互联网网络安全信息通报

国家计算机网络应急技术处理协调中心广东分中心　　5 月 13 日

“ wannacry ”

1.概述

1

Ooops, your files have been encrypted!

我的电脑出了什么问题？

您的一些重要文件被我加密保存了。

照片、图片、文档、压缩包、音频、视频文件、exe文件等，几乎所有类型的文件都被加密了，因此不能正常打开。

这和一般文件损坏有本质上的区别。您大可在网上找找恢复文件的方法，我敢保证，没有我们的解密服务，就算老天爷来了也不能恢复这些文档。

有没有恢复这些文档的方法？

当然有可恢复的方法。只能通过我们的解密服务才能恢复。我以人格担保，能够提供安全有效的恢复服务。

但这是收费的，也不能无限期的推迟。

请点击 <Decrypt> 按钮，就可以免费恢复一些文档。请您放心，我是绝不会骗你的。

但想要恢复全部文档，需要付款点费用。

是否随时都可以固定金额付款，就会恢复的吗，当然不是，推迟付款时间越长对你不利。

最好3天之内付款费用，过了三天费用就会翻倍。

还有，一个礼拜之内未付款，将会永远恢复不了。

对了，忘了告诉你，对半年以上没钱付款的穷人，会有活动免费恢复，能否轮

Send $300 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

●

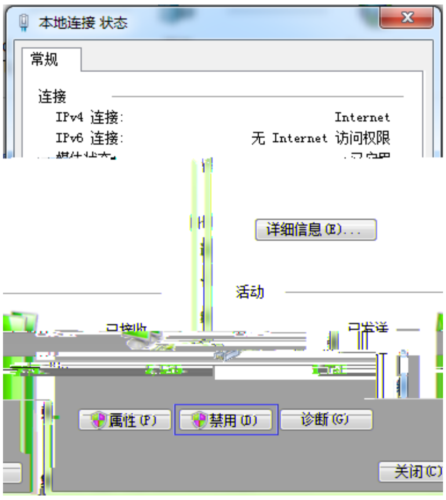
● 445

445

●

Win7 Win8 Win10

1)


本地连接 状态

常规

连接

IPv4 连接: Internet

IPv6 连接: 无 Internet 访问权限

2) - -Windows Windows


Windows 防火墙

控制面板 › 系统和安全 › Windows 防火墙

使用 Windows 防火墙来帮助保护你的电脑

Windows 防火墙有助于防止黑客或恶意软件通过 Internet 或网络访问你的电脑。

更新防火墙设置

Windows 防火墙未使用推荐的设置来保护计算机。

推荐的设置有哪些?

专用网络(R) 未连接

来宾或公用网络(P) 已连接

公共场所(例如机场或咖啡店)中的网络

3)


自定义各类网络的设置

你可以修改使用的每种类型的网络的防火墙设置。

专用网络设置

● 启用 Windows 防火墙

☐ 阻止所有传入连接，包括位于允许应用列表中的应用

☑ Windows 防火墙阻止新应用时通知我

○ 关闭 Windows 防火墙(不推荐)

公用网络设置

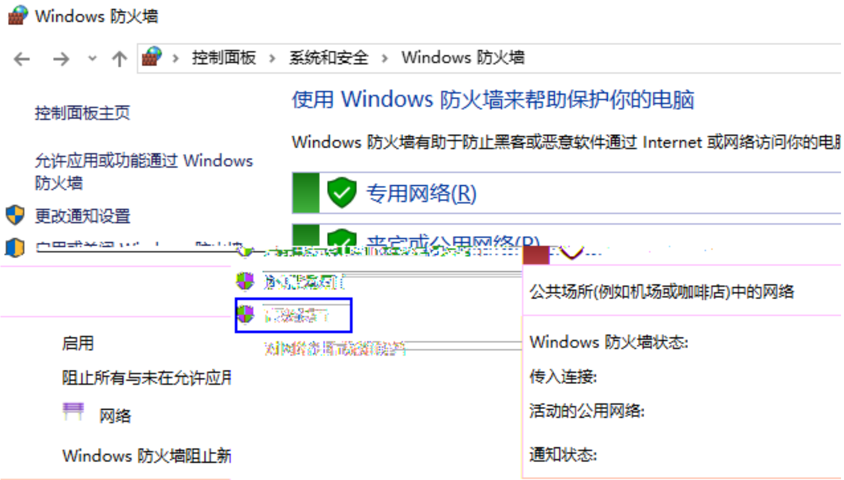
● 启用 Windows 防火墙

☐ 阻止所有传入连接，包括位于允许应用列表中的应用

☑ Windows 防火墙阻止新应用时通知我

○ 关闭 Windows 防火墙(不推荐)

4)



Windows 防火墙

控制面板 › 系统和安全 › Windows 防火墙

控制面板主页

允许应用或功能通过 Windows 防火墙

更改通知设置

使用 Windows 防火墙来帮助保护你的电脑

Windows 防火墙有助于防止黑客或恶意软件通过 Internet 或网络访问你的电脑

专用网络(R)

来宾或公用网络(P)

公共场所(例如机场或咖啡店)中的网络

Windows 防火墙状态:

传入连接:

活动的公用网络:

通知状态:

启用

阻止所有与未在允许应用

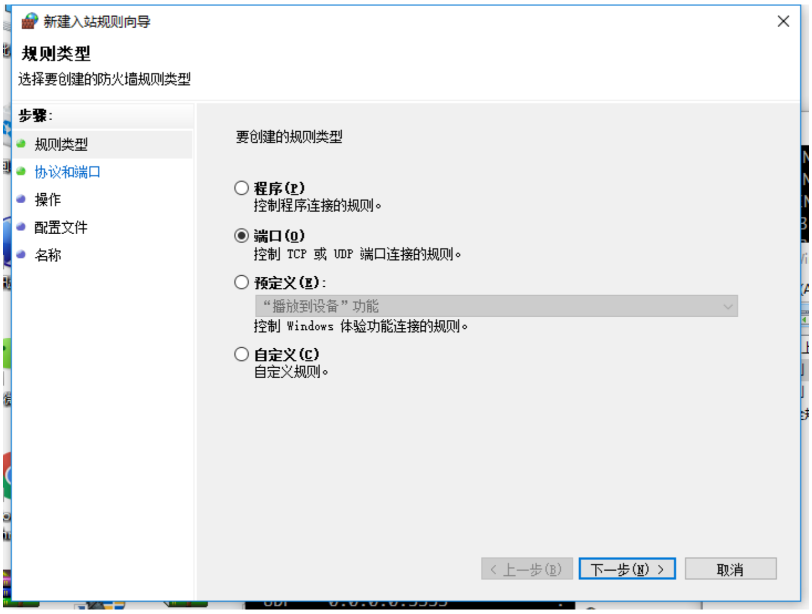
网络

Windows 防火墙阻止新

5) 445

高级安全 Windows 防火墙

6)



新建入站规则向导

规则类型

选择要创建的防火墙规则类型

步骤:
- 规则类型
- 协议和端口
- 操作
- 配置文件
- 名称

要创建的规则类型

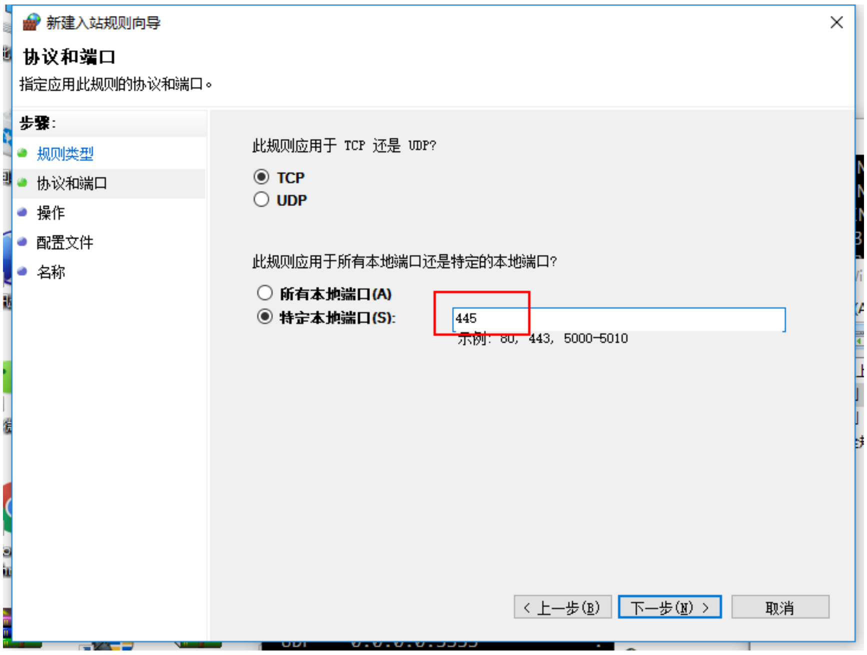
○ **程序(P)**
控制程序连接的规则。

● **端口(O)**
控制 TCP 或 UDP 端口连接的规则。

○ **预定义(E):**
"播放到设备" 功能
控制 Windows 体验功能连接的规则。

○ **自定义(C)**
自定义规则。

7) 445



新建入站规则向导

协议和端口

指定应用此规则的协议和端口。

步骤:
- 规则类型
- 协议和端口
- 操作
- 配置文件
- 名称

此规则应用于 TCP 还是 UDP?

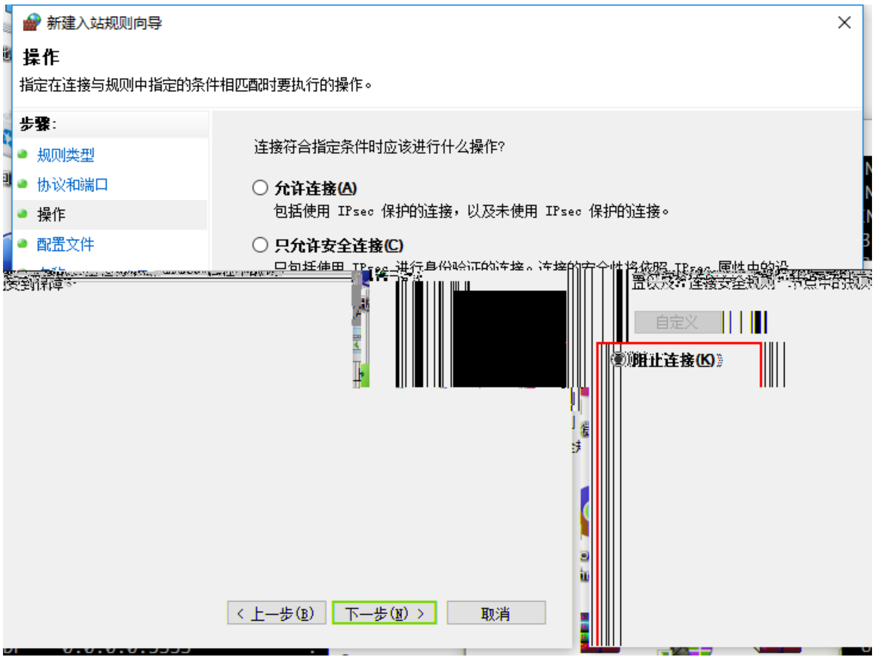
● TCP
○ UDP

此规则应用于所有本地端口还是特定的本地端口?

○ 所有本地端口(A)
● 特定本地端口(S): 445

示例: 80, 443, 5000-5010

8)



新建入站规则向导

操作

指定在连接与规则中指定的条件相匹配时要执行的操作。

步骤:
- 规则类型
- 协议和端口
- 操作
- 配置文件

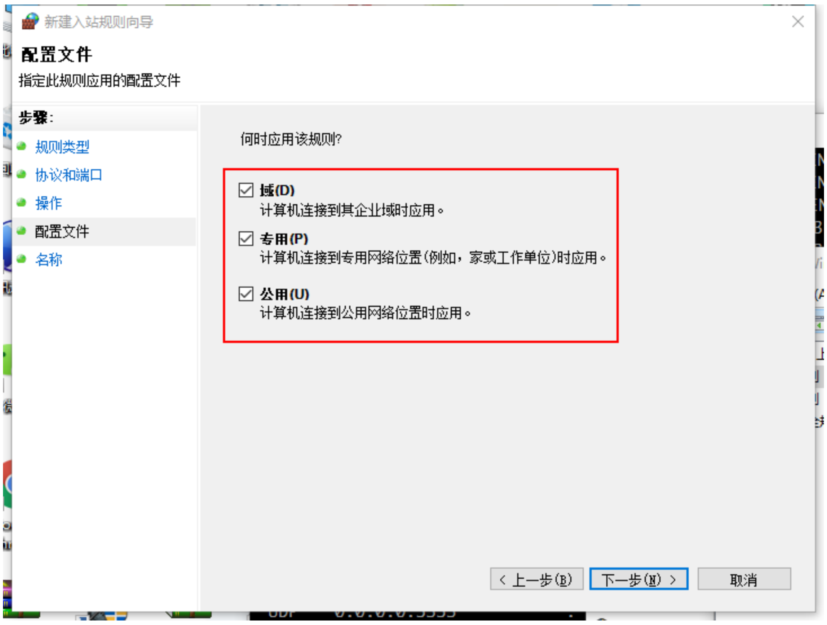
连接符合指定条件时应该进行什么操作?

○ 允许连接(A)
包括使用 IPsec 保护的连接，以及未使用 IPsec 保护的连接。

○ 只允许安全连接(C)
只包括使用 IPsec 进行身份验证的连接。连接的安全性将依照 IPsec 属性中的设置以及“连接安全规则”节点中的规则

● 阻止连接(K)

9)



配置文件

指定此规则应用的配置文件

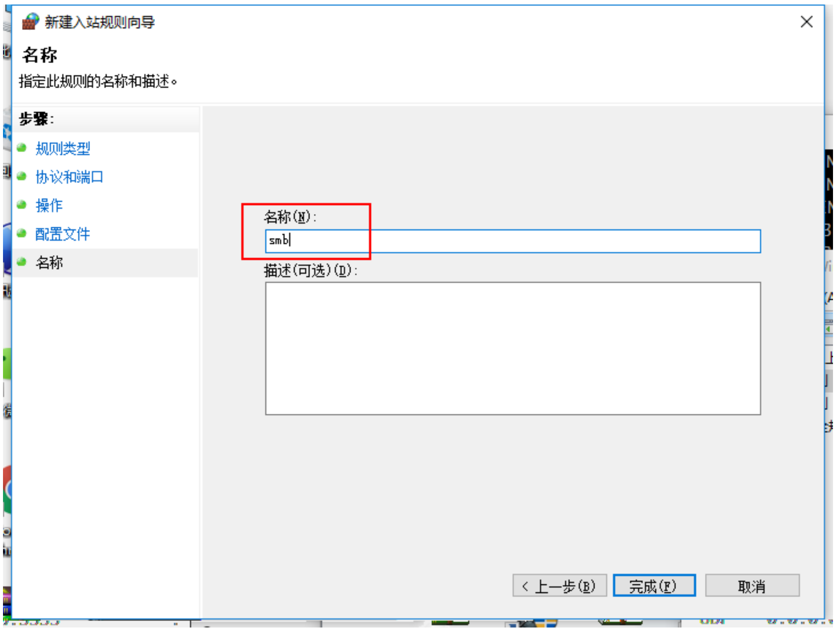
何时应用该规则?

☑ **域(D)**
计算机连接到其企业域时应用。

☑ **专用(P)**
计算机连接到专用网络位置(例如，家或工作单位)时应用。

☑ **公用(U)**
计算机连接到公用网络位置时应用。

10)



名称

指定此规则的名称和描述。

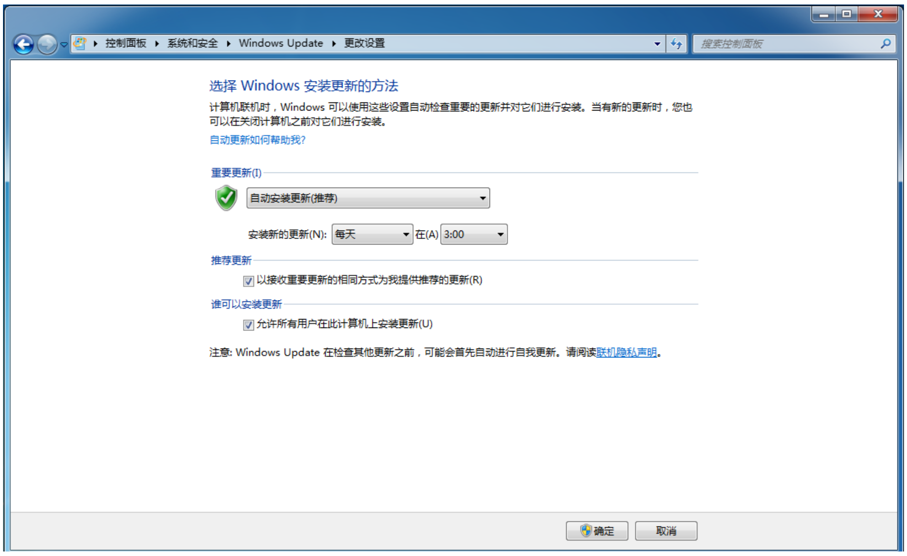
名称(N): smb

描述(可选)(D):

11) MS17-010 winxp_sp3 win10 win2003 win2016 https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/?from=timeline&isappinstalled=0

本地连接
已禁用
Intel(R) PRO/1000 MT Ne

12)



选择 Windows 安装更新的方法

计算机联机时，Windows 可以使用这些设置自动检查重要的更新并对它们进行安装。当有新的更新时，您也可以在关闭计算机之前对它们进行安装。

自动更新如何帮助我?

重要更新(I)

自动安装更新(推荐)

安装新的更新(N): 每天 在(A) 3:00

推荐更新

☑ 以接收重要更新的相同方式为我提供推荐的更新(R)

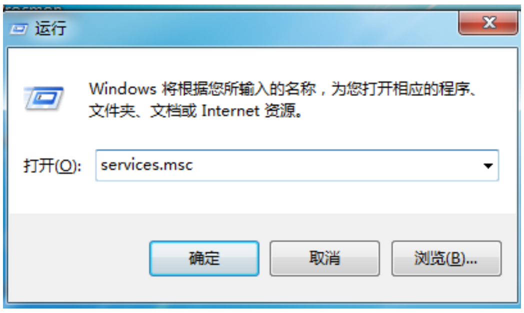
谁可以安装更新

☑ 允许所有用户在此计算机上安装更新(U)

注意: Windows Update 在检查其他更新之前，可能会首先自动进行自我更新。请阅读联机隐私声明。

13) Win7 Server 445

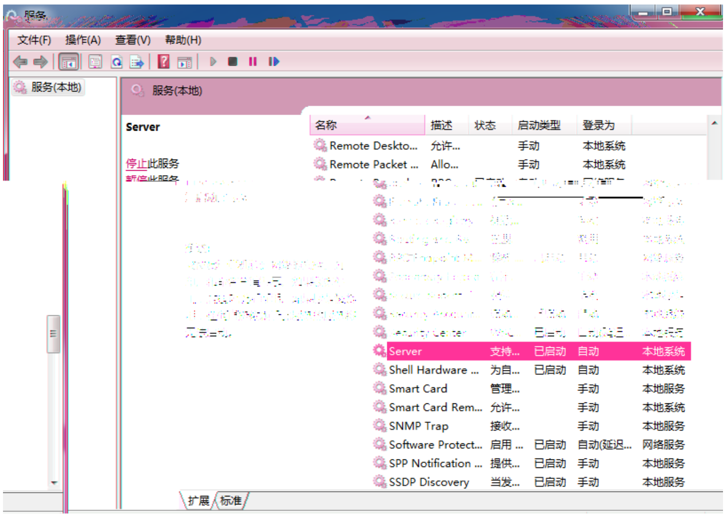
server services.msc



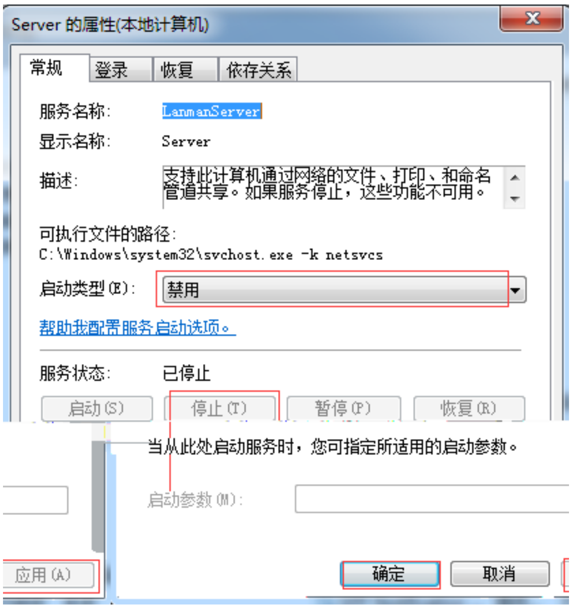
Windows 将根据您所输入的名称，为您打开相应的程序、文件夹、文档或 Internet 资源。

打开(O): services.msc

Server



名称	描述	状态	启动类型	登录为
Remote Deskto...	允许...		手动	本地系统
Remote Packet ...	Allo...		手动	本地系统
Server	支持...	已启动	自动	本地系统
Shell Hardware ...	为自...	已启动	自动	本地系统
Smart Card	管理...		手动	本地服务
Smart Card Rem...	允许...		手动	本地系统
SNMP Trap	接收...		手动	本地服务
Software Protect...	启用 ...	已启动	自动(延迟...	网络服务
SPP Notification ...	提供...	已启动	手动	本地服务
SSDP Discovery	当发...	已启动	手动	本地服务



服务名称: LanmanServer

显示名称: Server

描述: 支持此计算机通过网络的文件、打印、和命名管道共享。如果服务停止，这些功能不可用。

可执行文件的路径:
C:\Windows\system32\svchost.exe -k netsvcs

启动类型 (E): 禁用

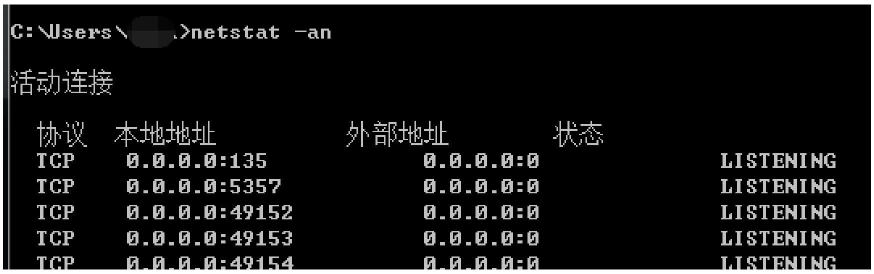
帮助我配置服务启动选项。

服务状态: 已停止

当从此处启动服务时，您可指定所适用的启动参数。

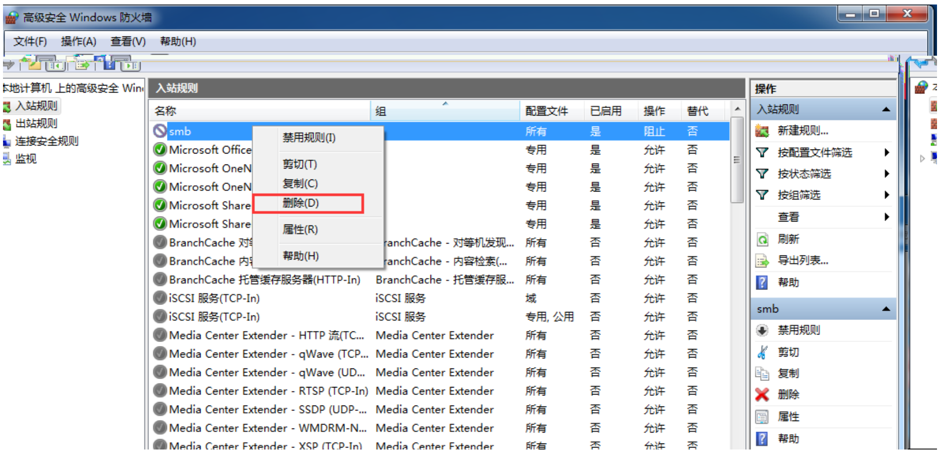
启动参数 (M):

win7 netstat an 445



```
C:\Users\[redacted]>netstat -an

活动连接

  协议  本地地址          外部地址        状态
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
```

SMB



名称	组	配置文件	已启用	操作	替代
smb		所有	是	阻止	否
Microsoft Office		专用	是	允许	否
Microsoft OneN		专用	是	允许	否
Microsoft OneN		专用	是	允许	否
Microsoft Share		专用	是	允许	否
Microsoft Share		专用	是	允许	否
BranchCache 对	anchCache - 对等机发现...	所有	否	允许	否
BranchCache 内	anchCache - 内容检索(...	所有	否	允许	否
BranchCache 托管缓存服务器(HTTP-In)	BranchCache - 托管缓存服...	所有	否	允许	否
iSCSI 服务(TCP-In)	iSCSI 服务	域	否	允许	否
iSCSI 服务(TCP-In)	iSCSI 服务	专用, 公用	否	允许	否
Media Center Extender - HTTP 流(TC...	Media Center Extender	所有	否	允许	否
Media Center Extender - qWave (TCP...	Media Center Extender	所有	否	允许	否
Media Center Extender - qWave (UD...	Media Center Extender	所有	否	允许	否
Media Center Extender - RTSP (TCP-In)	Media Center Extender	所有	否	允许	否
Media Center Extender - SSDP (UDP-...	Media Center Extender	所有	否	允许	否
Media Center Extender - WMDRM-N...	Media Center Extender	所有	否	允许	否
Media Center Extender - XSP (TCP-In)	Media Center Extender	所有	否	允许	否

Win

1) Windows

您的电脑未受保护：启用 Windows 防火墙

Windows 防火墙通过阻止未授权用户通过 Internet 或网络
机来帮助保护计算机。

○ 启用(推荐)(O)

访问您的计算

场)连接到公共网络时请选择此项。
序时不会通知您。在"例外"选项卡

在不太安全的地方 (如
Windows 防火墙阻止程
上的选择将被忽略。

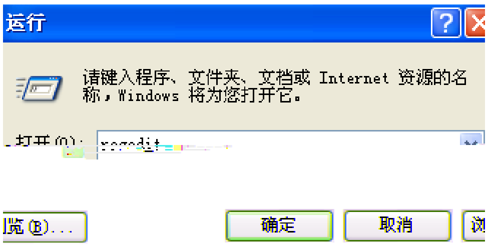
ndows 防火墙可能使计算机更容易受

○ 关闭(不推荐)(F)

避免使用此设置。关闭 Wi
病毒和入侵者的攻击。

了解 Windows 防火墙的其他信息

2) 445 regedit

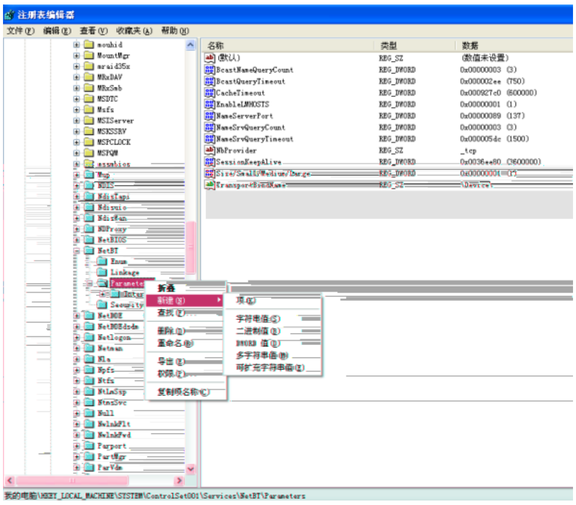


请键入程序、文件夹、文档或 Internet 资源的名
称，Windows 将为您打开它。

打开(O): regedit

3) HKEY_LOCAL_MACHINE\System\Controlset\Services\NetBT\Parameters

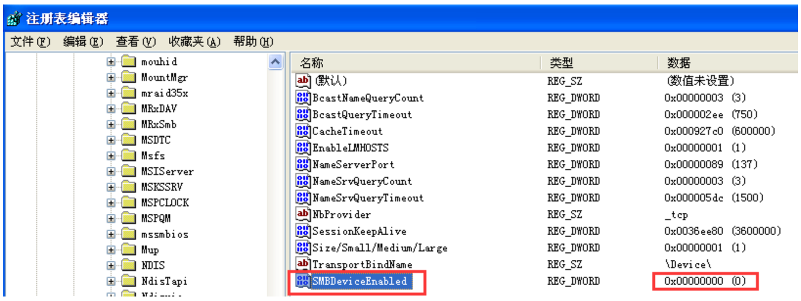
Parameters DWORD



名称	类型	数据
(默认)	REG_SZ	(数值未设置)
BcastNameQueryCount	REG_DWORD	0x00000003 (3)
BcastQueryTimeout	REG_DWORD	0x000002ee (750)
CacheTimeout	REG_DWORD	0x000927c0 (600000)
EnableLMHOSTS	REG_DWORD	0x00000001 (1)
NameServerPort	REG_DWORD	0x00000089 (137)
NameSrvQueryCount	REG_DWORD	0x00000003 (3)
NameSrvQueryTimeout	REG_DWORD	0x000005dc (1500)
NbProvider	REG_SZ	_tcp
SessionKeepAlive	REG_DWORD	0x0036ee80 (3600000)
Size/Small/Medium/Large	REG_DWORD	0x00000001 (1)
TransportBindName	REG_SZ	\Device\

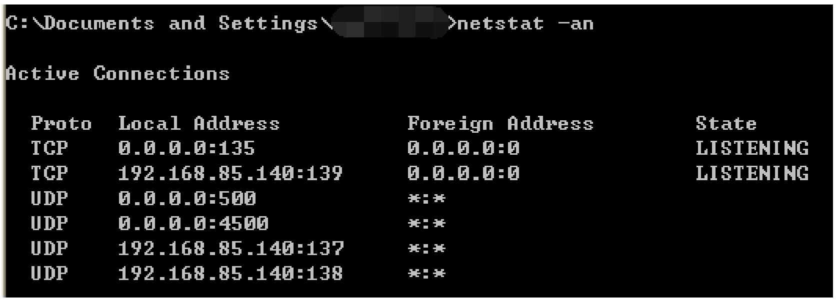
我的电脑\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\NetBT\Parameters

4) DWORD SMBDeviceEnabled 0



名称	类型	数据
(默认)	REG_SZ	(数值未设置)
BcastNameQueryCount	REG_DWORD	0x00000003 (3)
BcastQueryTimeout	REG_DWORD	0x000002ee (750)
CacheTimeout	REG_DWORD	0x000927c0 (600000)
EnableLMHOSTS	REG_DWORD	0x00000001 (1)
NameServerPort	REG_DWORD	0x00000089 (137)
NameSrvQueryCount	REG_DWORD	0x00000003 (3)
NameSrvQueryTimeout	REG_DWORD	0x000005dc (1500)
NbProvider	REG_SZ	_tcp
SessionKeepAlive	REG_DWORD	0x0036ee80 (3600000)
Size/Small/Medium/Large	REG_DWORD	0x00000001 (1)
TransportBindName	REG_SZ	\Device\
SMBDeviceEnabled	REG_DWORD	0x00000000 (0)

5) 445

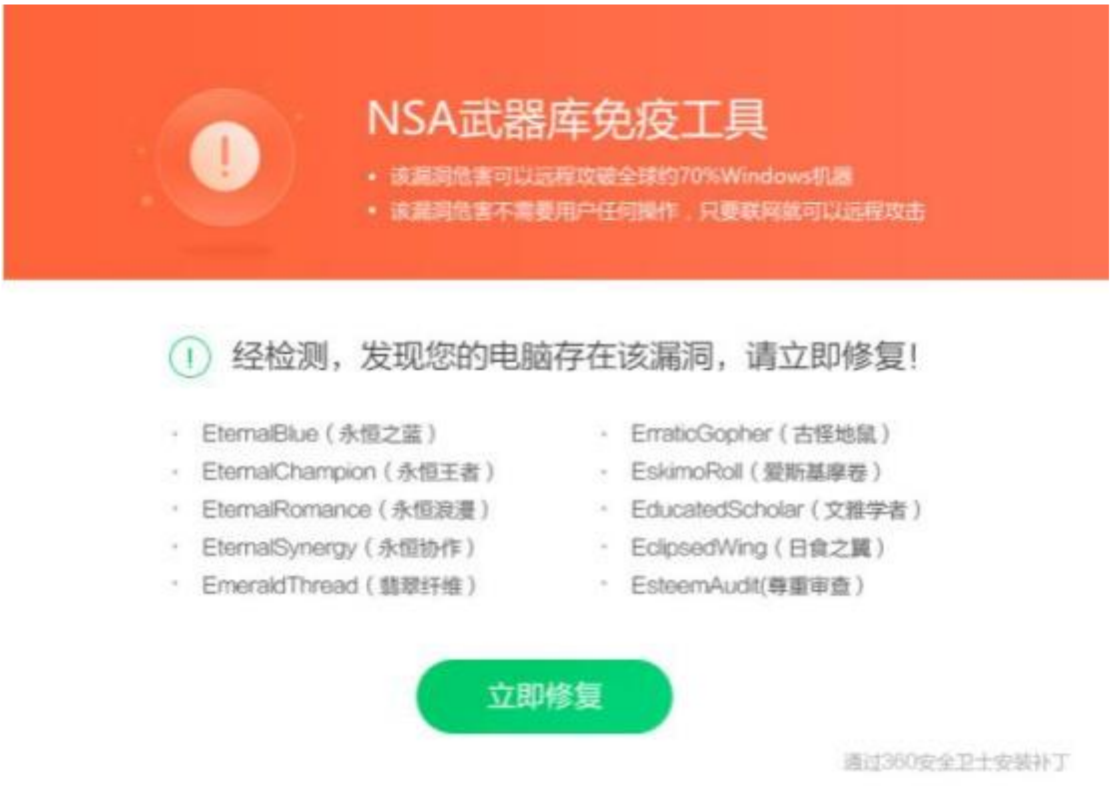


```
C:\Documents and Settings\[redacted]>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    192.168.85.140:139     0.0.0.0:0              LISTENING
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    192.168.85.140:137     *:*
  UDP    192.168.85.140:138     *:*
```

6) Wannacry XP

/

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



NSA武器库免疫工具

- 该漏洞危害可以远程攻破全球约70%Windows机器
- 该漏洞危害不需要用户任何操作，只要联网就可以远程攻击

经检测，发现您的电脑存在该漏洞，请立即修复！

- EternalBlue（永恒之蓝）
- EternalChampion（永恒王者）
- EternalRomance（永恒浪漫）
- EternalSynergy（永恒协作）
- EmeraldThread（翡翠纤维）
- ErraticGopher（古怪地鼠）
- EskimoRoll（爱斯基摩卷）
- EducatedScholar（文雅学者）
- EclipsedWing（日食之翼）
- EsteemAudit(尊重审查）