应对勒索软件“永恒之蓝”

周一开机指南

什么叫“网络安全就在你身边”？

不是《网络安全法》，也不是新等保要求，而是“wannacry”给大家上了生动的一课！

第 1 步：断网、断网、断网 -- 开机前一定要断网(什么？你不知道怎么断网？有线直接拔网线、无线请关闭无线网卡或者直接关闭无线路由器！)

第 2 步：开机，开启系统防火墙，利用防火墙高级设置，阻止 445 端口的一切连接，(仅适用于 WIN7/WIN8/WIN10，运行时请使用管理员权限运行！切记)

下面介绍具体手动操作步骤如下：

Win7、Win8、Win10 的处理流程

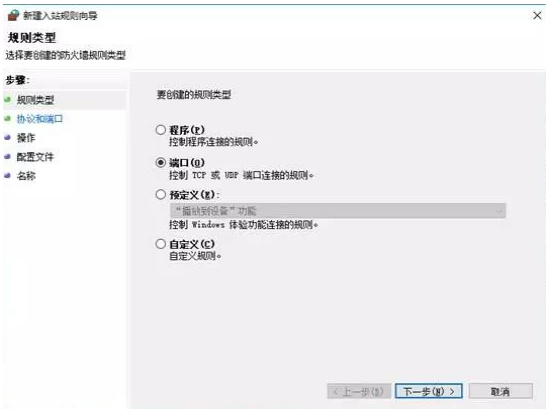
1）打开控制面板-系统与安全-Windows 防火墙，点击左侧“启动或关闭 Windows 防火墙”

2）选择“启动防火墙”，并点击“确定”

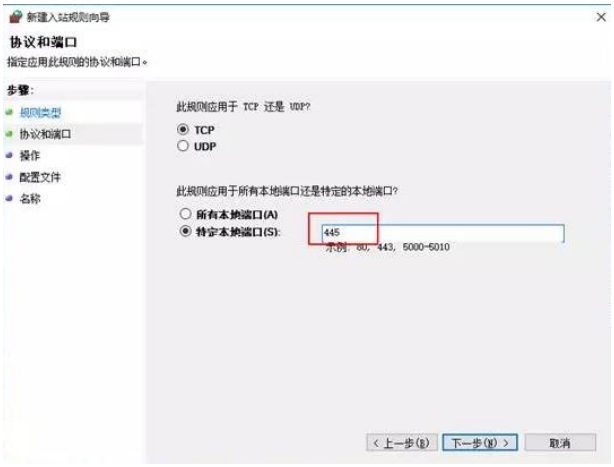
3）点击“高级设置”

4）点击“入站规则”，并点击“新建规则”

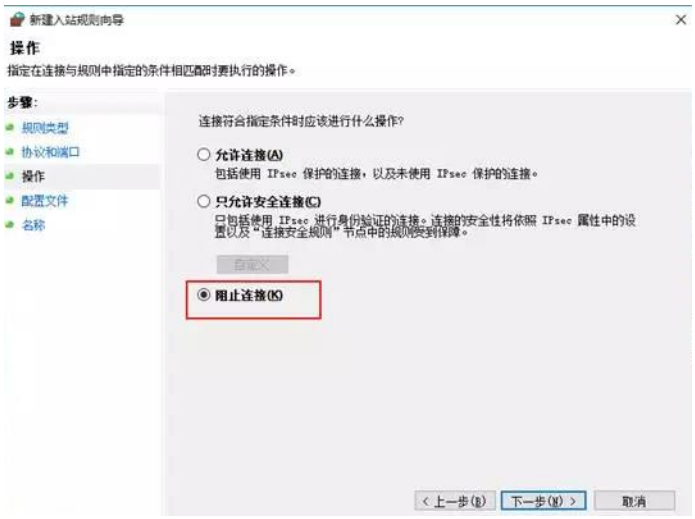
5）选择“端口”，点击“下一步”



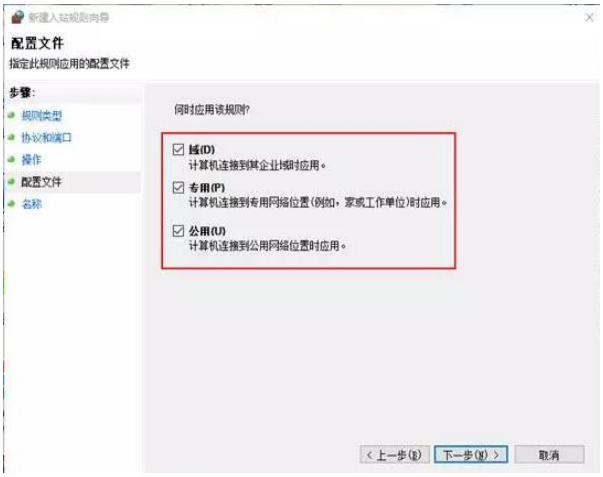
6）选择“特定本地端口”，并输入 445，点击“下一步”



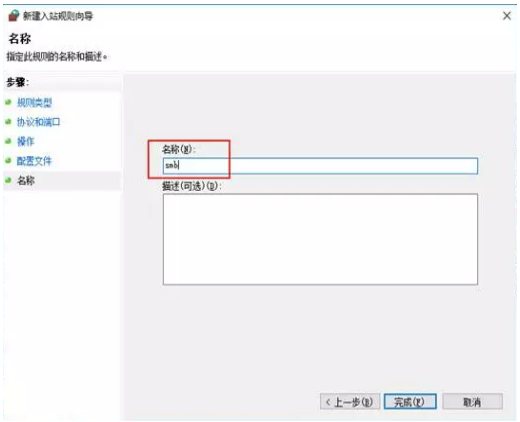
7）选择“阻止连接”，点击“下一步”



8）配置文件，全选，下一步

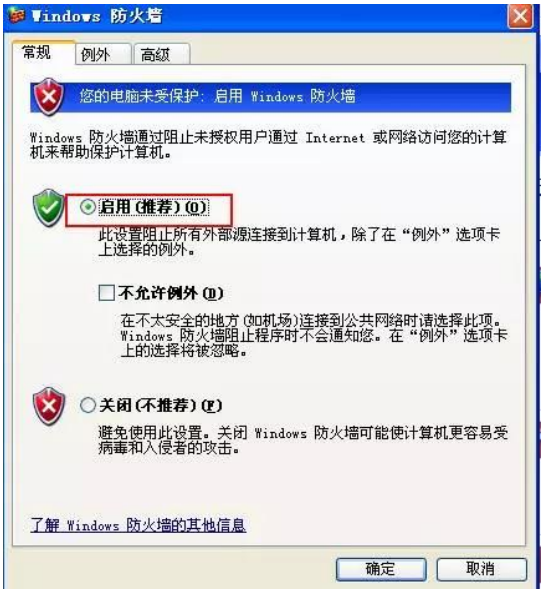


9）名称部分，可以任意输入，之后点击“完成”即可。



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”。



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
```

第 3 步：做好重要文件的备份工作（不是本地备份，是备份在其它存储介质中，如 U 盘，移动硬盘等，如云盘或者移动硬盘），当然做备份的前提是还未受到病毒感染！

第 4 步：下载操作系统补丁，更新你的系统。（不同系统的官方补丁下载地址如下，请根据自己电脑的位数下载。当然你也可以联网自动更新）

漏洞补丁下载

win7 x64 官方补丁下载地址：

（http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu）

win7 x86 官方补丁下载地址：

（http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x86_6bb04d3971bb58ae4bac44219e7169812914df3f.msu）

win10 x64 官方补丁下载地址：

（http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4012606-x64_e805b81ee08c3bb0a8ab2c5ce6be5b35127f8773.msu）

win10 x86 官方补丁下载地址：

（http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4012606-x86_8c19e23de2ff92919d3fac069619e4a8e8d3492e.msu）

XP 和 WIN2003 补丁下载地址：

（http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598）

第 5 步：下载专杀工具“景云反勒索防护系统”，更新景云杀毒病毒库，进行深度扫描查杀，以保障彻底清除勒索病毒；

下载专杀工具

（http://u.v-secure.cn/client/tools/辰信领创勒索病毒专杀 3.0.exe）

好吧，暂时安全了！

已感染的系统处理办法

如果你的电脑已经不幸感染了此病毒？只能交钱或者格盘重装系统了

这是很多同事可能会想到的办法，但是这是以牺牲数据为代价，如果确实有云盘备份或者移动硬盘备份，那么可以直接格盘重装，如果没有进行过备份，建议暂停使用受感染的电脑，相信随着全球各大安全厂家的介入，很快就会有解决办法。

其他专用查杀工具（选一即可）

启明星辰-景云病毒专杀
http://u.v-secure.cn/client/tools/辰信领创勒索病毒专杀 3.0.exe

360 工具
http://dl.360safe.com/nsa/nsatool.exe

腾讯工具
http://dlied6.qq.com/invc/xfspeed/qqpcmgr/download/VulDetector.exe

瑞星工具
http://download.rising.net.cn/zsgj/EternalBluemianyi.exe

安天工具
http://www.antiy.com/tools.html

教育技术与网络中心
2017 年 5 月 15 日