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

针对勒索软件“wannacry”紧急防范处置手册

1.概述

北京时间 5 月 13 日，互联网上出现针对 Windows 操作系统的勒索软件的攻击案例，此次攻击事件的主角即名为“WannaCry”的勒索软件。该勒索软件同时具备加密勒索功能和内网蠕虫传播能力，属于新型的勒索软件家族，危害极大。勒索软件利用此前披露的 Windows SMB 服务漏洞（对应微软漏洞公告：MS17-010）攻击手段，向终端用户进行渗透传播，并向用户勒索比特币或其他价值物，涉及到国内用户（已收到多起高校案例报告），已经构成较为严重的攻击威胁，广东互联网应急中心综合相关材料[1]形成针对勒索软件“wannacry”紧急防范处置手册。

2. 应急处置方案

2.1 主机应急处置操作指南

2.1.1 确认主机是否被感染

被感染的机器屏幕会显示如下的告知付赎金的界面：

[1] 来源国家互联网应急中心、360 公司、安天公司、数字观星等单位

2.1.2 已感染的用户的补救措施

据目前了解情况，无法解密该勒索软件加密的文件，不建议用户向勒索者支付赎金。如果发现网内有感染的机器，应将其及时断网关机隔离处理，同时通告运维人员切断网络连接（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待处理。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，同样等候使用离线工具处理。若用户存在主机备份，则启动备份恢复程序。

2.1.3 尚未感染主机防护步骤

- 关闭网络，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）及网络共享；
- 针对主机进行漏洞补丁升级安装。

2.1.3.1 Win7、Win8、Win10 系统的处理流程

1) 关闭网络

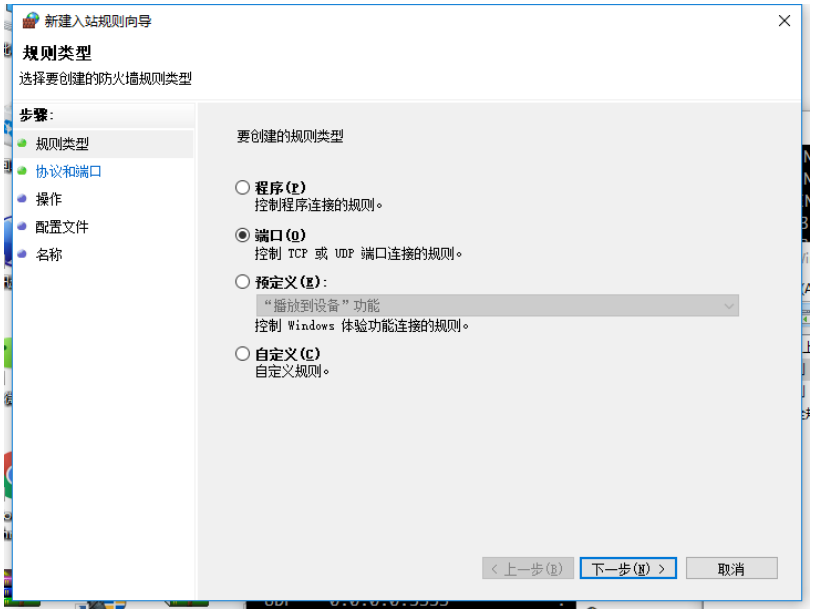
2) 打开控制面板-系统与安全-Windows 防火墙，点击左侧启动或关闭 Windows 防火墙

3) 选择启动防火墙，并点击确定

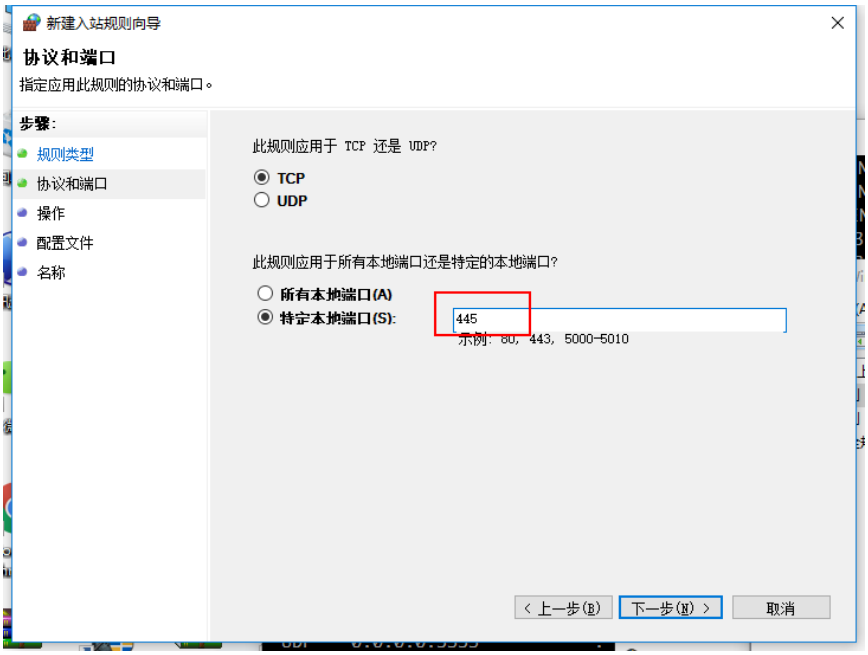
4) 点击高级设置

5) 点击入站规则，新建规则，以 445 端口为例

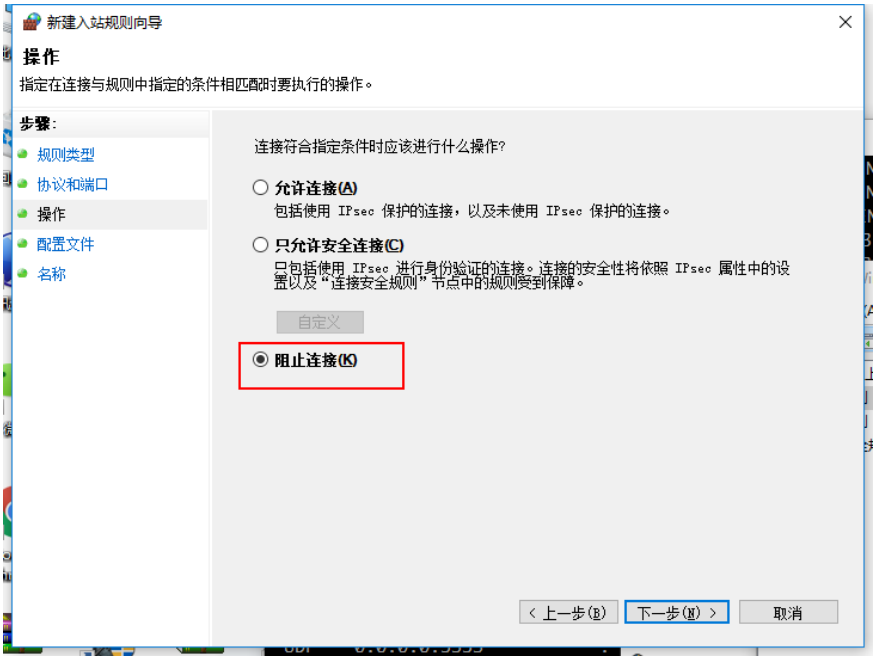
6) 选择端口、下一步



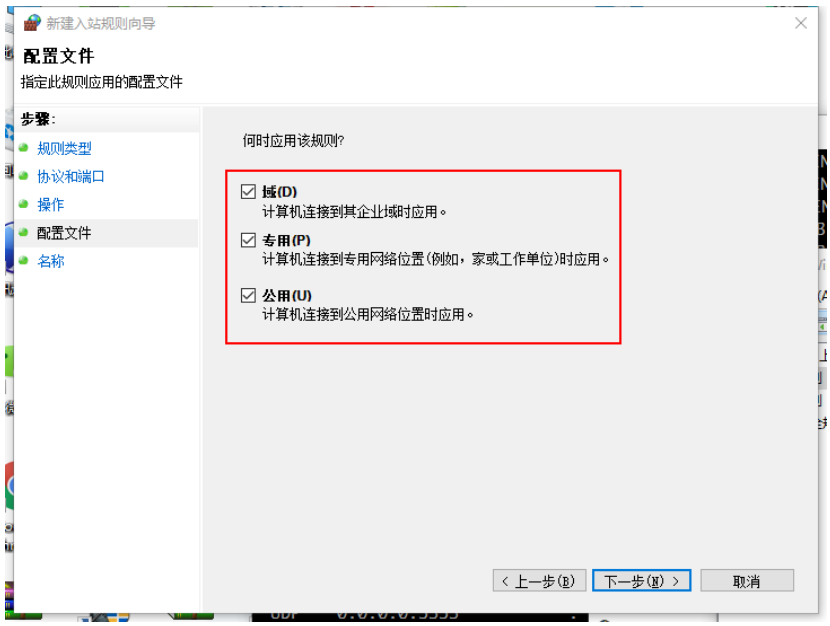
7) 选择特定本地端口，输入 445，下一步



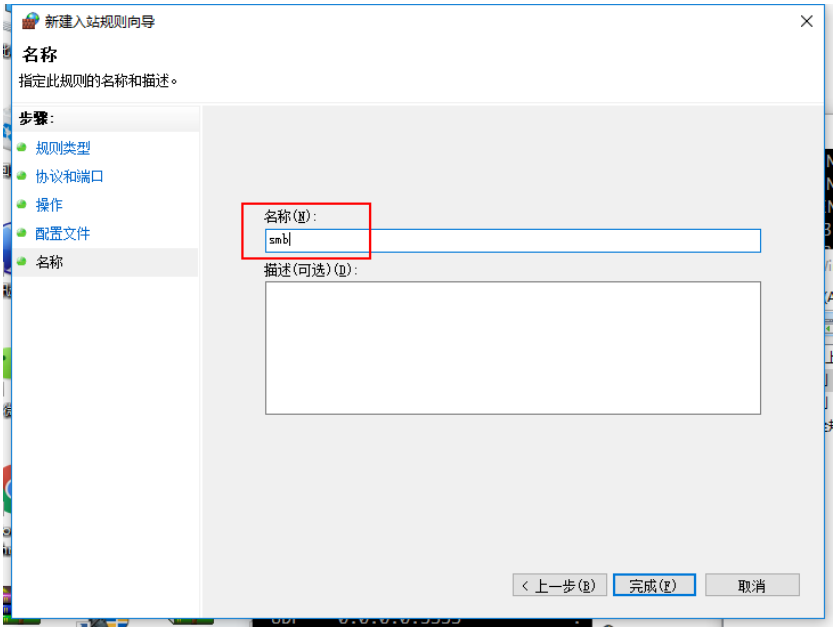
8) 选择阻止连接，下一步



9) 配置文件，全选，下一步

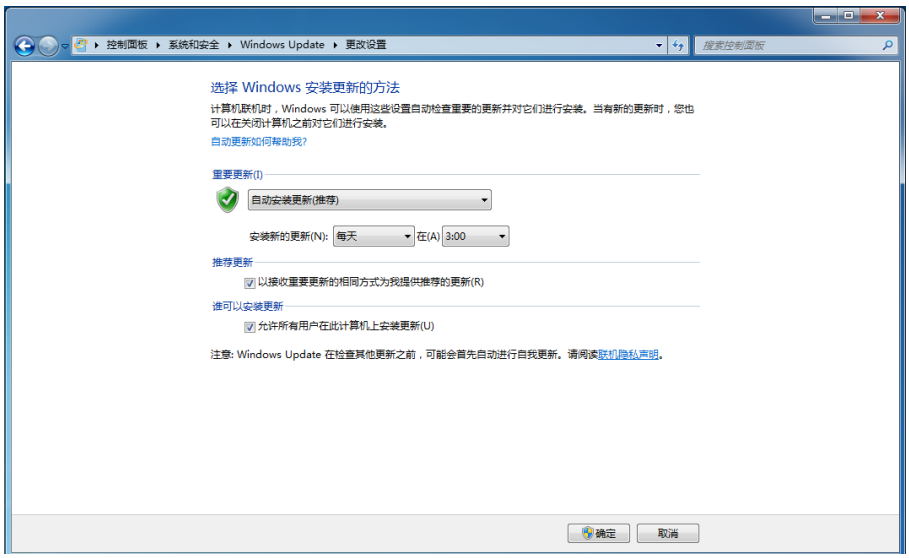


10) 名称，可以任意输入，完成即可。



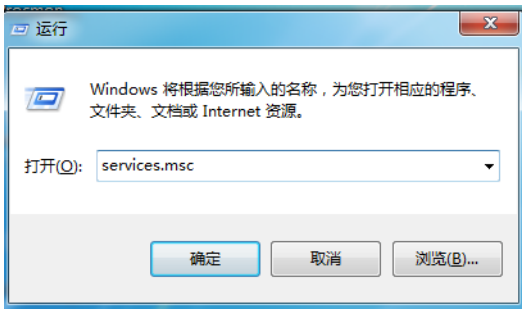
11) 请安装 MS17-010 补丁，微软已经发布 winxp_sp3 至 win10、win2003 至 win2016 的全系列补丁。微软官方下载地址：https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/?from=timeline&isappinstalled=0，或者恢复网络升级。

12) 开启系统自动更新，并检测更新进行安装

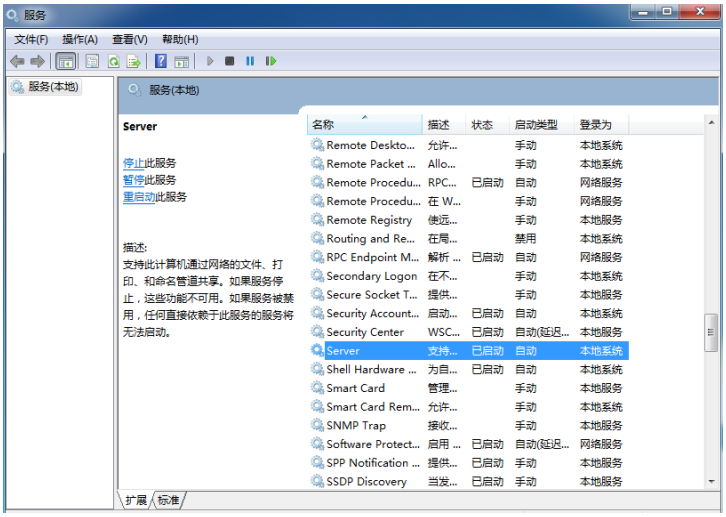


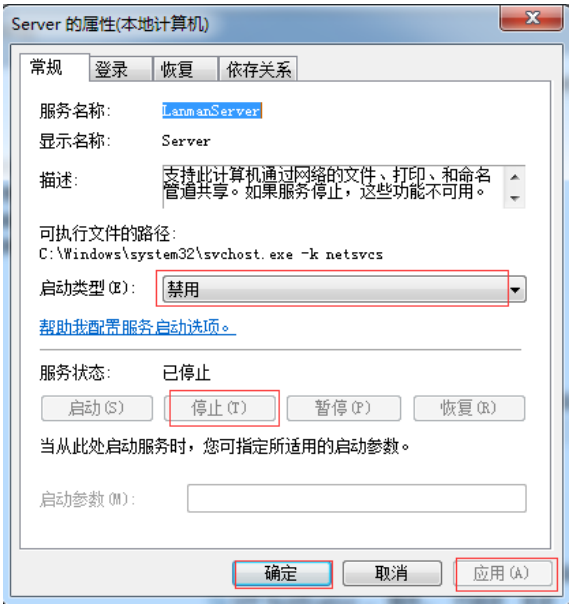
13) Win7 系统需要关闭 Server 服务才能够禁用 445 端口的连接

需要操作系统的 server 服务关闭，依次点击“开始”，“运行”，输入 services.msc，进入服务管理控制台。

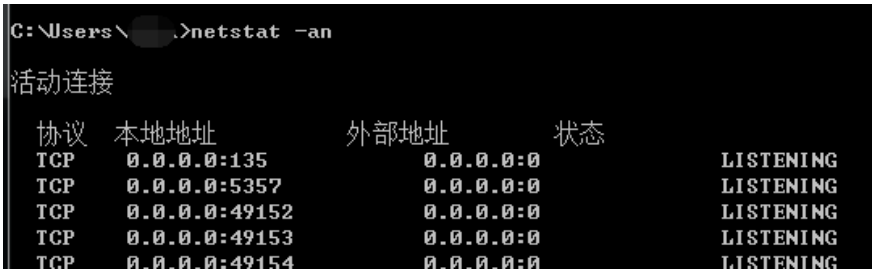


双击 Server，先停用，再选择禁用。

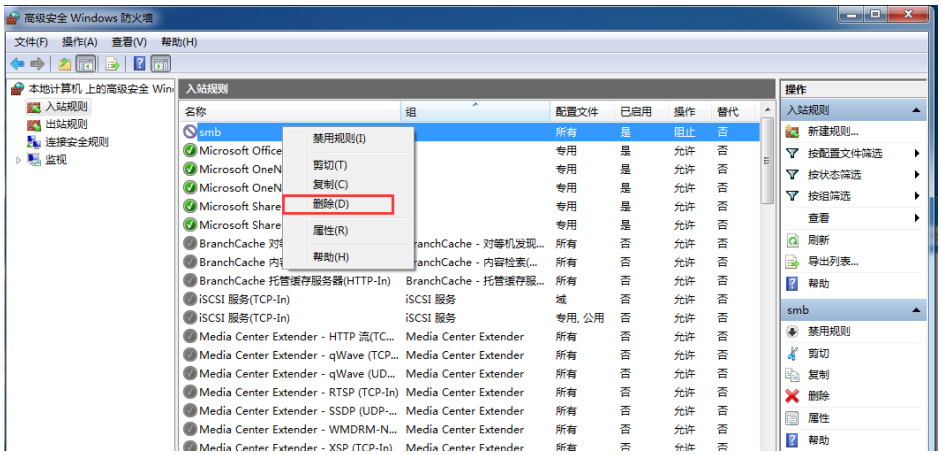




最后重启 win7。使用 netstat –an 查看 445 端口不存在了。

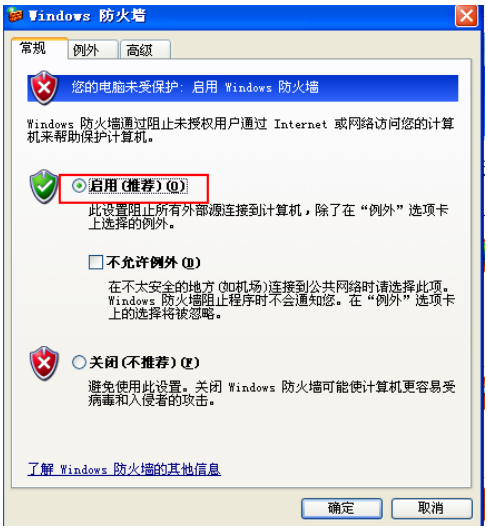


注：在系统更新完成后，如果业务需要使用 SMB 服务，将上面设置的防火墙入站规则删除即可。

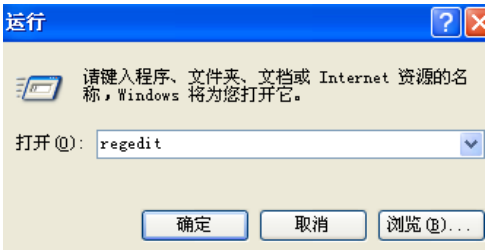


2.1.3.2 Win XP 系统的处理流程

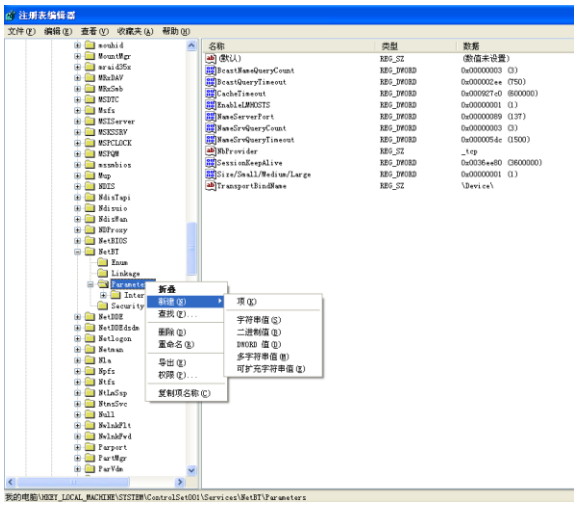
1) 依次打开控制面板，安全中心，Windows 防火墙，选择启用



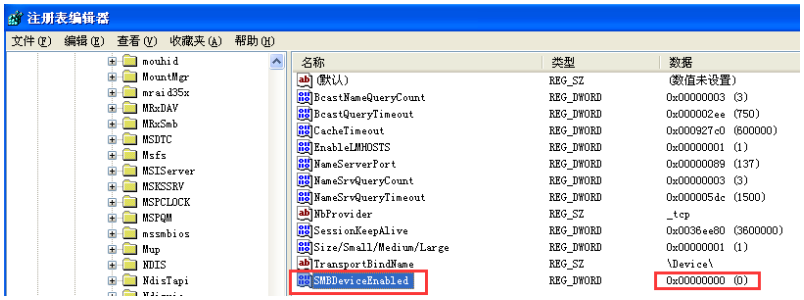
2) 通过注册表关闭 445 端口，单击“开始”——“运行”，输入“regedit”，单击“确定”按钮，打开注册表。



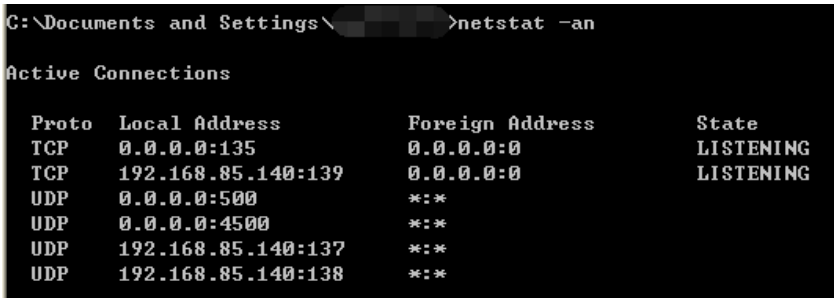
3) 找到 HKEY_LOCAL_MACHINE\System\Controlset\Services\NetBT\Parameters，选择“Parameters”项，右键单击，选择“新建”——“DWORD 值”。



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) 鉴于本次 Wannacry 蠕虫事件的影响恶劣，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，微软公告详情/。https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

2.2 网络设备应急处置操作指南

部分机构由于设备众多，为了避免感染设备之后的广泛传播，建议利用各网络设备的进行 ACL 访问控制策略配置，以实现临时应急方案。由于该蠕虫病毒主要利用 TCP 的 445 端口进行传播，为了阻断病毒快速传播，建议在核心网络设备的三层接口位置，配置 ACL 规则从网络层面阻断 TCP 445 端口的通讯。以下内容

是基于较为流行的网络设备，举例说明配置 ACL 规则，以禁止 TCP 445 网络端口传输，仅供大家参考。在实际操作中，请协调网络管理人员或网络设备厂商服务人员，根据实际网络环境在核心网络设备上进行配置。

2.2.1 Juniper 设备的建议配置（示例）：

```
set firewall family inet filter deny-wannacry term deny445 from protocol tcp
set firewall family inet filter deny-wannacry term deny445 from
destination-port 445
set firewall family inet filter deny-wannacry term deny445 then discard
set firewall family inet filter deny-wannacry term default then accept
#在全局应用规则
set forwarding-options family inet filter output deny-wannacry
set forwarding-options family inet filter input deny-wannacry
#在三层接口应用规则
set interfaces [需要挂载的三层端口名称] unit 0 family inet filter
output deny-wannacry
set interfaces [需要挂载的三层端口名称] unit 0 family inet filter input
deny-wannacry
```

2.2.2 华三(H3C)设备的建议配置（示例）：

新版本:

```
acl number 3050
rule deny tcp destination-port 445
rule permit ip
interface [需要挂载的三层端口名称]
packet-filter 3050 inbound
packet-filter 3050 outbound
```

旧版本:

```
acl number 3050
rule permit tcp destination-port 445
```

```
traffic classifier deny-wannacry
if-match acl  3050

traffic behavior deny-wannacry
filter deny

qos policy deny-wannacry
classifier deny-wannacry behavior deny-wannacry
#在全局应用
qos apply policy deny-wannacry global inbound
qos apply policy deny-wannacry global outbound
#在三层接口应用规则
Interface [需要挂载的三层端口名称]
qos apply policy deny-wannacry inbound
qos apply policy deny-wannacry outbound
```

2.2.3 华为设备的建议配置（示例）：

```
acl number 3050
rule deny tcp destination-port  eq  445
rule permit ip

traffic classifier deny-wannacry type  and
if-match acl  3050

traffic behavior deny-wannacry

traffic policy deny-wannacry
classifier deny-wannacry behavior deny-wannacry   precedence 5
```

```
interface [需要挂载的三层端口名称]
traffic-policy deny-wannacry    inbound
traffic-policy deny-wannacry    outbound
```

2.2.4 Cisco 设备的建议配置（示例）：

```
旧版本:
ip  access-list extended deny-wannacry
deny tcp any any  eq 445
permit ip any any

interface [需要挂载的三层端口名称]
ip  access-group deny-wannacry  in
ip  access-group deny-wannacry  out

新版本:
ip  access-list deny-wannacry
deny tcp any any  eq 445
permit ip any any

interface [需要挂载的三层端口名称]
ip  access-group deny-wannacry  in
ip  access-group deny-wannacry  out
```

2.2.5 锐捷设备的建议配置（示例）：

```
ip  access-list extended deny-wannacry
deny tcp any any  eq  445
permit ip any any
interface  [需要挂载的三层端口名称]
```

```
ip  access-group deny-wannacry in
ip access-group deny-wannacry out
```

2.3 其他应急处置操作指南

其他快速处置方式可使用“NSA 武器库免疫工具”，一键检测修复漏洞、关闭高风险服务，可精准检测出 NSA 武器库使用的漏洞是否已经修复，提示用户安装相应的补丁。

针对 XP、2003 等无补丁的系统版本用户，防御工具能够帮助用户关闭存在高危风险的服务，从而对 NSA 黑客武器攻击的系统漏洞防护。

NSA 武器库免疫工具下载地址：http://dl.360safe.com/nsa/nsatool.exe

关于国家计算机网络应急技术处理协调中心广东分中心

国家计算机网络应急技术处理协调中心广东分中心（中文简称“广东互联网应急中心”，英文简称 GDCERT/CC 或 GDCERT）是国家计算机网络应急技术处理协调中心（中文简称“国家互联网应急中心”，英文简称 CNCERT/CC 或 CNCERT）在广东的省级分中心，受国家互联网应急中心与广东省通信管理局的双重领导。目

前，广东互联网应急中心依托国家级全程全网的应急体系和技术平台，为我省公共互联网、重要政府部门、骨干运营企业、重要行业提供互联网安全的事件发现、预警通报、应急处置和测试评估等技术支撑。

联系我们

网址：www.cert.org.cn

email：gd@cert.org.cn

电话：020-85613834