安天应对勒索软件“WANNACRY”防护手册

首次发布时间：2017 年 05 月 13 日

本版本更新时间：2017 年 05 月 13 日

一、 概述

全球爆发大规模勒索软件感染事件，我国大量行业企业内网大规模感染，教育网受损严重，政府、能源、交通等行业均受到不同程度影响。英国、美国、俄罗斯、西班牙、意大利、越南、美国等一百多个国家和地区出现了被感染的情况。

经过安天 CERT 紧急分析，判定该勒索软件是一个名称为“wannacry”的新家族，目前无法解密该勒索软件加密的文件。该勒索软件迅速感染全球大量主机的原因是利用了基于 445 端口传播扩散的 SMB 漏洞 MS17-010，微软在今年 3 月份发布了该漏洞的补丁。2017 年 4 月 14 日黑客组织 Shadow Brokers（影子经纪人）公布的 Equation Group（方程式组织）使用的“网络军火”中包含了该漏洞的利用程序，而该勒索软件的攻击者或攻击组织在借鉴了该“网络军火”后进行了这次全球性的大规模攻击事件。

二、 防护解决方案

2.1 关于尚未感染的用户群体的详细防护步骤如下：

1. 关闭网络，开启系统防火墙；
2. 利用系统防火墙高级设置阻止向 445 端口进行连接（该操作会影响使用 445 端口的服务）；
3. 打开网络，开启系统自动更新，并检测更新进行安装；

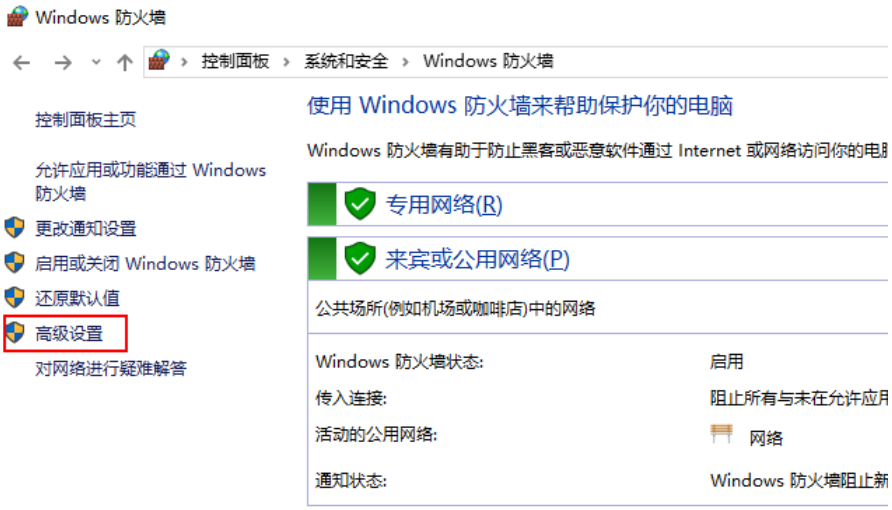
2.1.1 Win7、Win8、Win10 的处理流程：

1. 关闭网络

2. 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

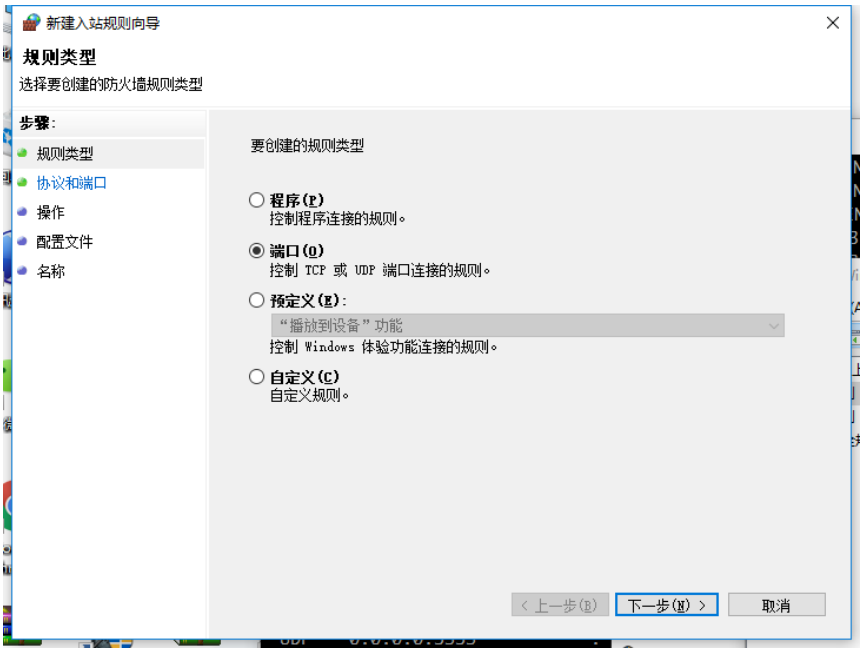
3. 选择启动防火墙，并点击确定

4. 点击高级设置

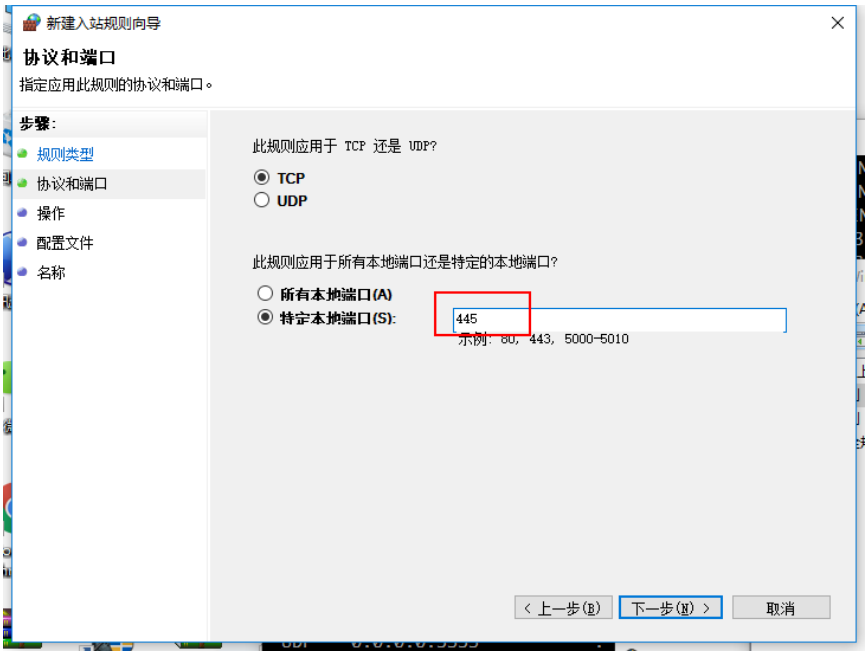


5. 点击入站规则，新建规则

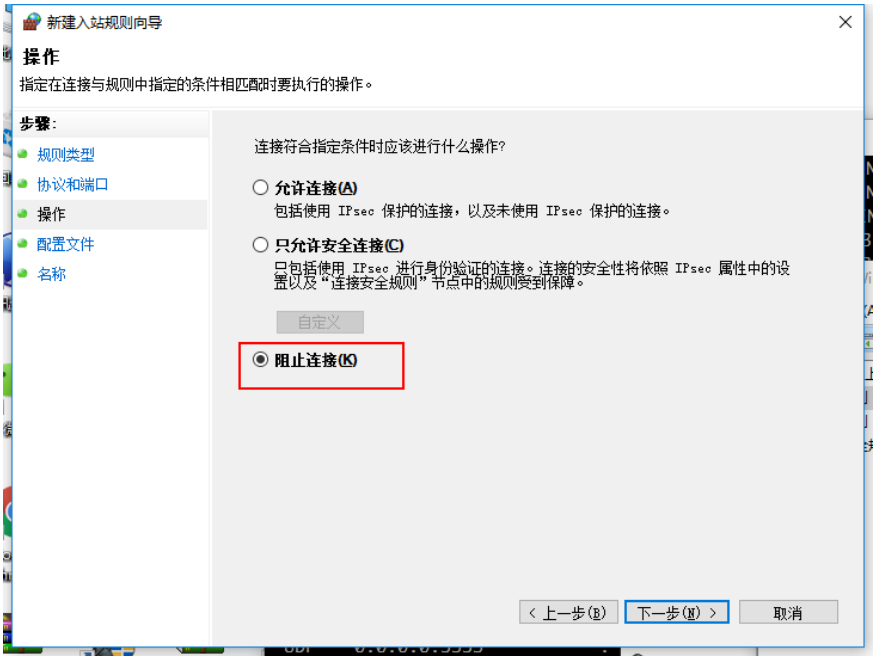
6. 选择端口、下一步



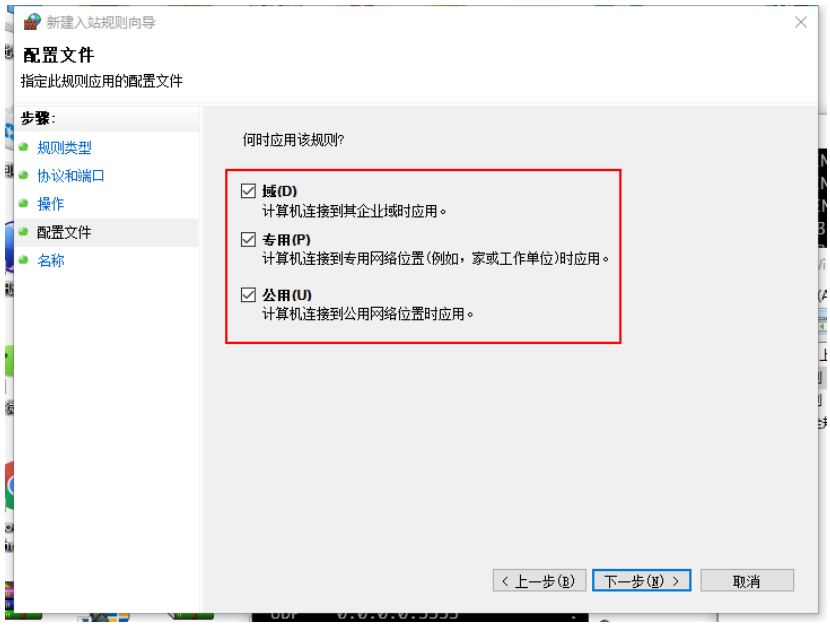
7. 选择特定本地端口，输入 445，下一步



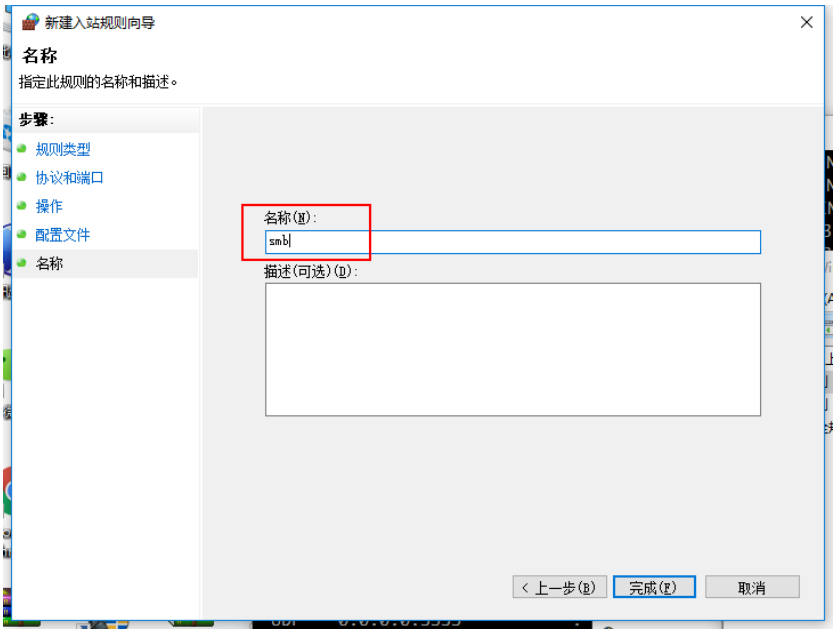
8. 选择阻止连接，下一步



9. 配置文件，全选，下一步

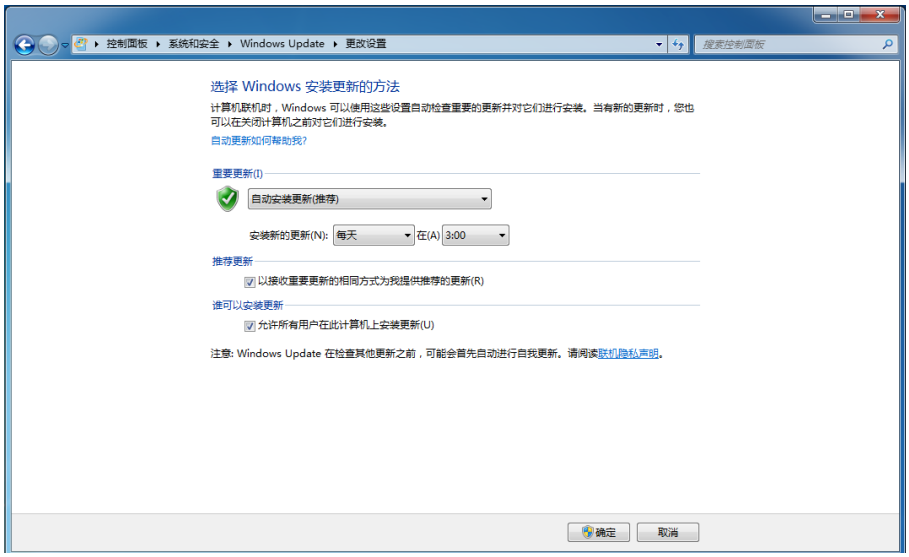


10. 名称，可以任意输入，完成即可。

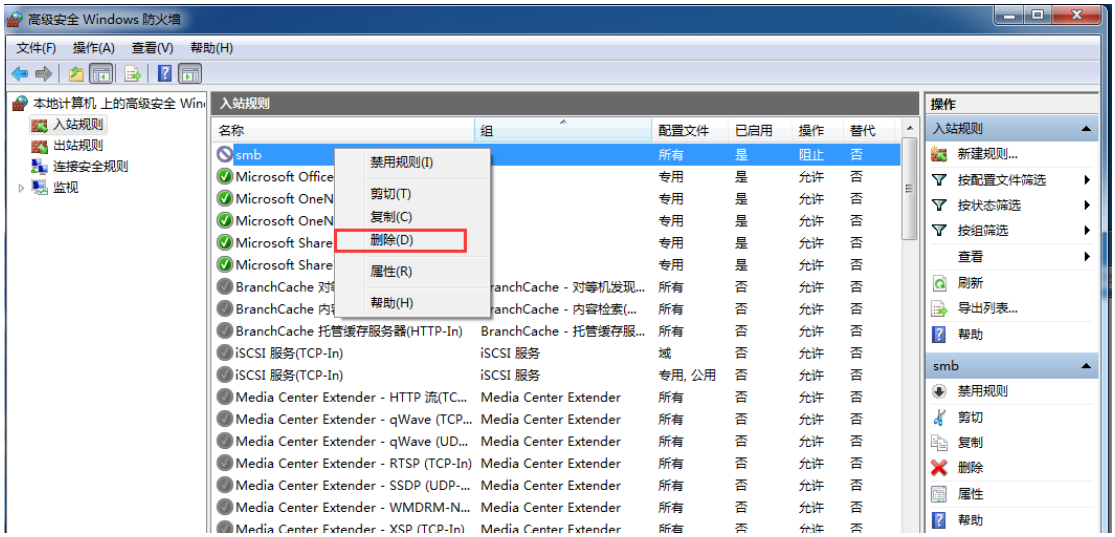


11. 恢复网络

12. 开启系统自动更新，并检测更新进行安装

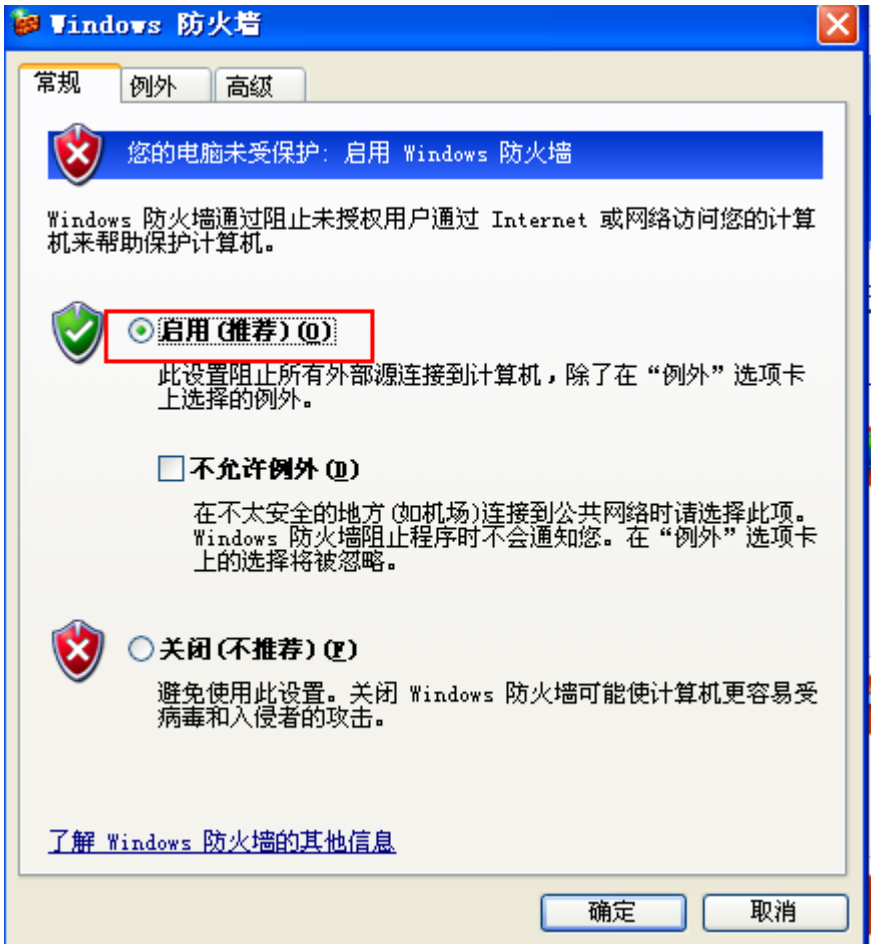


注：在系统更新完成后，如果业务需要使用 SMB 服务，将上面设置的防火墙入站规则删除即可。



2.1.2 XP 系统的处理流程

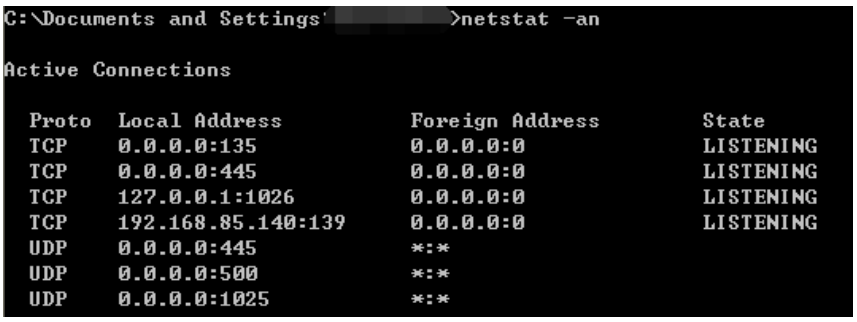
1、依次打开控制面板，安全中心，Windows 防火墙，选择启用



2、点击开始，运行，输入 cmd，确定执行下面三条命令禁止系统 SMB 机制

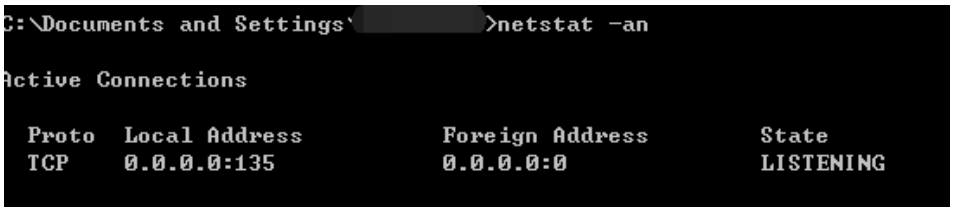
```
net stop rdr
net stop srv
net stop netbt
```

执行命令之前：



命令执行完成后，输入 netstat -an 验证是否还存在 445 的连接端口。如果还存在，使用 sc config netbt start= disabled 命令，执行后重启机器，再使用 netstat -an 验证。

执行命令后：



3、由于微软已经不再为 XP 系统提供系统更新，建议用户尽快升级到高版本系统。

2.2 关于已感染的用户群体的补救措施

目前无法解密该勒索软件加密的文件。但不建议因被非重要文件被加密向勒索者支付赎金。可采取的补救措施：

1. 断开内外网络，尽量组织追踪溯源，保护现场并取证。
2. 格式化所有硬盘，重新安装操作系统，并按照未感染勒索软件的处置方式做安全配置，如有数据备份，可恢复数据。
3. 系统性检查内外网系统的 445 SMB 服务端口开放情况，并及时处置。
4. 如果发现内网有感染的机器，及时断网关机隔离处理。同时通告运维人员切断内网的网络连接（如关闭交换机等网络连接设备），避免勒索软件的进一步扩散，内网的有关机器尽量做到断网关机，等候使用离线病毒查杀工具处理。
5. 如有重要文件数据幸存，做好备份处理。但并不能说明备份的数据中没有被感染，存储到磁盘后，同样等候使用离线病毒查杀工具处理。