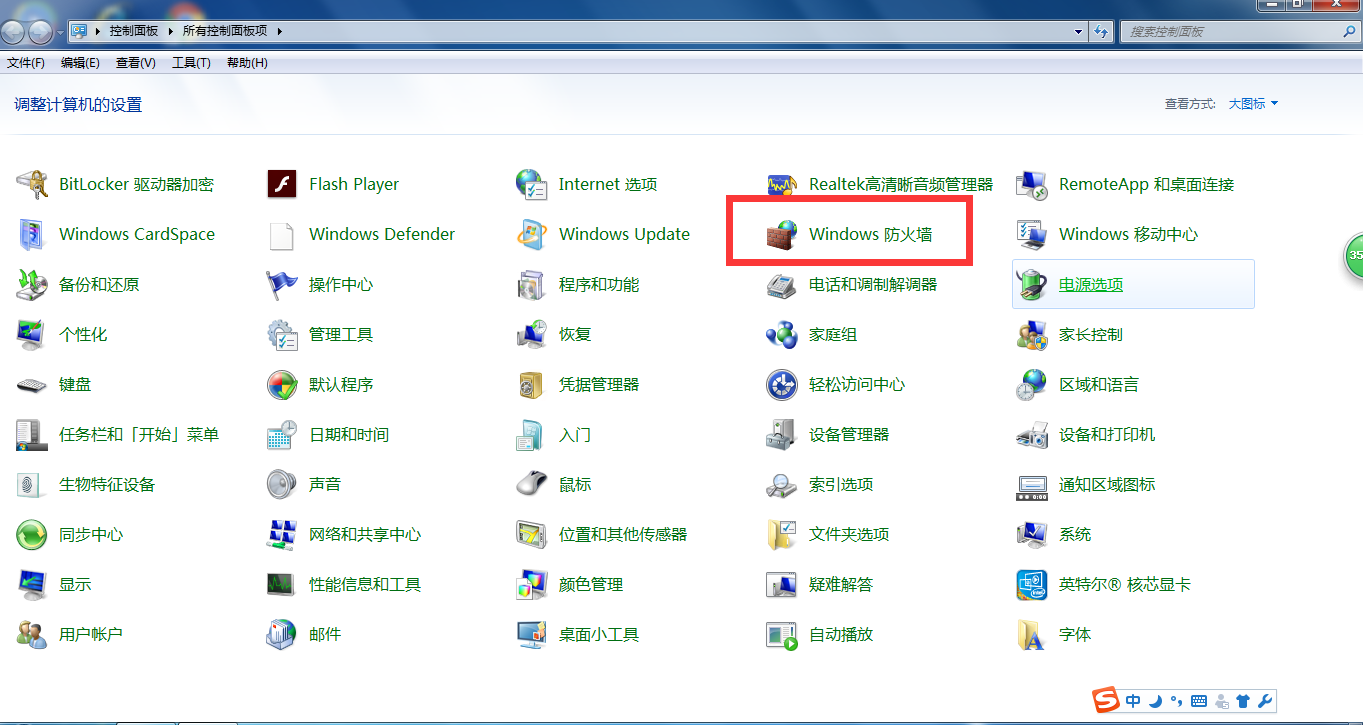
**三、员工相关操作步骤**

（一）win7、win8、win10处理流程

1、打开控制面板



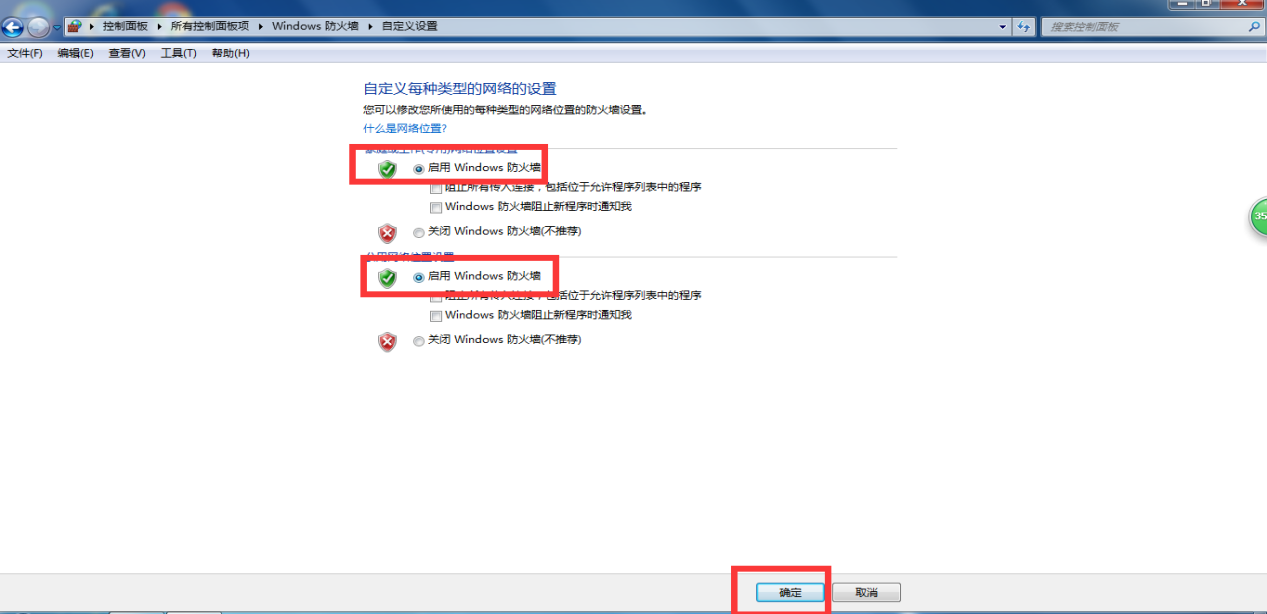
2、打开操作系统防火墙



3、点击打开或关闭防火墙



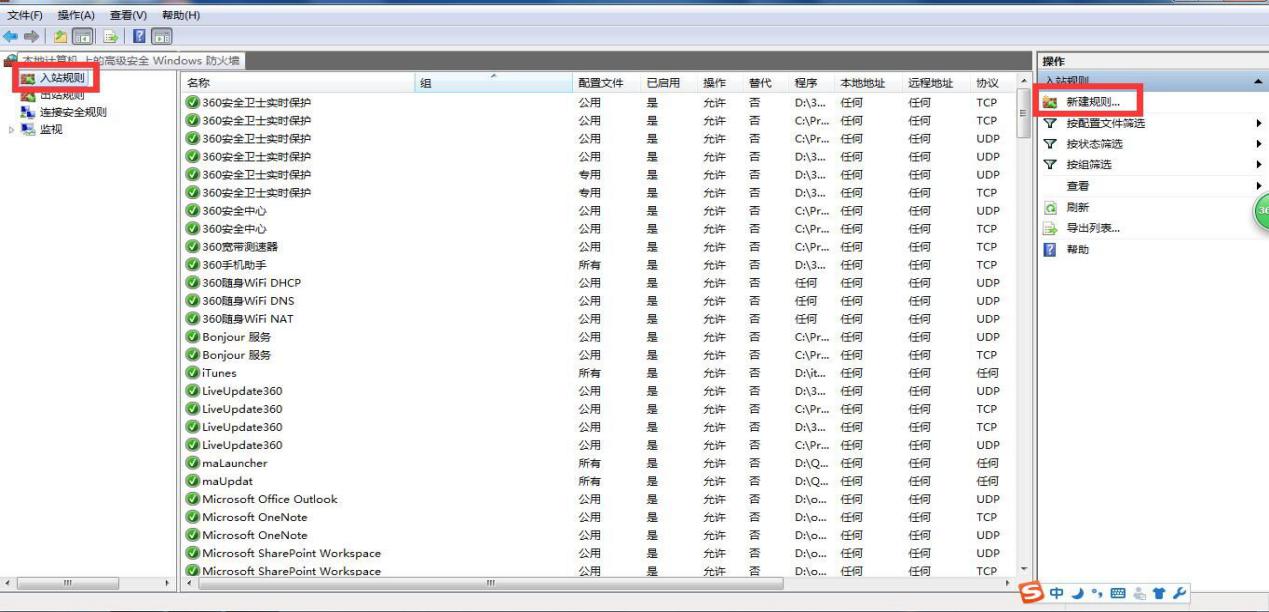
4、打开防火墙



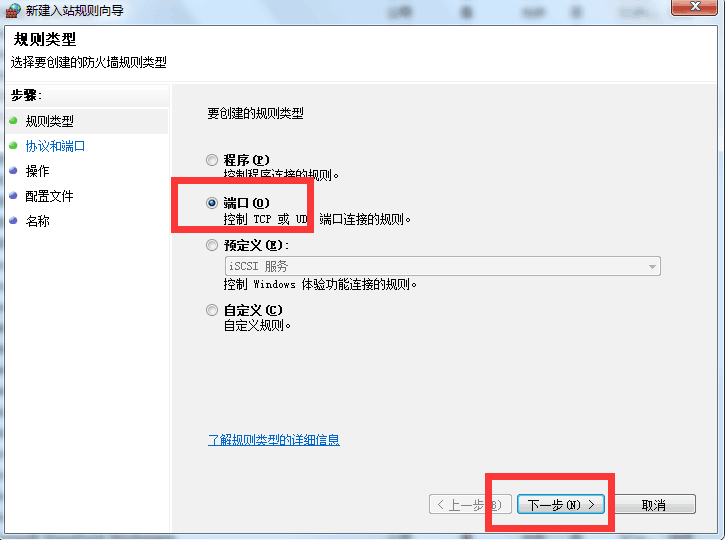
5、点击高级设置



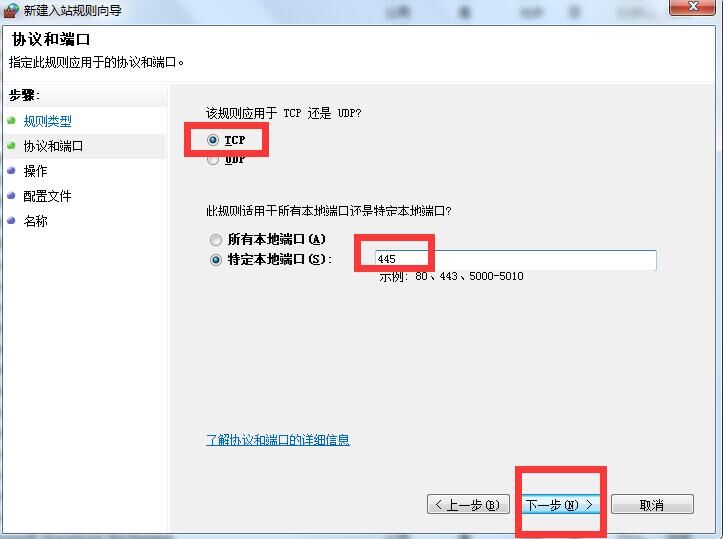
6、点击入站规则，再点击新建规则



7、点击端口，下一步



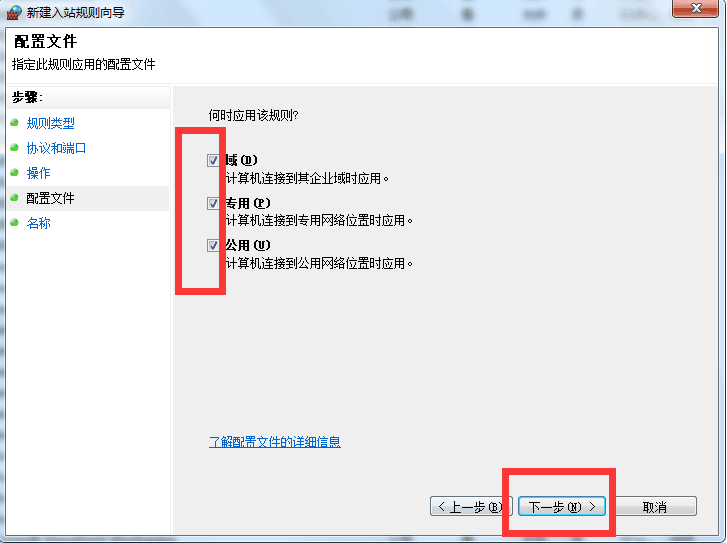
8、选择TCP，输入特定本地端口445，下一步



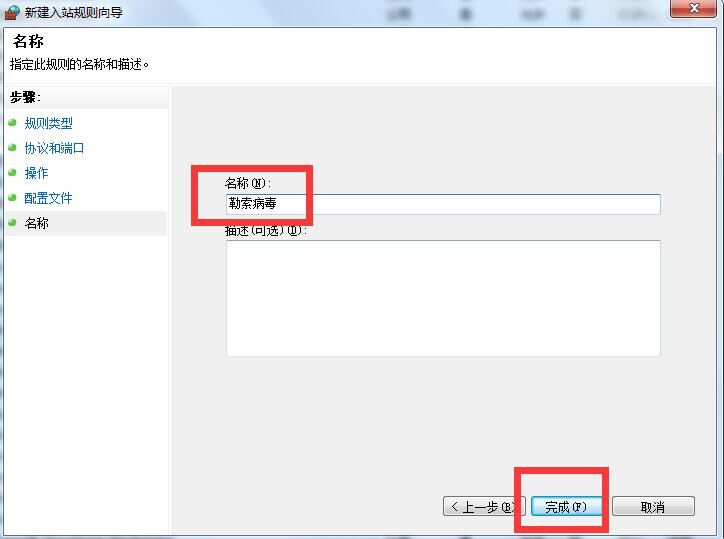
9、点击阻止连接，下一步



10、配置全选，下一步



11、名称输入“勒索病毒”，点击完成即可



（二）XP系统处理流程



**四、其他说明**

1、各单位信息部门应按业务紧急重要程度依次解决补丁修复及打印功能问题。

2、由于此次属于突发事件，涉及面较广，各业务部门可指派专人到各单位信息部门学习解决办法，协助信息部门尽快完成此次工作。

3、另外如有其他疑问请及时联系各自单位信息部门，感谢支持！

太极实业信息部

2017年5月14日