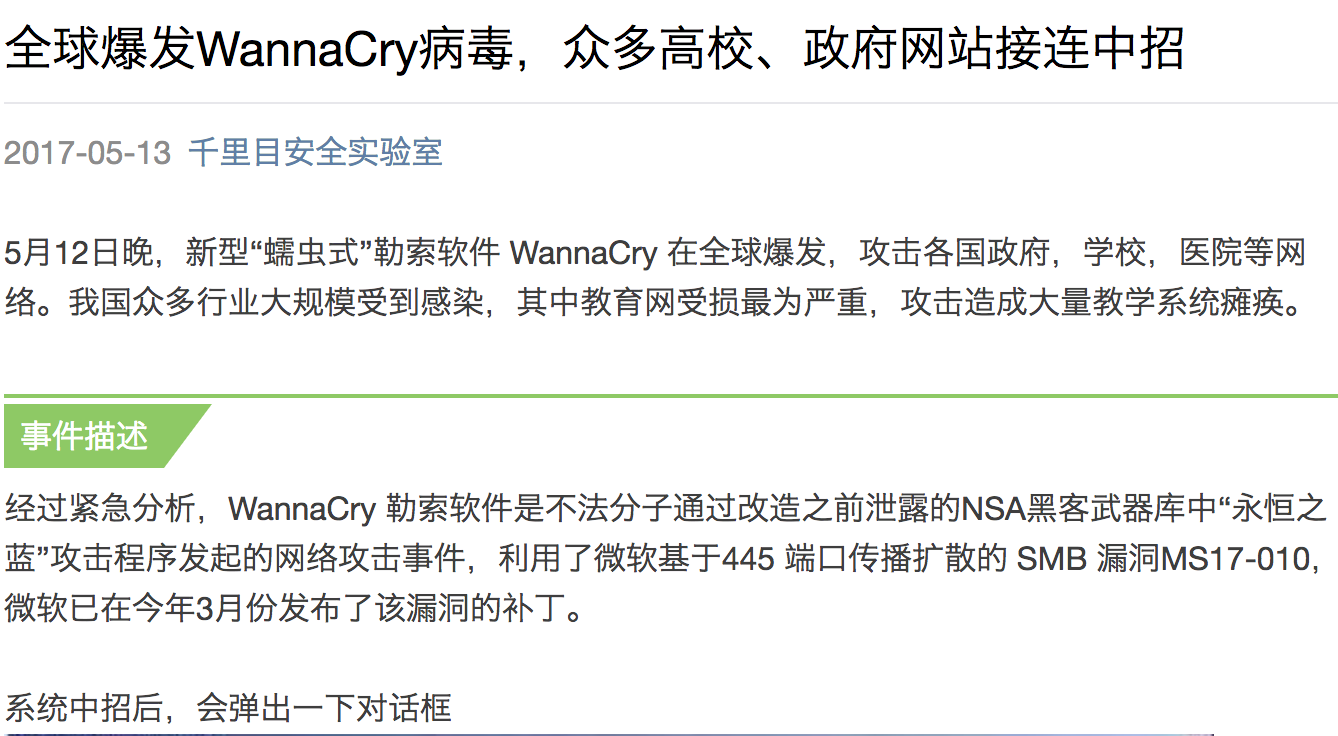
**上海市实验学校勒索病毒解决方案(1.0)**





**一、解决方案：**

1、升级针对MS17-010的微软的漏洞补丁，可以采用自动更新或下载更新补丁的方法，请下载相应操作系统的补丁，如发生提示不能安装则请核对操作系统版本，并联网升级。请按照相应版本复制到计算机本地运行（软件包已经在相应的文件夹内）：

**Windows 7 32位**

windows6.1-kb4012215-x86\_e5918381cef63f171a74418f12143dabe5561a66.msu

**Windows 10 32位**

windows10.0-kb4013429-x86\_8b376e3d0bff862d803404902c4191587afbf065.msu

**Windows XP**

windowsxp-kb4012598-x86-custom-chs\_dca9b5adddad778cfd4b7349ff54b51677f36775.exe

2、对于补丁失败的系统，可以禁止使用smb 服务的445端口：

通用方法如下（不同操作系统略有差异）：

* 【运行】输入“regedit”。
* 确定后定位到

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Servi ces\NetBT\Parameters目录。

* 新建名为“SMBDeviceEnabled”的DWORD值，并将其设置为 0，则可关闭 445 端口。

3、备份系统中的重要文件，请尽快进行备份；

**二、禁用445端口方法**

开启系统防火墙

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）

打开系统自动更新，并检测更新进行安装

2.1  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



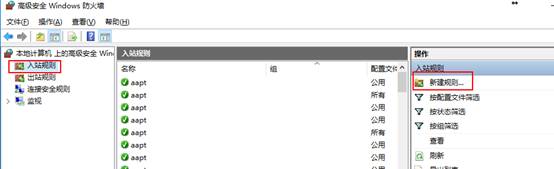
   2、选择启动防火墙，并点击确定



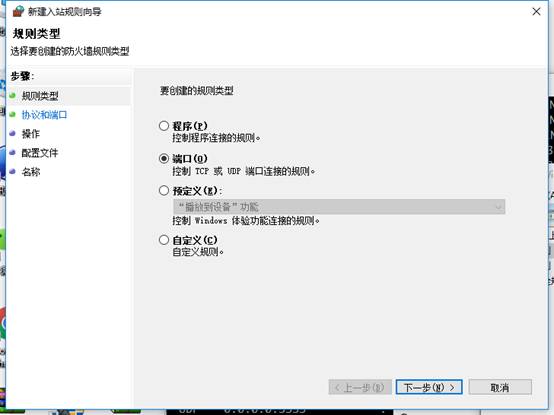
  3、点击高级设置



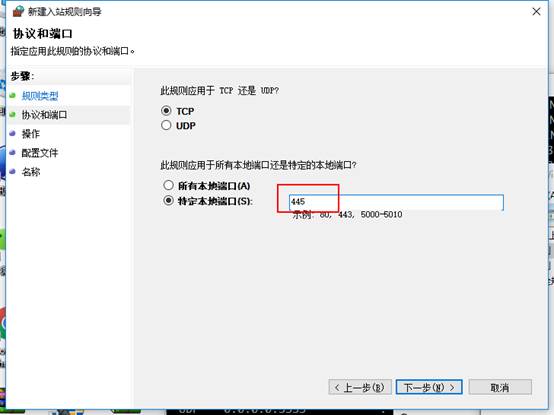
 4、点击入站规则，新建规则



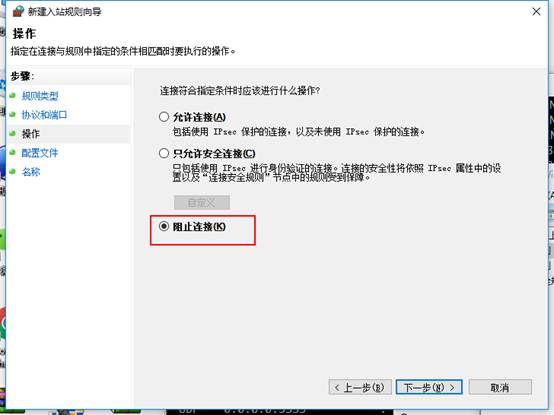
 5、选择端口，下一步



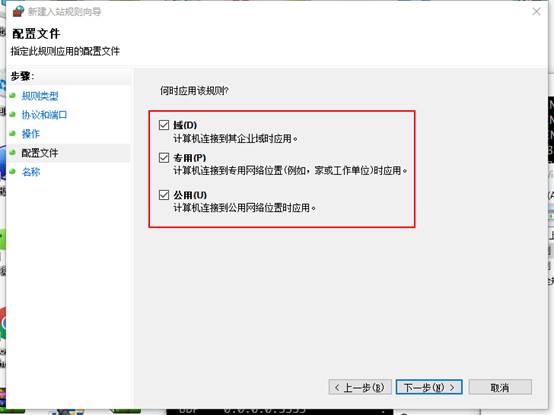
6、特定本地端口，输入445，下一步



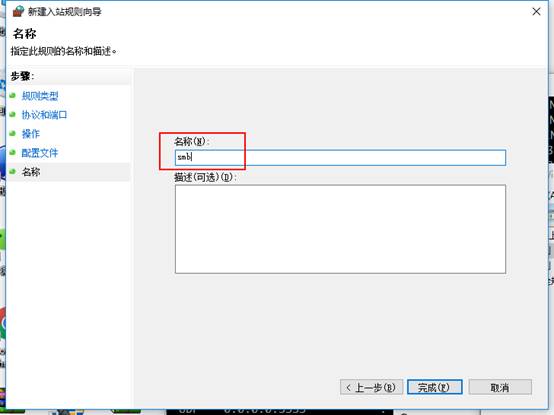
7、选择阻止连接，下一步



8、配置文件，全选，下一步

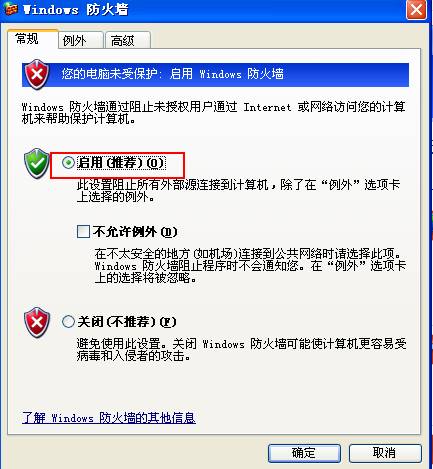


9、名称，可以任意输入，完成即可。



2.2  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

net  stop rdr

net  stop srv

net  stop netbt

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。