应对 Windows 操作系统勒索软件“WannaCry”处置手册

参考：CNCERT 应对 Windows 操作系统勒索软件“WannaCry”处置手册（网址：http://www.cnvd.org.cn/webinfo/show/4140）

一、确认主机是否被感染

被感染主机会在屏幕显示类似如下的支付赎金通知的界面：

二、被感染主机处置流程

1）将该主机隔离或断网（拔网线）；

2）使用 PE 盘进入操作系统，将可用文件进行备份，并对备份数据进行离线处理；

3）重新安装操作系统，或者利用安天发布的专杀工具[1]清除主机中的勒索软件；

4）若采用专杀工具方式清除主机中勒索软件，则可以利用 360 发布的文件恢复工具[4]尝试恢复部分被勒索软件加密的文档；

5）根据未感染主机处置流程对主机进行安全防护；

6）若存在该主机备份，则启动备份恢复程序。

三、未感染主机处置流程

对于未感染主机，可以通过手动修改配置或者使用免疫工具进行防护，避免主机被感染。

1、手动修改系统安全配置

主要流程概括如下：

1）关闭网络，开启系统防火墙；

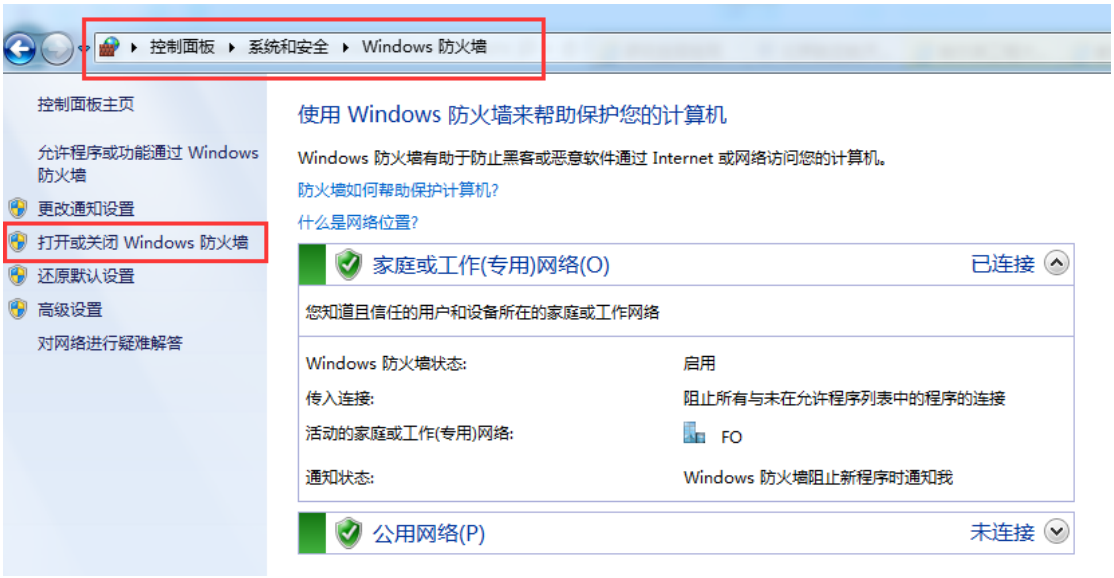
2）利用系统防火墙高级设置阻止向 445 端口进行连接（该操作会影响使用 445 端口的服务）及网络共享或者手动停止 SMB 服务；

3）打开网络，升级操作系统补丁。建议使用 win10 系统的用户，尽快将系统升级到 1703 版本。

1.1 Win7、Win8、Win10 的处理流程

1）关闭网络

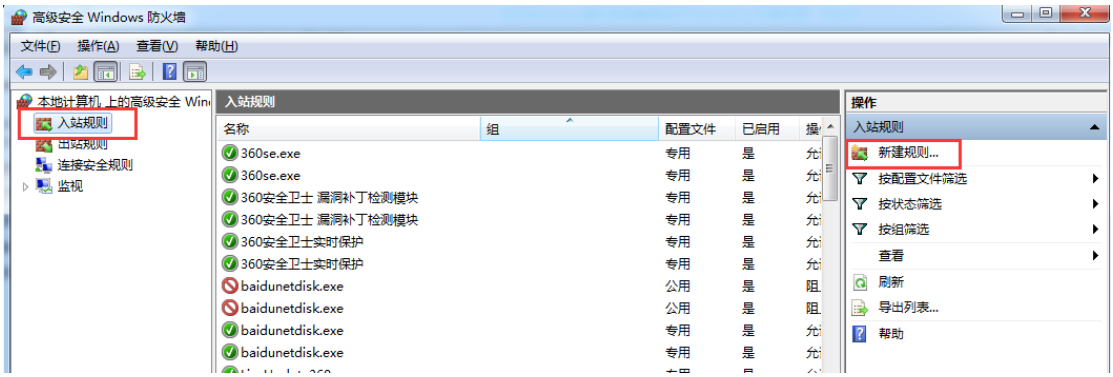
2）打开控制面板-系统与安全-Windows 防火墙，点击左侧启动或关闭 Windows 防火墙



3）选择启动防火墙，并点击确定

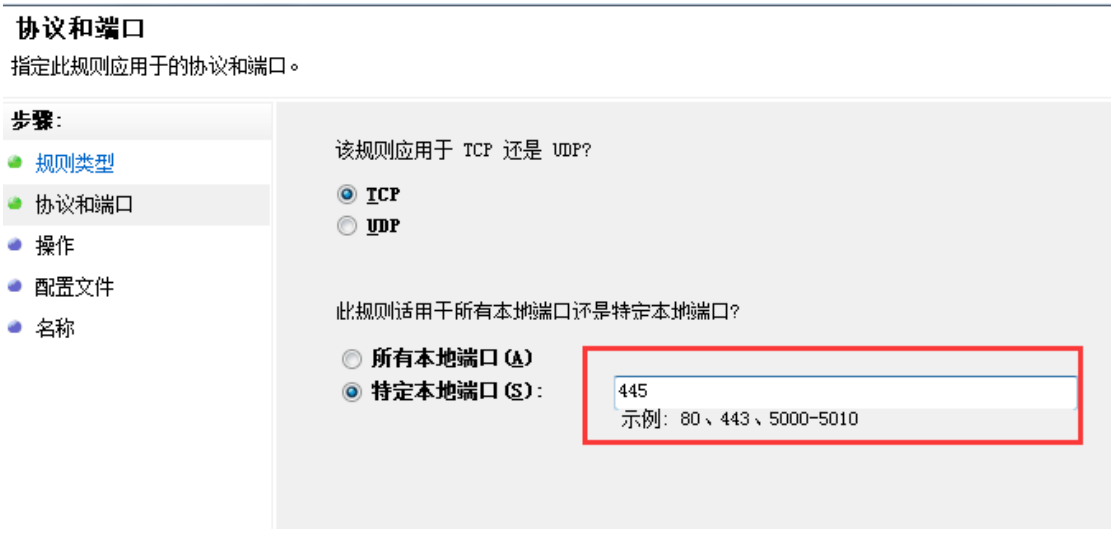
4）点击高级设置

5）点击入站规则，新建规则，以 445 端口为例

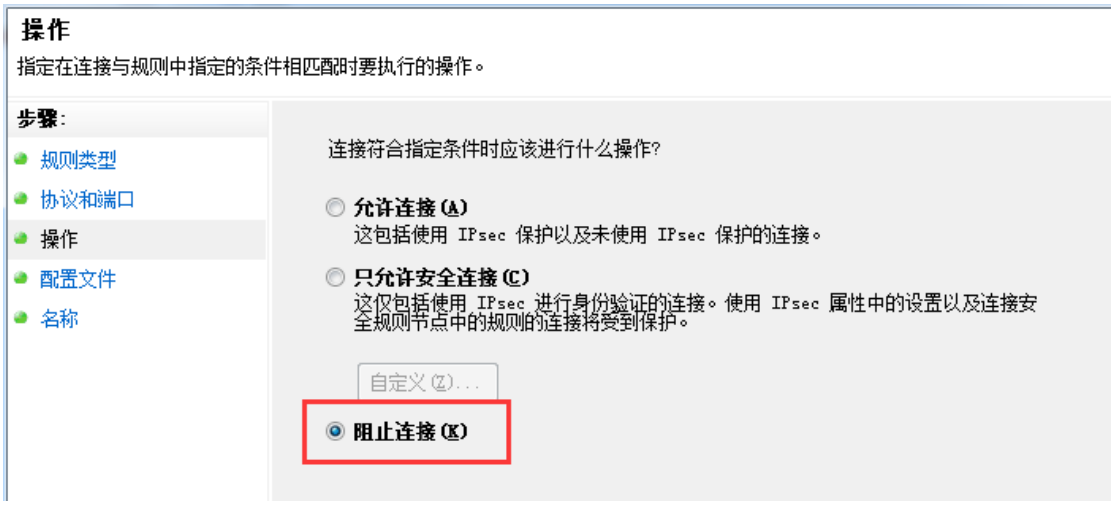


6）选择端口、下一步

7）选择特定本地端口，输入 445，下一步

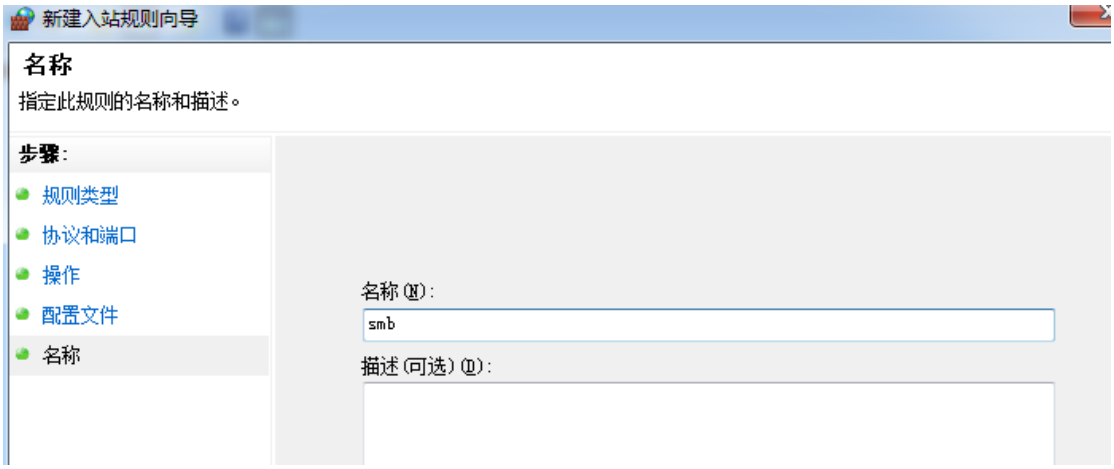


8）选择阻止连接，下一步



9）配置文件，默认全选，下一步

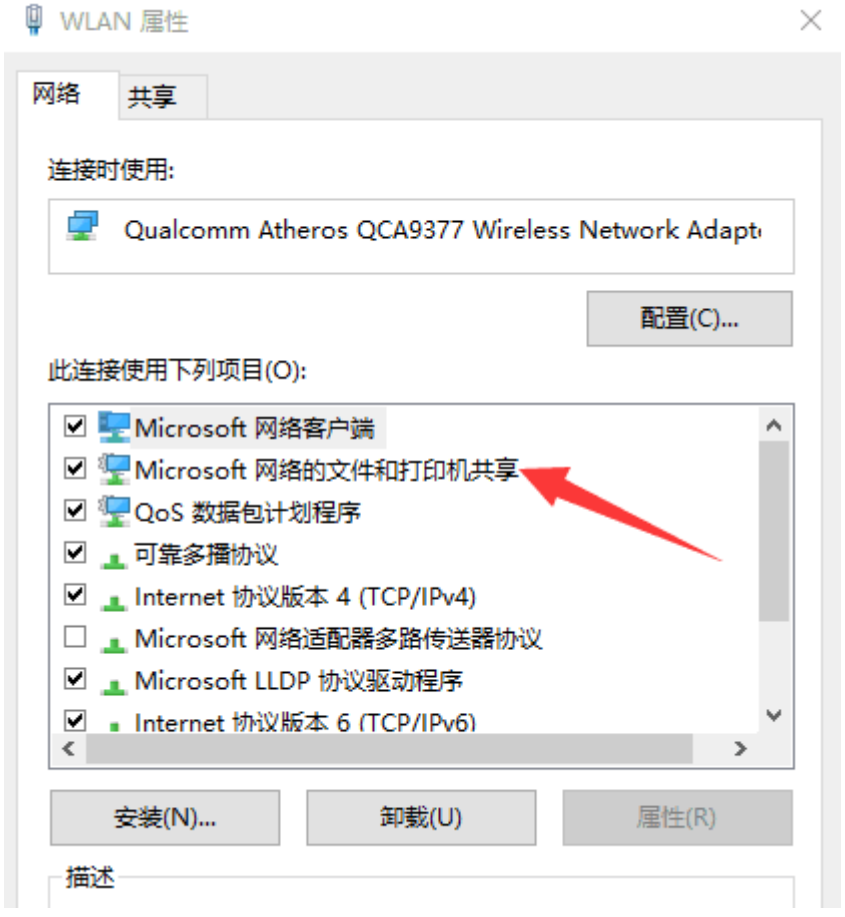
10）设置名称，可以任意输入，完成即可。



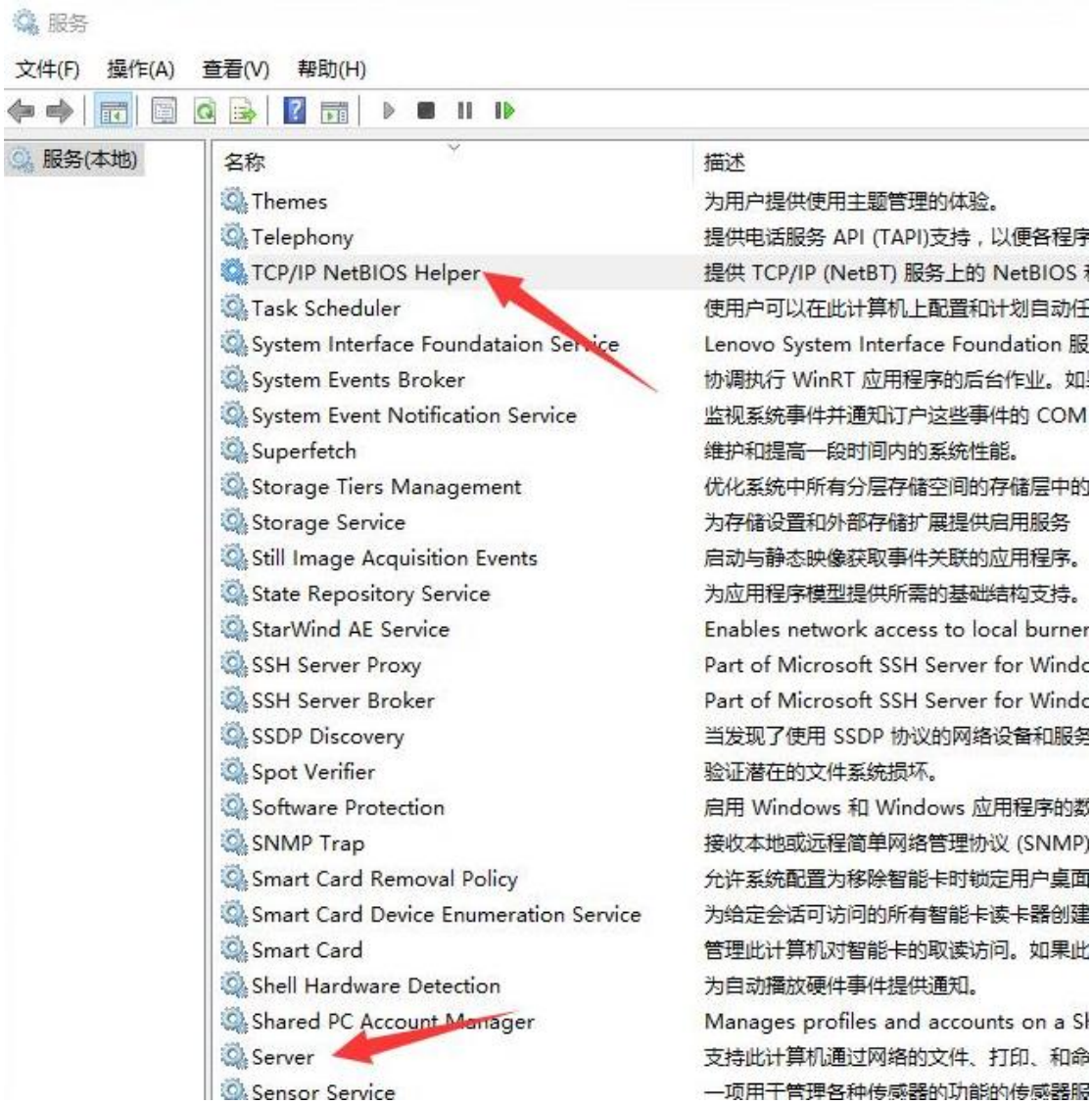
11）手动停止 SMB 服务

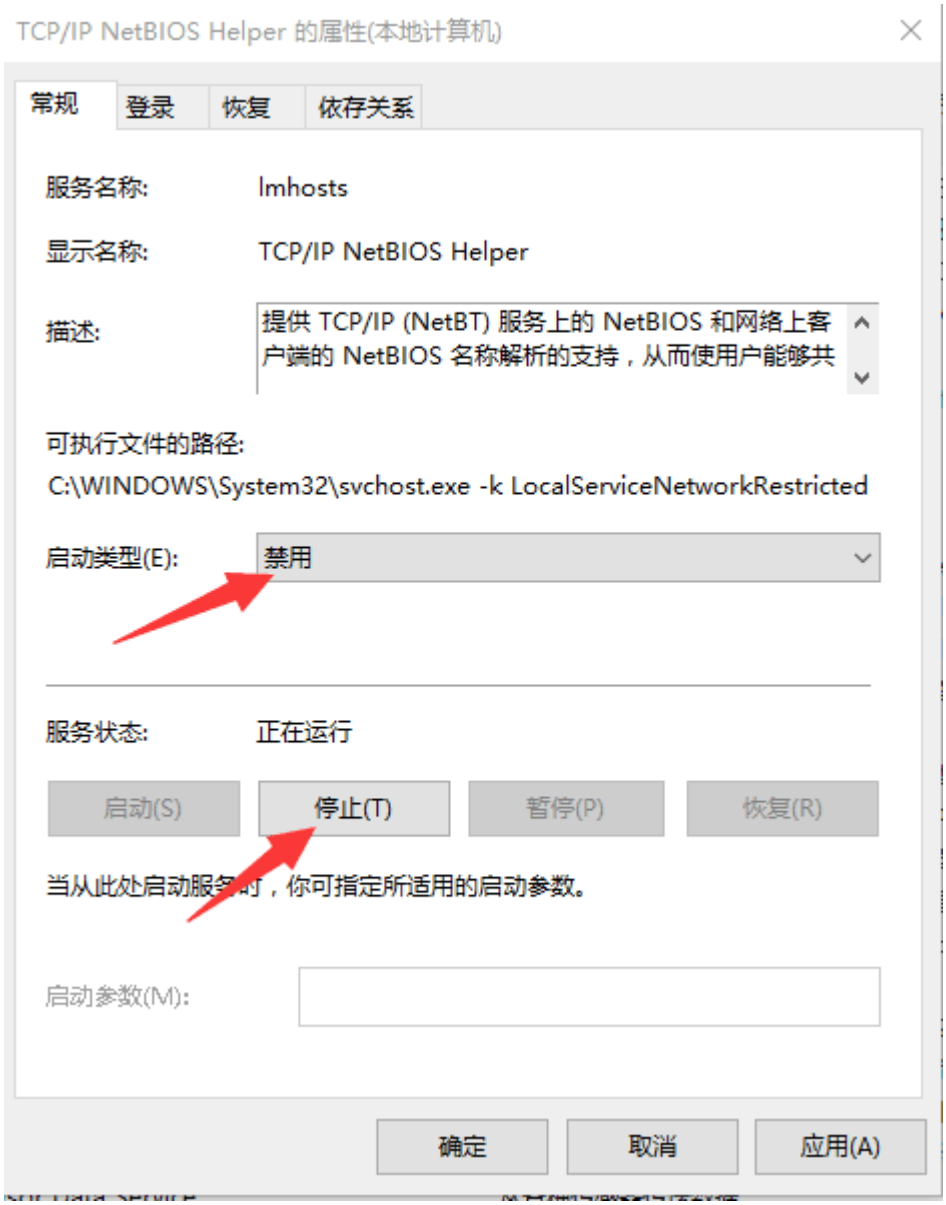
控制面板→网络与共享中心→更改适配器设置→选择当前连接的网络图标→右键属性→取消对“Microsoft 网络的文件和打印机共享”的勾选→确定


控制面板\网络和 Internet\网络连接
控制面板 › 网络和 Internet › 网络连接
文件(F) 编辑(E) 查看(V) 高级(N) 工具(T)
组织
My VPN
已断开连接
WAN Miniport (IKEv2)
WLAN
HEU-GUEST
以太网
网络电缆被拔出
Intel(R) Ethernet Connection (4...


WLAN 属性
网络
共享
连接时使用:
Qualcomm Atheros QCA9377 Wireless Network Adapt
配置(C)...
此连接使用下列项目(O):
Microsoft 网络客户端
Microsoft 网络的文件和打印机共享
QoS 数据包计划程序
可靠多播协议
Internet 协议版本 4 (TCP/IPv4)
Microsoft 网络适配器多路传送器协议
Microsoft LLDP 协议驱动程序
Internet 协议版本 6 (TCP/IPv6)
安装(N)...
卸载(U)
属性(R)
描述

计算机右键→选择管理菜单→展开服务和应用程序菜单→点击服务菜单→禁用“sever”、“TCP/IP NetBIOS Helper”服务




TCP/IP NetBIOS Helper 的属性(本地计算机)
常规
登录
恢复
依存关系
服务名称:
lmhosts
显示名称:
TCP/IP NetBIOS Helper
描述:
提供 TCP/IP (NetBT) 服务上的 NetBIOS 和网络上客户端的 NetBIOS 名称解析的支持，从而使用户能够共
可执行文件的路径:
C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted
启动类型(E):
禁用
服务状态:
正在运行
启动(S)
停止(T)
暂停(P)
恢复(R)
当从此处启动服务时，你可指定所适用的启动参数。
启动参数(M):
确定
取消
应用(A)

11）恢复网络

12）升级操作系统补丁

任何升级都可能带来不可预见的问题，因此请提前对重要数据进行备份。

方法一：自动安装补丁

开启系统自动更新，并检测更新进行安装

方法二：手动安装补丁（以 Windows7 为例）

步骤一、查看操作系统版本

1、开始菜单“计算机”右键选择“属性”；

2、弹出的系统属性中，可以查看版本。

3、到微软官方网站【9】或者学校 FTP【10】下载对应版本的补丁，下载后手动安装。安装完毕后，按照系统提示重新启动电脑。

注：学校 FTP 补丁从微软官方网站下载，但受用户电脑软硬件、操作系统等环境影响，不能保证所有系统都能安装成功，请您谨慎操作，升级前做好文件备份工作。

FTP 目录 /patch/MS17-010%20%B8%FC%D0%C2%B0%FC/ 位于 ftp.hrbeu.edu.cn

若要在文件资源管理器中查看此 FTP 站点，请单击“视图”，然后单击“在文件资源管理器中打开 FTP 站点”。

转到高层目录

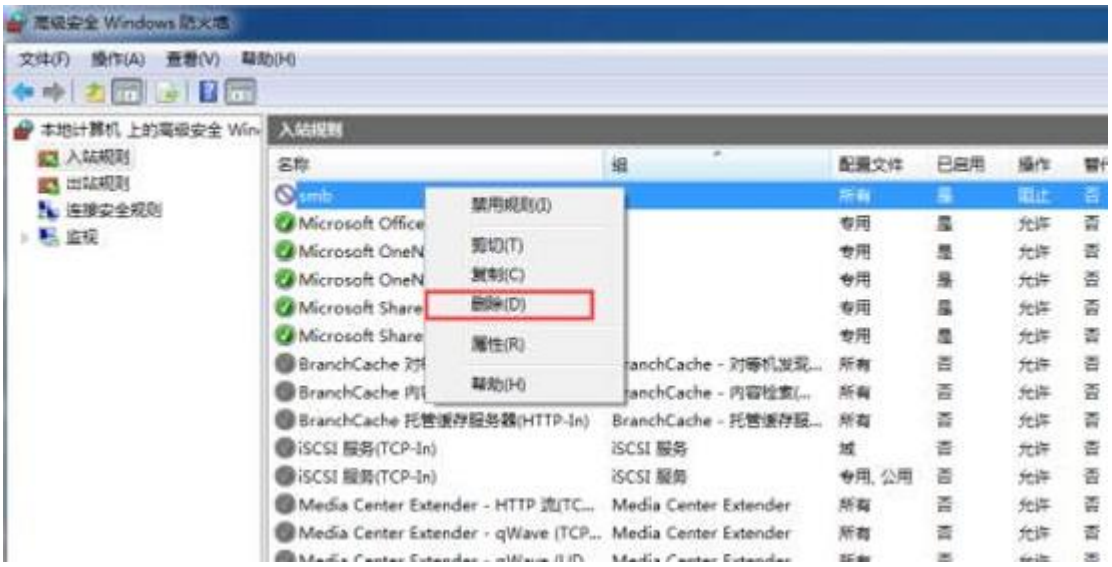
05/13/2017 09:42上午	1,132,391,933	Windows 10 Version 1511 64位系统更新包-KB4013198.msu
05/13/2017 09:26上午	607,275,721	Windows 10 Version 1607 32位系统更新包-KB4013429.msu
05/13/2017 09:33上午	1,105,744,002	Windows 10 Version 1607 64位系统更新包-KB4013429.msu
05/13/2017 08:53上午	597,308,991	Windows 10 version 1511 32位系统更新包-KB4013198.msu
05/13/2017 08:38上午	527,401,823	Windows 10 （2015年7月初始版）32位系统更新包-KB4012606.msu
05/13/2017 09:20上午	1,126,641,287	Windows 10 （2015年7月初始版）64位系统更新包-KB4012606.msu
05/14/2017 02:57上午	19,729,107	Windows 7 SP1 32位系统更新包-KB4012212.msu
05/14/2017 02:54上午	34,790,450	Windows 7 SP1 64位系统更新包-KB4012212.msu
05/13/2017 09:59上午	893,501	Windows 8 32位系统更新包-KB4012598.msu
05/13/2017 10:03上午	1,008,565	Windows 8 64位系统更新包-KB4012598.msu
05/13/2017 08:56上午	25,342,912	Windows 8.1 32位系统更新包-KB4012213.msu
05/13/2017 09:02上午	38,813,702	Windows 8.1 64位系统更新包-KB4012213.msu
05/13/2017 09:20上午	705,272	Windows Server 2003 32位系统更新包-KB4012598.exe
05/14/2017 02:31上午	980,728	Windows Server 2003 64位系统更新包-KB4012598.exe
05/14/2017 02:38上午	36,137,230	Windows Server 2008 R2 SP 1 Itanium系统更新包-KB4012598.msu
05/13/2017 08:44上午	34,790,450	Windows Server 2008 R2 SP 1 64位系统更新包-KB4012598.msu
05/14/2017 02:51上午	1,237,796	Windows Server 2008 SP 2 32位系统更新包-KB4012598.msu
05/14/2017 02:50上午	1,384,825	Windows Server 2008 SP 2 64位系统更新包-KB4012598.msu
05/14/2017 02:48上午	1,209,596	Windows Server 2008 SP 2 Itanium系统更新包-KB4012598.msu
05/14/2017 03:07上午	38,813,702	Windows Server 2012 R2 系统更新包-KB4012213.msu
05/14/2017 03:03上午	27,899,294	Windows Server 2012 系统更新包-KB4012214.msu
05/14/2017 03:30上午	733,806,940	Windows Server 2016 64位系统更新包-KB4013429.msu
05/14/2017 02:42上午	1,237,796	Windows Vista SP 2 32位系统更新包-KB4012598.msu
05/14/2017 02:46上午	1,384,825	Windows Vista x64 Edition SP 2 64位系统更新包-KB4012598.msu
05/14/2017 04:02上午	683,760	Windows XP SP3 32位系统更新包-KB4012598.exe
05/13/2017 09:33上午	974,072	Windows XP SP3 64位系统更新包- KB4012598.exe

4、检查是否安装成功

查看更新历史记录

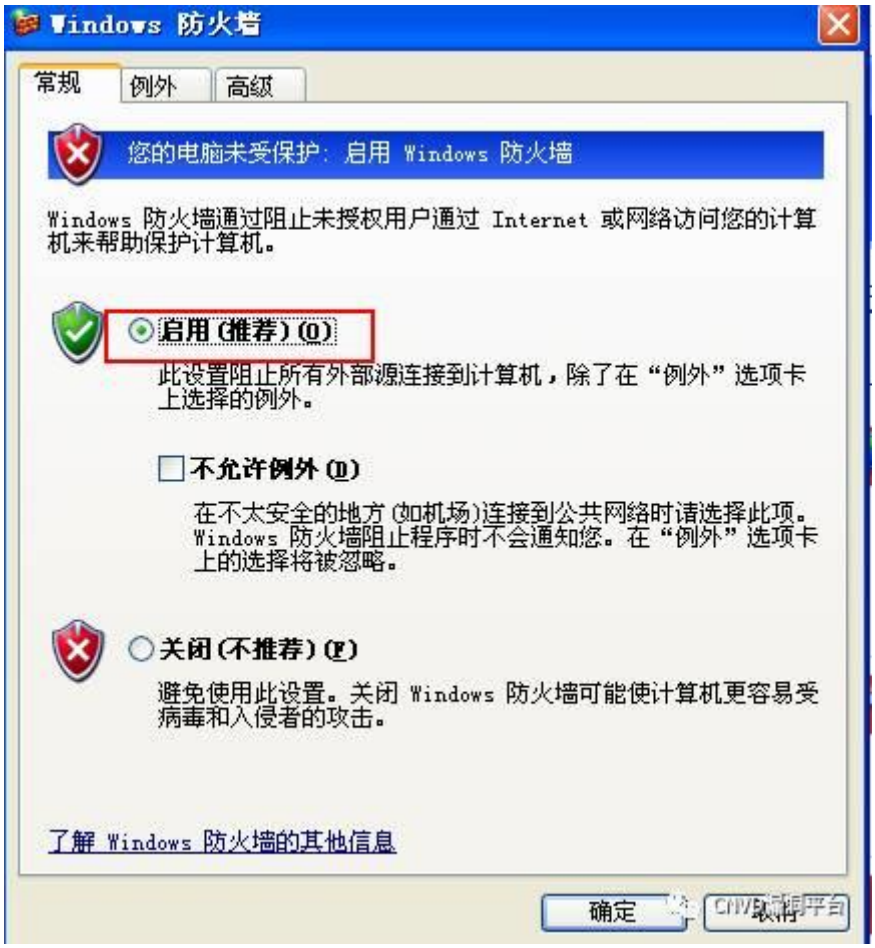
搜索对应版本号的更新记录，查看是否安装成功。

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。

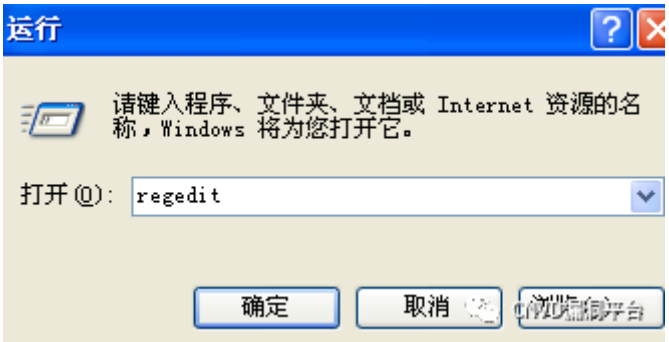


1.2 XP 系统的处理流程

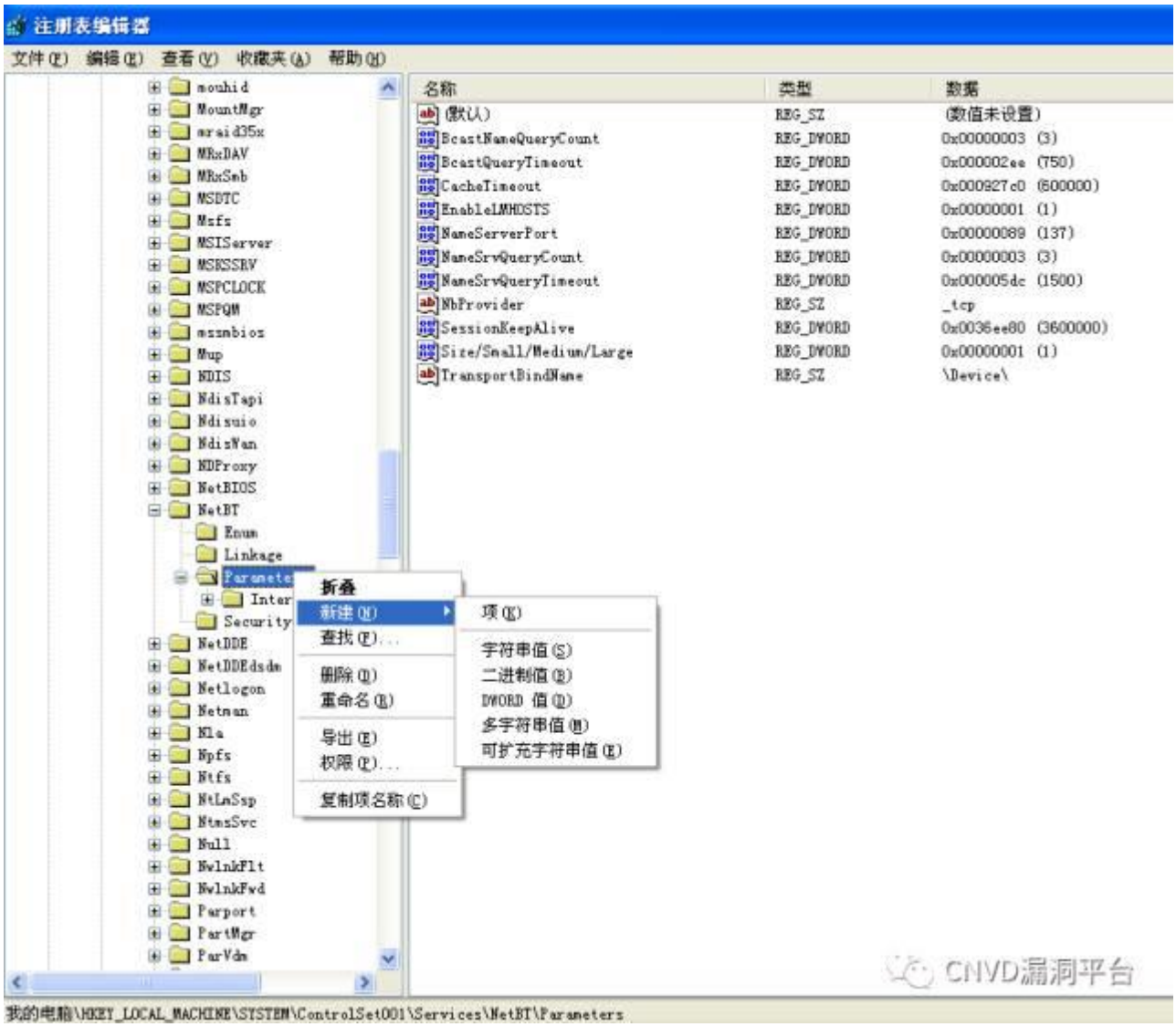
1）依次打开控制面板，安全中心，Windows 防火墙，选择启用。



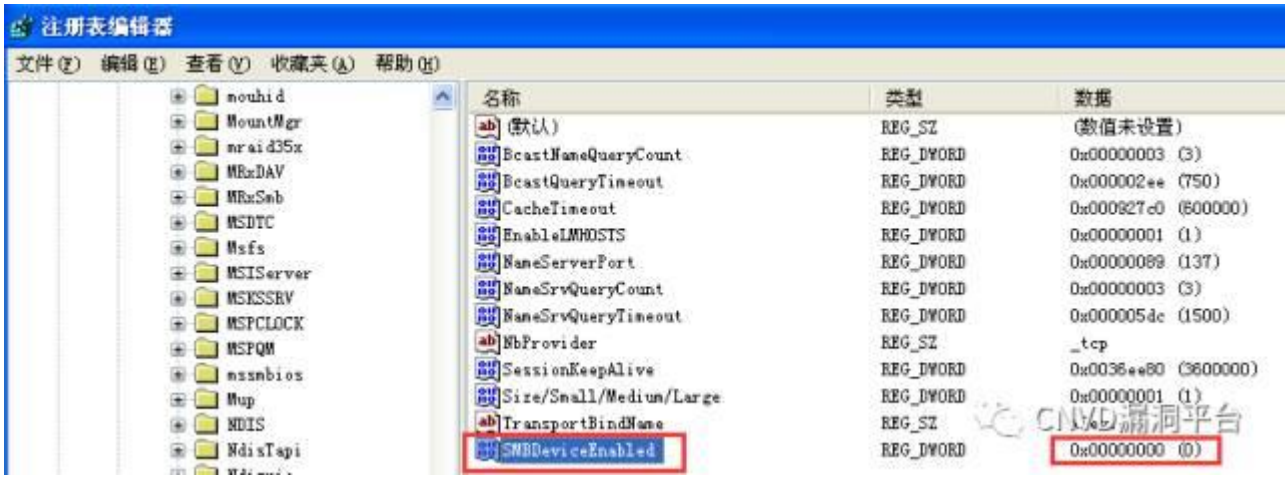
2）通过注册表关闭 445 端口，单击“开始”——“运行”，输入“regedit”，单击“确定”按钮，打开注册表。



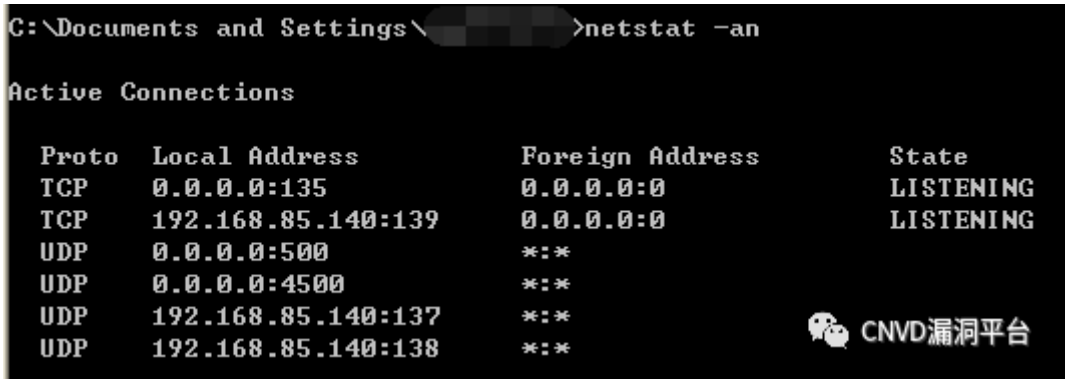
3）找到 HKEY_LOCAL_MACHINE\System\Controlset\Services\NetBT\Parameters，选择“Parameters”项，右键单击，选择“新建”——“DWORD 值”。



4）将 DWORD 值命名为“SMBDeviceEnabled”，值修改为 0。



5）重启机器，查看 445 端口连接已经没有了。



6）安装微软总部针对该漏洞（MS17-010）发布的特别补丁[5]。

参考

[1]蠕虫勒索软件专杀工具（WannaCry）（安天提供）：

http://www.antiy.com/response/wannacry/ATScanner.zip

[2]蠕虫勒索软件免疫工具（WannaCry）（安天提供）：

http://www.antiy.com/response/wannacry/Vaccine_for_wannacry.zip

[3]“永恒之蓝”勒索蠕虫（WannaCry）检测工具（360 提供）

http://b.360.cn/other/onionwormkiller

[4]勒索病毒份文件恢复工具（360 提供）：

https://dl.360safe.com/recovery/RansomRecovery.exe

[5]微软总部决定对已停服的 XP 和部分服务器版本发布特别补丁公告

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-WannaCrypt-attacks/

[6]安天应对勒索软件“wannacry”配置指南

http://www.antiy.com/response/Antiy_Wannacry_Protection_Manual/Antiy_Wannacry_Protection_Manual.html

[7] 安天应对勒索软件“WannaCry”开机指南

http://www.antiy.com/response/Antiy_Wannacry_Guide.html

[8] 360 针对“永恒之蓝”攻击紧急处置手册（蠕虫 WannaCry）

http://zt.360.cn/1101061855.php?dtid=1101062514&did=490458365

【9】微软补丁下载地址

https://technet.microsoft.com/zh-cn/library/security/MS17-010

【10】学校 FTP 地址

ftp://ftp.hrbeu.edu.cn/patch