NSFOCUS

“WannaCry”勒索事件处置手册

■ **文档编号**	请输入文档编号	■ **密级**	请输入文档密级
■ **版本编号**	1.0	■ **日期**	

■ **版权声明**

■ **版本变更记录**

时间	版本	说明	修改人
2017/5/13	1.0	创建	曹嘉

■ **适用性声明**

本文档用于引导企业通过正确的流程和手段进行危害抑制和损失控制，供企业安全管理人员、运维人员以及绿盟科技安全服务人员使用。

目录

一. 文档用途

“WannaCry”勒索事件自爆发以来，造成了大量 Windows 主机感染，本文档用于指导企业安全管理人员可以在第一时间对可能发生的病毒爆发进行充分准备，引导企业通过正确的流程和手段进行危害抑制和损失控制。

二. 准备工作

2.1 内部通告

企业应首先建立组织内部的通告机制，确保全员了解并遵从相关指导，避免错误操作所造成的不必要的损失，内部通告包括但不限于：

- 微信客户端 / 短信通告
- 办公环境人工通告

通告内容可参考下文：

由于近日爆发 WannaCry 勒索病毒，此病毒可在局域网内通过 445 端口自行传播，为了避免周一上班后刚开机就被感染，且把硬盘所有文件都加密，请开机前先断网，按顺序执行如下 4 条防护操作，windows 服务器运维人员请尽早执行。

已经发现自己中病毒，文件被加密的电脑、服务器，禁止接入网络！

防护操作：

1. 断网（拔网线）
2. 开机（若关机状态）
3. 关闭 445 端口并确认（如自行可处理）：本机 cmd 窗口执行命令"netstat -ano | findstr ":445""，回车后无任何返回。
4. 联系企业 IT 运维或安全人员协助离线打补丁

2.2 相关工具

企业应自行或联系安全服务供应商提供相关工具，建议工具如下：

工具类型	工具名称	相关规则/版本
检测类	绿盟远程安全评估系统（RSAS）	V5 系统插件版本在 5.0.16.48 以上 V6 系统插件版本在 V6.0R02F01.0604 以上
修复类	WannaCry 勒索病毒一键加固脚本	V1.4 版本及后续更新版本
	Wireshark	测试使用 V2.2.2 版
	绿盟科技离线升级工具	V1.1
边界防护类	绿盟网络入侵防护/检测系统（IPS/IDS）	5.6.10 规则版本 5.6.10.15956 以上 5.6.9 规则版本 5.6.9.15956 以上 5.6.8 规则版本 5.6.8.643 以上 5.6.7 规则版本 5.6.7.643 以上

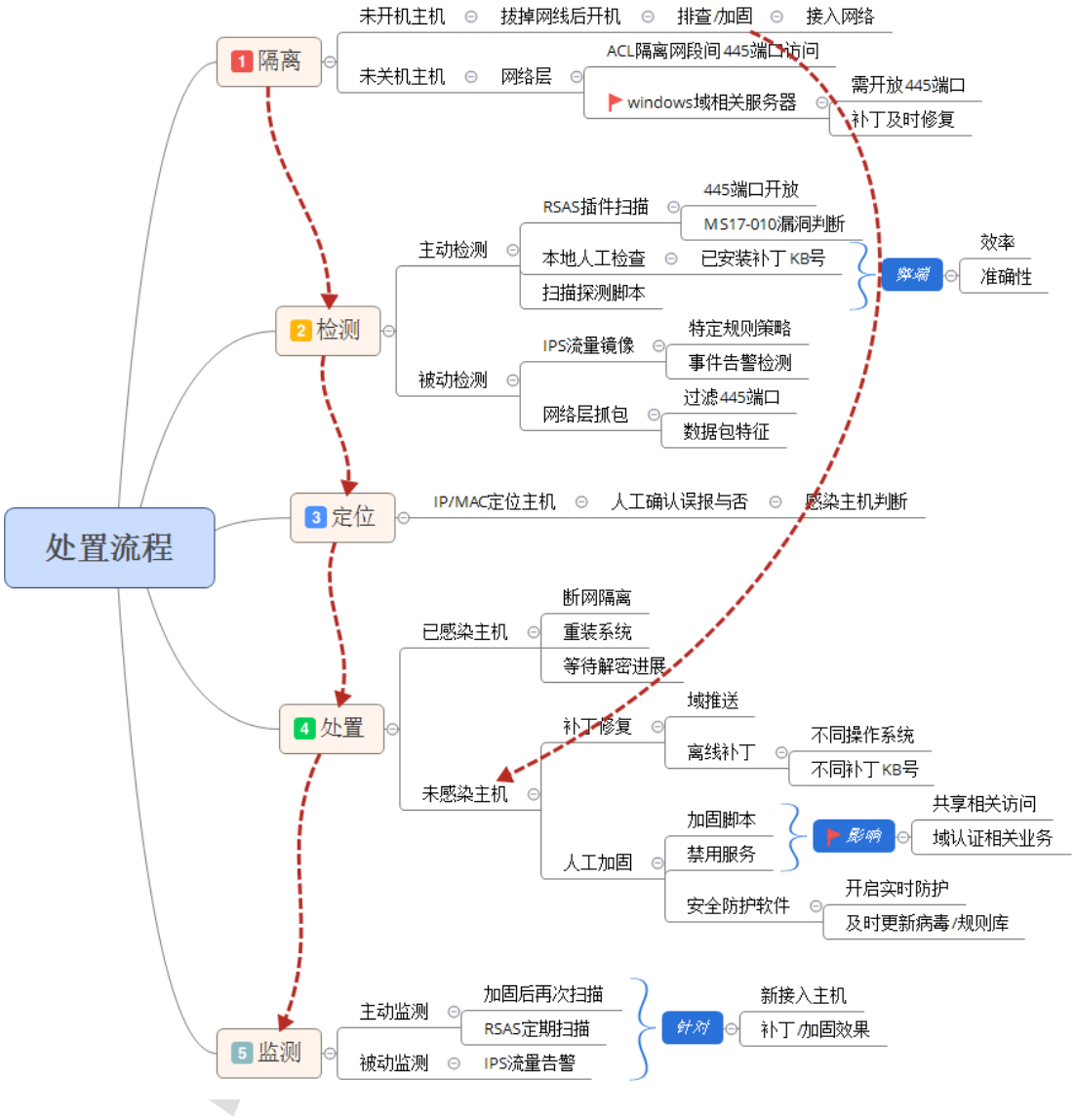
三. 启动必读

1、尽可能保持主机关闭以及断网状态：部分解决方案建议通过联网下载修复工具的方式对漏洞进行修补，这种行为在当前的互联网环境下是非常危险的，已经发现有部分处于专网内的用户在打开电脑联网下载修复工具时被蠕虫感染。这是由于存在漏洞的主机在联网的同时，会迅速的被蠕虫扫描到，相当于给了蠕虫可乘之机。建议如主机未开机，继续保持主机关闭，并拔掉网线，关闭 Wifi 等可能的网络接入。

2、付费风险：部分中招主机可能包含关键信息，企业处于业务考虑可能会考虑通过比特币付款，目前尚未确认付款可以恢复数据，建议企业慎重考虑。

四. 处置流程

WannaCry 勒索蠕虫病毒处置五步走，如下图。



4.1 网络隔离

网络中可能存在持续运行的主机，这部分主机很可能已经被感染了蠕虫病毒，由于蠕虫病毒可利用 SMB 漏洞在本网段和跨网段传播，因此，为了防止病毒进一步扩散，风险控制

第一步：通过 ACL 网段访问控制做网络层的隔离处理，防止蠕虫病毒通过 445 端口在网段间传播。详细操作参考**附录 B ACL 网络访问控制**。

以 Cisco 设备配置为例，在网络边界（出口网关、路由器或安全设备）、内部网络区域（交换机及无线设备）处部署安全策略，以防范和降低攻击产生的影响。详细配置方案如下：

Cisco 设备旧版本配置：

```
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
```

Cisco 设备新版本配置：

```
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
```

其他设备的配置可参考**附录 B ACL 网络访问控制**，或联系相关设备厂商进行配置。

4.2 风险检测

做好网段间的 445 端口访问控制后，使用主动检测结合被动检测的方式，对网络中存在的被感染主机以及漏洞主机进行风险排查。

4.2.1 主动检测

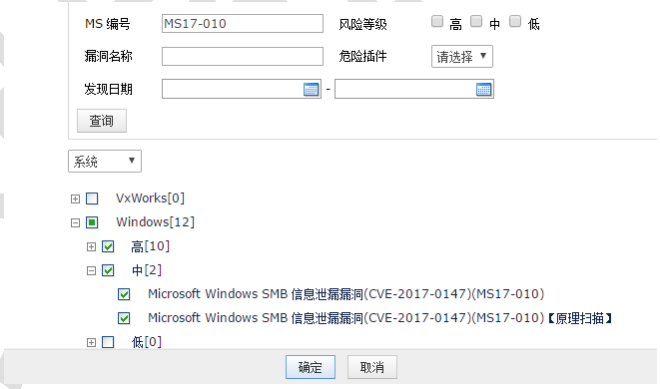
4.2.1.1 MS17-010 漏洞扫描

使用绿盟科技远程安全评估工具，加载 MS17-010 插件扫描分析网段中存在的受漏洞影响的主机。详细操作步骤如下：

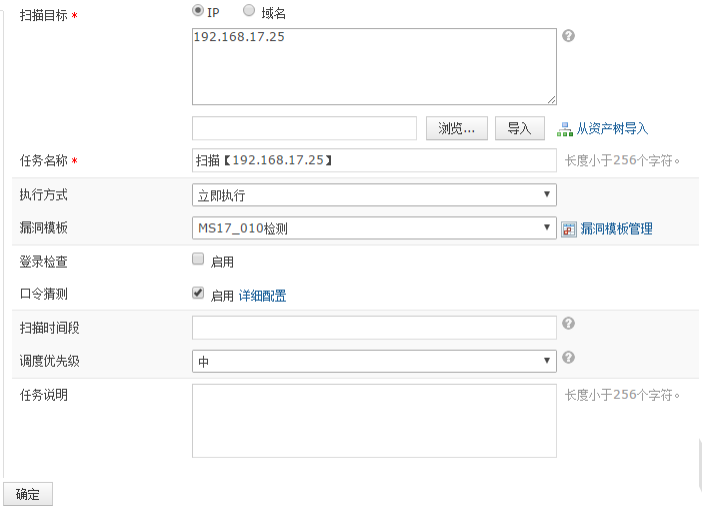
1. 升级 RSAS 检测规则，将规则升级至最新版

2. 在模版管理—漏洞模版中，点击添加，新增 MS17-010 漏洞模版。

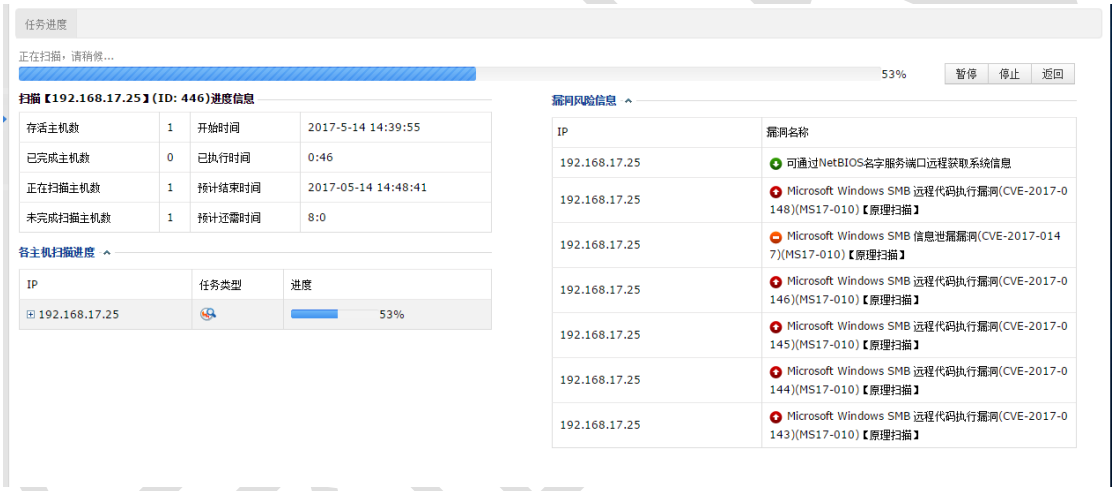
3. 搜索 MS17-010，勾选规则。



4. 新建对网络主机 MS17-010 漏洞的扫描任务，勾选上一步新建的漏洞模板。



5. 如果主机存在漏洞，扫描结果中会出现漏洞风险信息。



4.2.1.2 人工排查

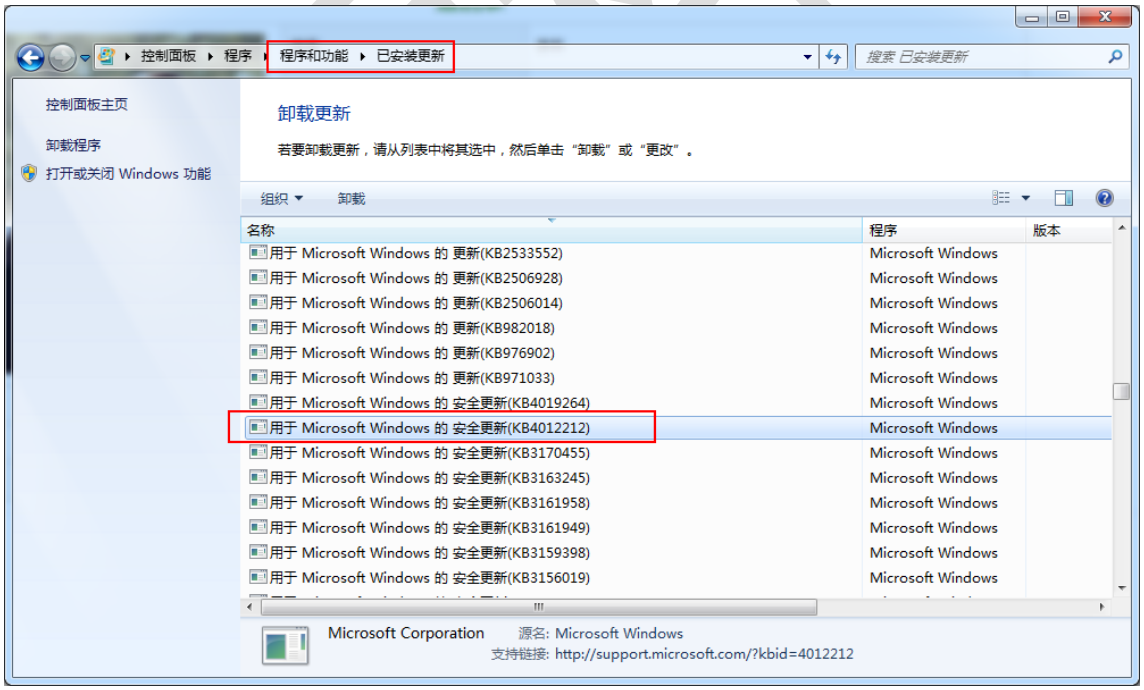
1. 对于未开机的主机，风险排查确认网络中不存在感染主机后，断开网络后再进行开机检查；
2. 对于持续开机运行的主机，人工查看是否感染了勒索蠕虫病毒。
   - 若感染病毒，立即断网隔离，等待下一步处置；
   - 若未感染病毒，断网查看是否安装了相关的安全补丁，排查方法如下：

windows Server 2003 检测方法

在“添加或者删除程序”功能面板中，开启“显示更新”，查找是否存在 KB4012598 补丁。下图为已安装补丁显示。

Windows 7 补丁检测方法：

打开“控制面板”——> “程序和功能”——> “查看已安装的更新”，查找 Windows 7 操作系统的 MS17-010 漏洞对应的更新补丁（KB4012212）。



由于不同系统版本中补丁编号不同，对照如下表所示的相应补丁进行查找：

系统版本	补丁号
Windows XP SP3	KB4012598

Windows XP x64 SP2	KB4012598
Windows 2003 SP2	KB4012598
Windows 2003 x64 SP2	KB4012598
Windows Vista Windows Server 2008	KB4012598
Windows 7/Windows Server 2008 R2	KB4012212
	KB4012215
Windows 8.1	KB4012213
	KB4012216
Windows Server2012	KB4012214
	KB4012217
Windows Server2012 R2	KB4012213
	KB4012216
Windows 10	KB4012606
Windows 10 1511	KB4013198
Windows 10 1607	KB4013429

如果找不到该补丁安装记录，需要及时下载对应版本的升级补丁进行安装，请参考**附录 A MS17-010 补丁对应和下载列表**。

4.2.2 被动检测

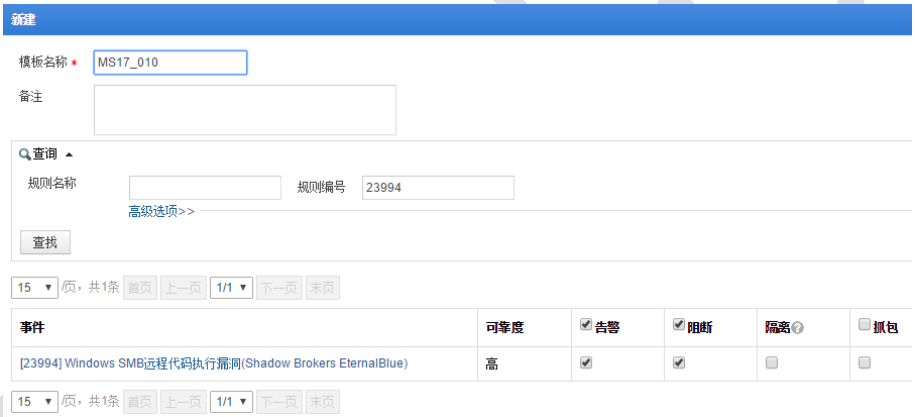
通过 IPS 工具的分析方案和网络层抓包的分析方案，排查网络中是否存在被感染主机。

4.2.2.1 IPS 流量镜像分析

绿盟科技 NIPS 工具提供了针对网络中蠕虫病毒流量特征分析功能，并进行流量告警。详细检测步骤如下：

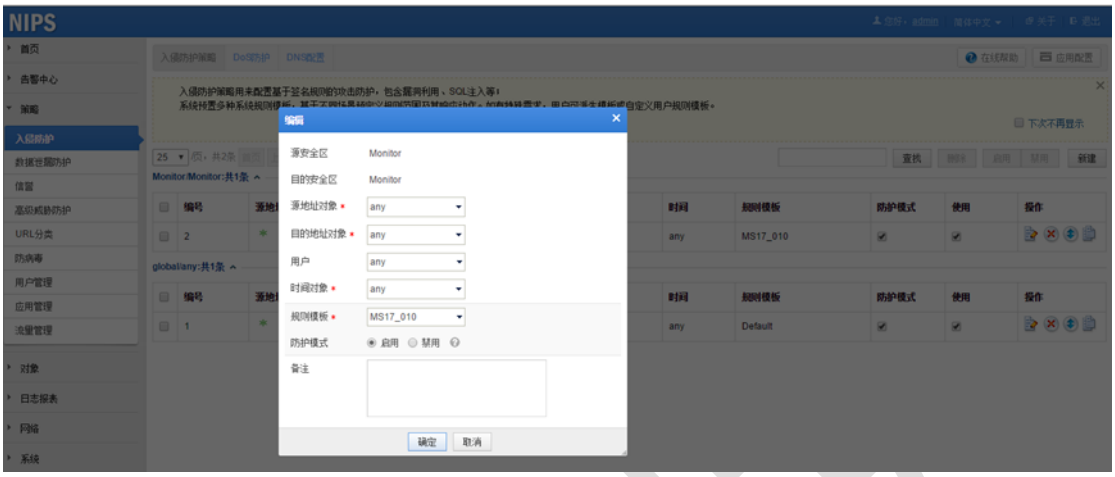
1. 升级 NIPS 规则，将规则升级至最新版。

2. 新建防护规则，编号 23994，检测 MS17-010 漏洞攻击。



3. 新建防护规则，编号 41489，检测 Doublepulsar 后门通信。

4. 新建入侵防护策略，选择刚才创建的规则模版。

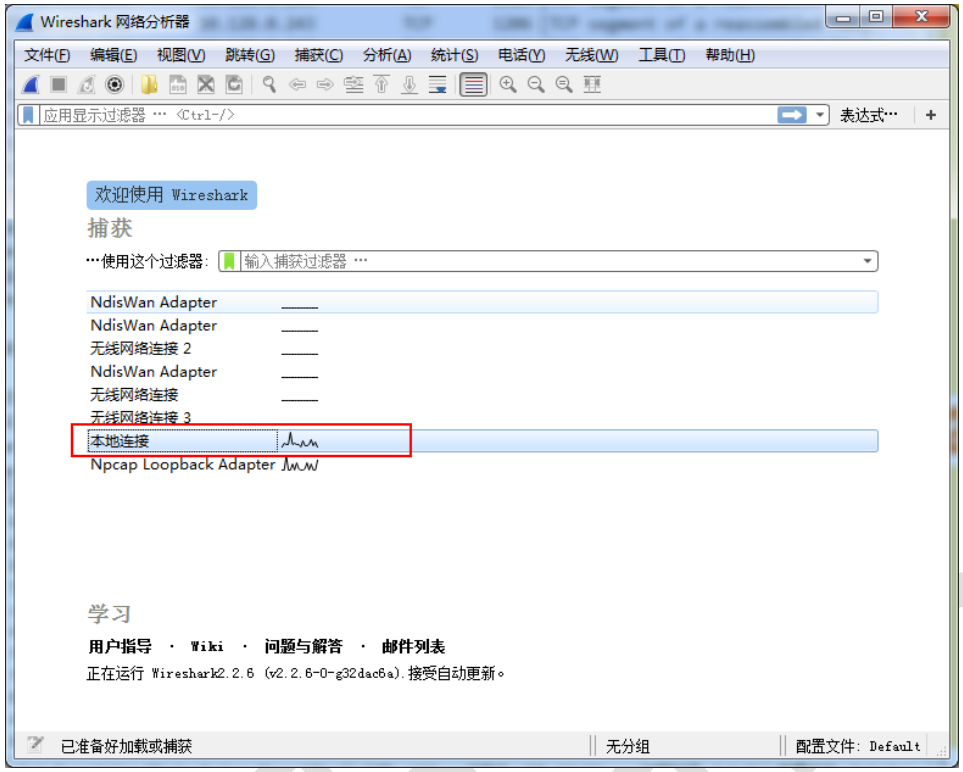


5. 当检测出攻击时，会产生入侵防护事件告警。就可判断出蠕虫病毒利用漏洞在网络中传播。

4.2.2.2 网络层抓包分析

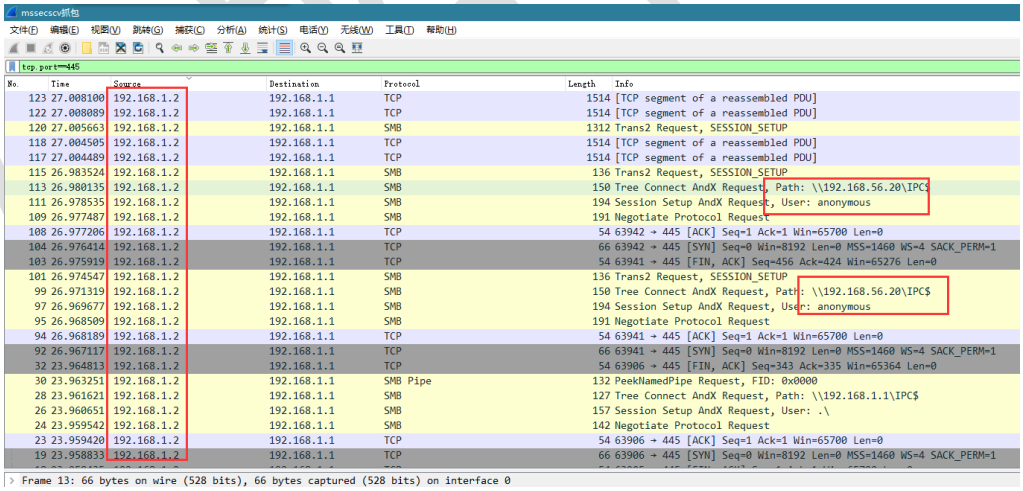
若网络中存在被感染主机，则 WannaCry 病毒会持续不断的发起探测请求，因此，接入主机可通过抓取网络层流量，查看是否存在感染主机。具体操作过程如下：

1. 接入设备（设备系统已升级至最新补丁，确定不会受蠕虫病毒感染），开放 445 端口；
2. 打开抓包工具 wireshark，监听本地网卡，抓取网络层流量。



3. 蠕虫攻击探测

通过规则 tcp.port==445 过滤网络中发起的 445 端口流量，若能看到存在大量的 445 请求，并出现 IPC$共享链接请求，可初步判断网络中存在蠕虫病毒。



4. 通过上图可以看到，192.168.1.2 主机正在向外发起大量 TCP 请求，并且在连接 192.168.56.20 主机的 IPC 共享，可初步判断 192.168.1.2 主机已被感染且正在探测 56.20 主机。

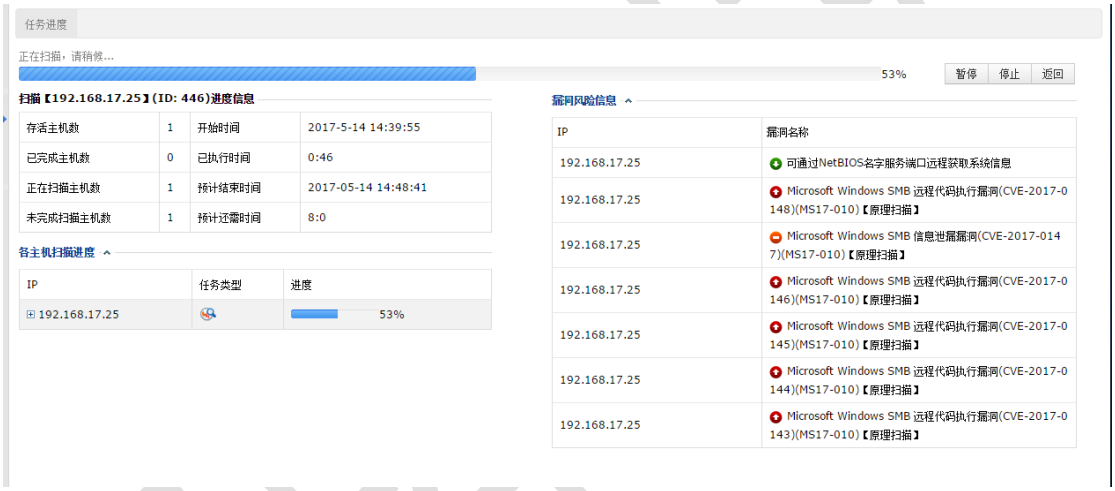
4.3 风险定位

通过主动检测和被动检测的方式，排查网段中是否存在被感染主机，若排查确认存在，则通过 IP/MAC 定位主机，然后人工确认是否误报并判断是否感染病毒，进行下一步处理。

根据 NIPS 病毒感染探测和 RSAS 漏洞风险检测交叉得出风险评估结论：

- 无主机感染+无漏洞影响=安全；
- 无主机感染+有漏洞影响=有风险；

如下图所示，经人工确认开机主机未受病毒感染，但存在漏洞影响，就可判断网络存在风险，需及时更新安全补丁。



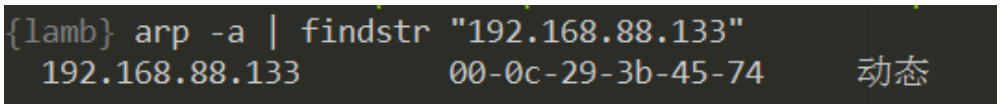
- 有主机感染+有漏洞影响/无漏洞影响=危险；

若主机已被感染病毒，屏幕会显示如下的告知付赎金的界面。

若通过分析和扫描，确认存在感染主机后，可在命令行下通过 IP 获取主机 MAC 地址，执行如下命令，查看 IP 地址对应的 Mac 地址。

```
arp -a | findstr "192.168.88.133"   或者   arp -a |find "192.168.88.133"
```

然后依据 Mac 查找到具体的主机。



4.4 风险处置

4.4.1 已感染病毒病毒主机处置

4.4.1.1 感染主机处置

针对已感染 WannaCry 病毒的主机，**首先进行断网隔离**，判断加密文件的重要性，决定是否格式化磁盘重装系统，还是保持断网状态等待进一步解密进展。

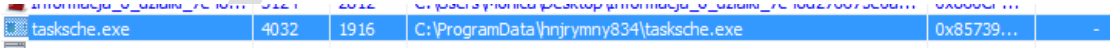
如果内网存在主机无法访问外部网络的情况，需要迅速在内网中添加 DNS 解析，将 www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com 解析到某台内网中可以访问的主机上，确保内网主机可以访问该域名，阻断蠕虫的进一步传播。

4.4.1.2 病毒清除

在被感染主机上，需要对蠕虫进行清除：

1. 关闭进程：

关闭 tasksche.exe 进程：



不完全执行的状态下，还可能有 mssecsvc.exe，即最初启动的那个进程，在后续完全执行的状态下，还可能有其他 tor 等的进程，建议在关闭进程的时候，将下面所列举的可执行文件涉及的相关进程都关闭掉，如下图所示。

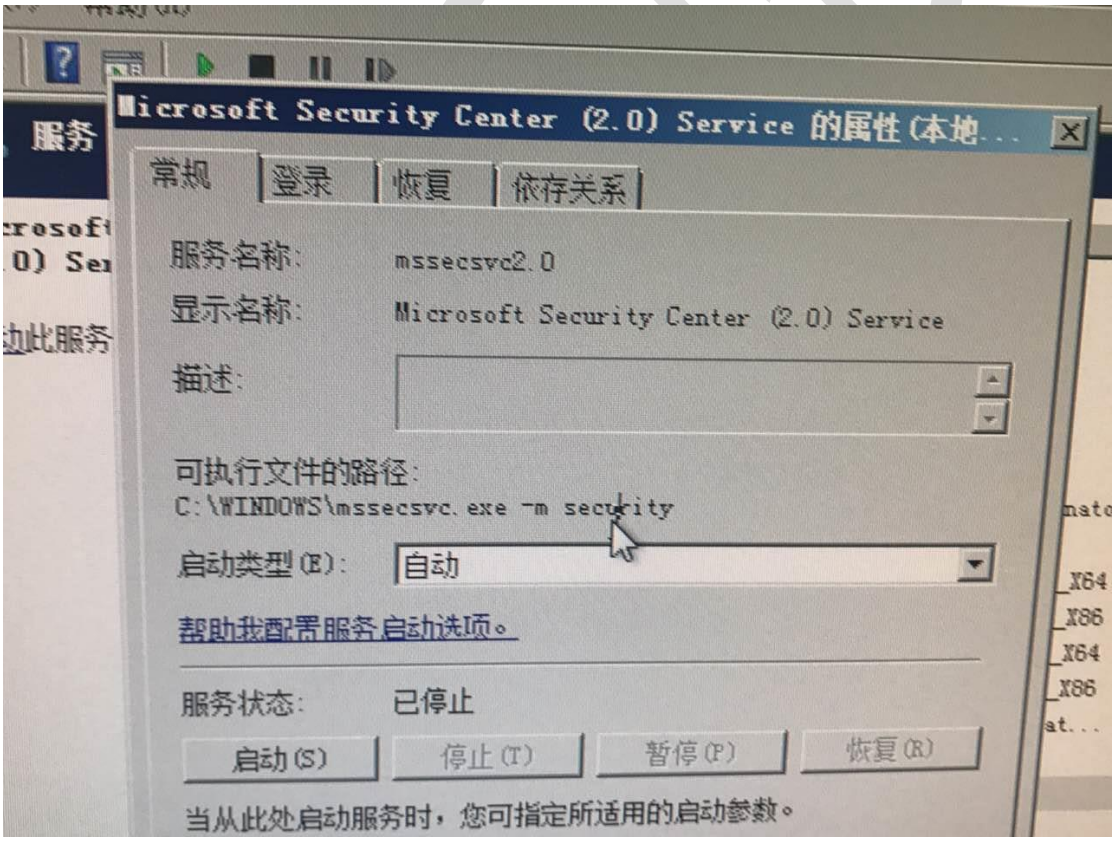
```
C:.
    00000000.eky
    00000000.pky
    00000000.res
    @Please_Read_Me@.txt
    @WanaDecryptor@.exe
    @WanaDecryptor@.exe.lnk
    b.wnry
    c.wnry
    f.wnry
    out.txt
    r.wnry
    s.wnry
    t.wnry
    taskdl.exe
    taskse.exe
    u.wnry

├─msg
└─TaskData
    ├─Data
    │   └─Tor
    └─Tor
            libeay32.dll
            libevent-2-0-5.dll
            libevent_core-2-0-5.dll
            libevent_extra-2-0-5.dll
            libgcc_s_sjlj-1.dll
            libssp-0.dll
            ssleay32.dll
            taskhsvc.exe
            tor.exe
            zlib1.dll
```

2. 删除相关服务：

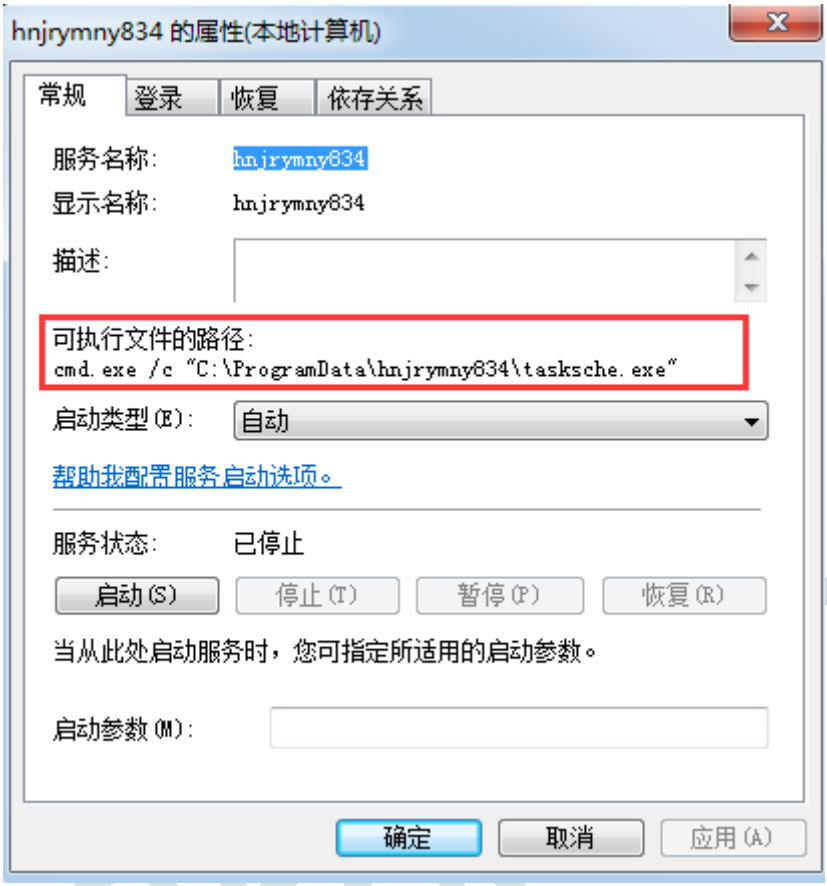
（1）删除服务 mssecsvc2.0，服务路径：

C:/WINDOWS/tasksche.exe 或者 C:/WINDOWS/mssecsvc.bin -m security



（2）删除 hnjrymny834（该服务名可能随机）服务：

查找对应的路径，在其路径名下删除可执行文件。



3. 清除注册表项：

在注册表中，删除以下键值：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\hnjrymny834 "C:\ProgramData\hnjrymny834\tasksche.exe"

或者

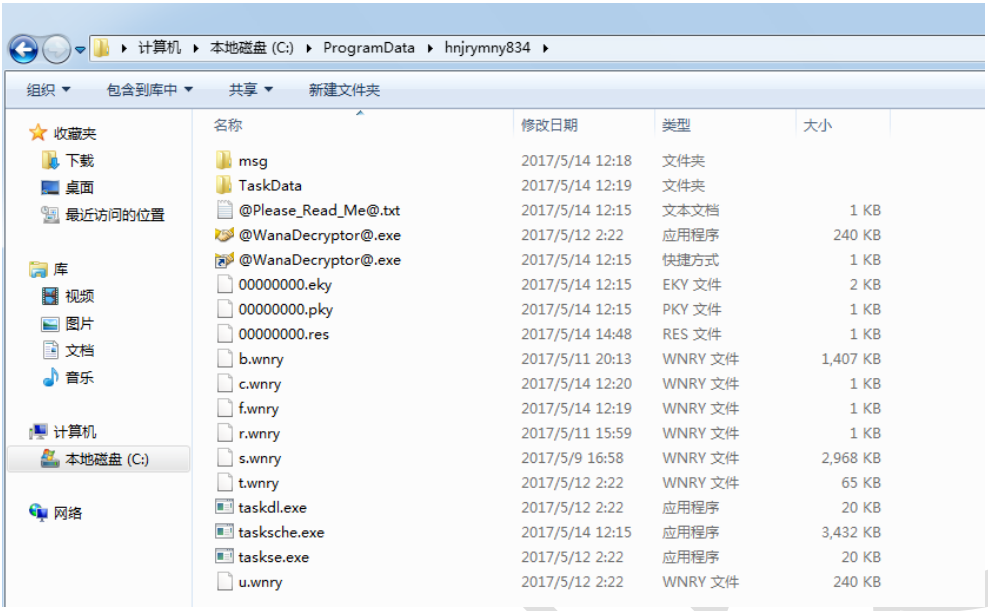
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\hnjrymny834

4. 删除病毒文件：

病毒运行后，释放的文件目录存在于

- C:\ProgramData\hnjrymny834
- C:\Users\All Users\hnjrymny834

如下图所示：



病毒的可执行文件主要有以下文件：

```
C:\WINDOWS\tasksche.exe
C:\ProgramData\hnjrymny834\tasksche.exe
C:\Users\All Users\hnjrymny834\tasksche.exe
```

其他病毒相关文件还存在于：

```
文件夹 PATH 列表：
C:.
|   00000000.eky
|   00000000.pky
|   00000000.res
|   @Please_Read_Me@.txt
|   @WanaDecryptor@.exe
|   @WanaDecryptor@.exe.lnk
|   b.wnry
|   c.wnry
|   f.wnry
|   out.txt
|   r.wnry
|   s.wnry
|   t.wnry
|   taskdl.exe
|   taskse.exe
|   u.wnry
|
```

```
├──msg
│       m_bulgarian.wnry
│       m_chinese (simplified).wnry
│       m_chinese (traditional).wnry
│       m_croatian.wnry
│       m_czech.wnry
│       m_danish.wnry
│       m_dutch.wnry
│       m_english.wnry
│       m_filipino.wnry
│       m_finnish.wnry
│       m_french.wnry
│       m_german.wnry
│       m_greek.wnry
│       m_indonesian.wnry
│       m_italian.wnry
│       m_japanese.wnry
│       m_korean.wnry
│       m_latvian.wnry
│       m_norwegian.wnry
│       m_polish.wnry
│       m_portuguese.wnry
│       m_romanian.wnry
│       m_russian.wnry
│       m_slovak.wnry
│       m_spanish.wnry
│       m_swedish.wnry
│       m_turkish.wnry
│       m_vietnamese.wnry
│
└──TaskData
    ├──Data
    │   └──Tor
    └──Tor
            libeay32.dll
            libevent-2-0-5.dll
            libevent_core-2-0-5.dll
            libevent_extra-2-0-5.dll
            libgcc_s_sjlj-1.dll
            libssp-0.dll
            ssleay32.dll
```

taskhsvc.exe tor.exe zlib1.dll

4.4.2 未感染病毒主机处置

剔除掉网段中存在的被感染病毒的主机后，对网段中的其他未感染的和未开机的终端进行安全排查并进行加固。

4.4.2.1 补丁修复

对于提供文件共享以及与认证服务相关的服务器，由于业务需求不能关闭端口和禁用服务，因此，建议使用升级补丁的方式进行加固处理。

您可选择如下方式的任意一种，对网络中的主机进行修复漏洞。

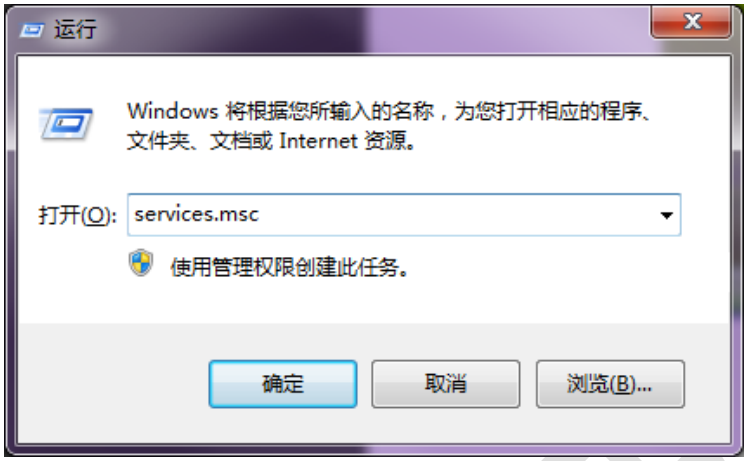
- 根据**附录 A MS17-010 补丁对应和下载列表**查找机器对应的更新补丁包，使用一台合理加固后的主机下载漏洞修复补丁，拷贝至目标主机后进行安装升级。
- 在域的机器如果配置有 WSUS，可以进行域推送。统一修复对应的漏洞。
- 使用“绿盟科技离线补丁升级工具”对存在漏洞的主机离线安装补丁，或者禁用 Server 服务进行临时加固，确保漏洞被合理修复后，再使用“绿盟科技一键加固恢复脚本”对服务器进行恢复。

4.4.2.2 人工加固

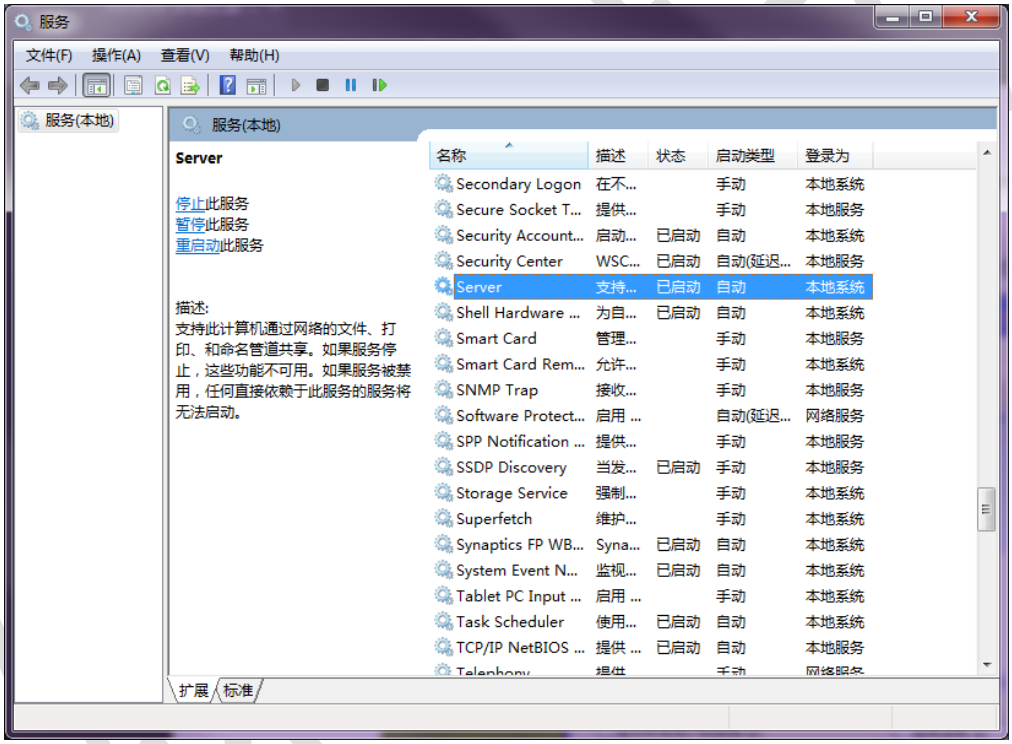
如果不方便使用脚本可以采取手动加固的方式进行加固，可通过防火墙过滤 445 端口或者禁用 Server 服务的方式，针对 WannaCry 蠕虫病毒做临时防护处理，最终的解决方案还是升级补丁。

禁用 Server 服务加固处理

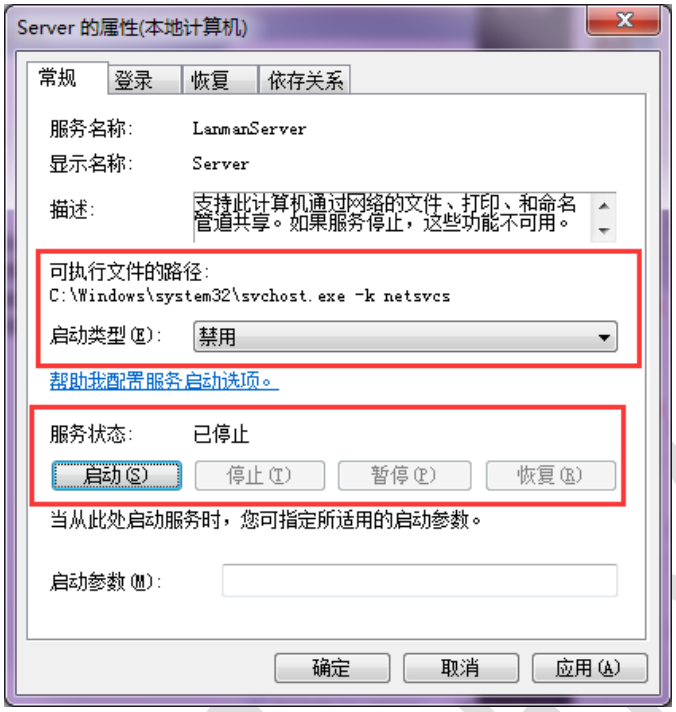
1. 使用 win+r 组合按键，调出运行框，输入“services.msc”调出本地服务浏览窗口。



2. 打开服务后，查找 server 服务：

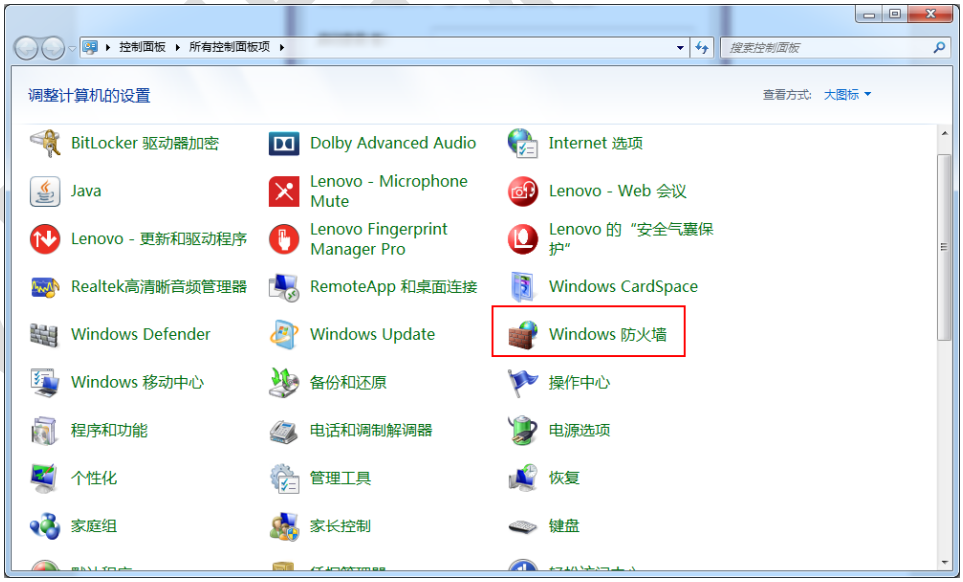


3. 将启动类型修改为禁用，此操作会防止重启以后 server 服务重新启动。点击停止按钮，将服务状态修改为‘已停止’状态。如下图所示

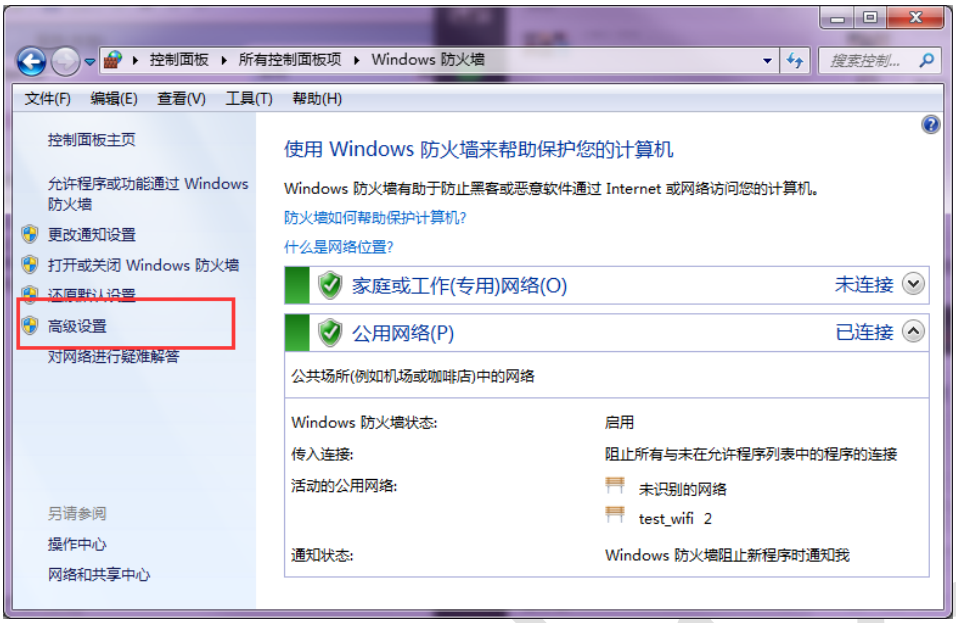


本机防火墙策略屏蔽 445 端口流量防护

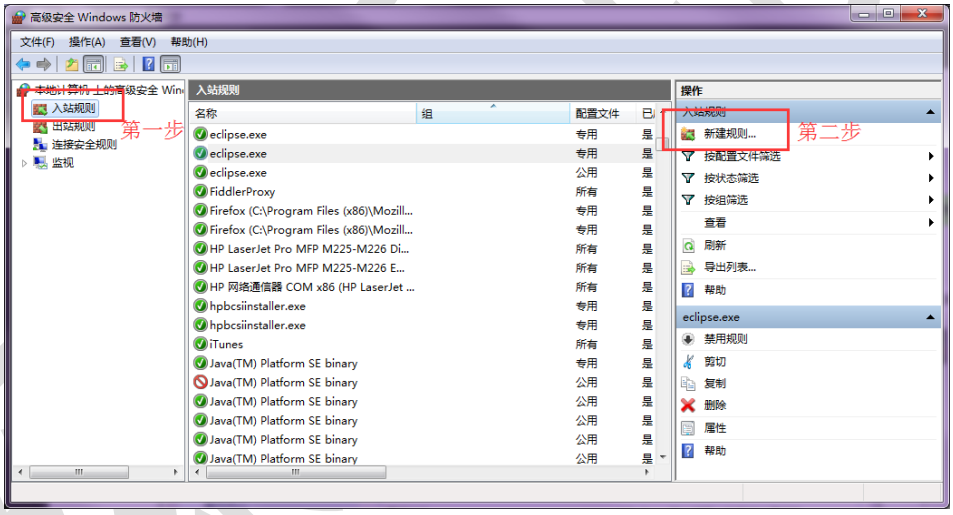
1. 在控制面板中打开 Windows 防火墙：



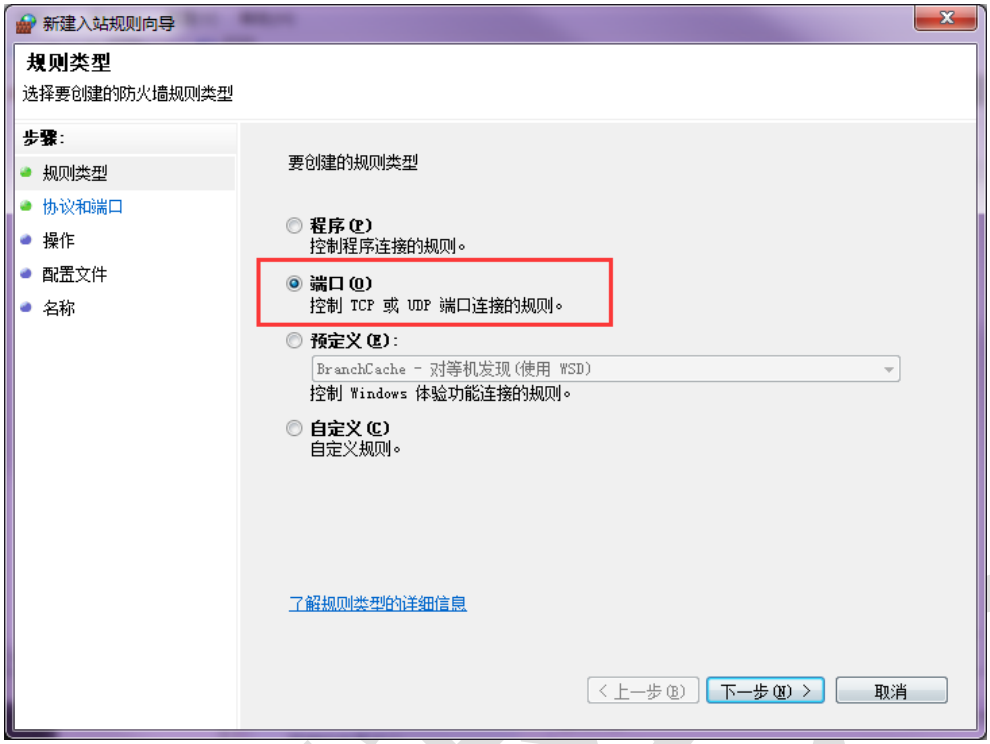
2. 进入 Windows 防火墙配置界面，点击“高级设置”。



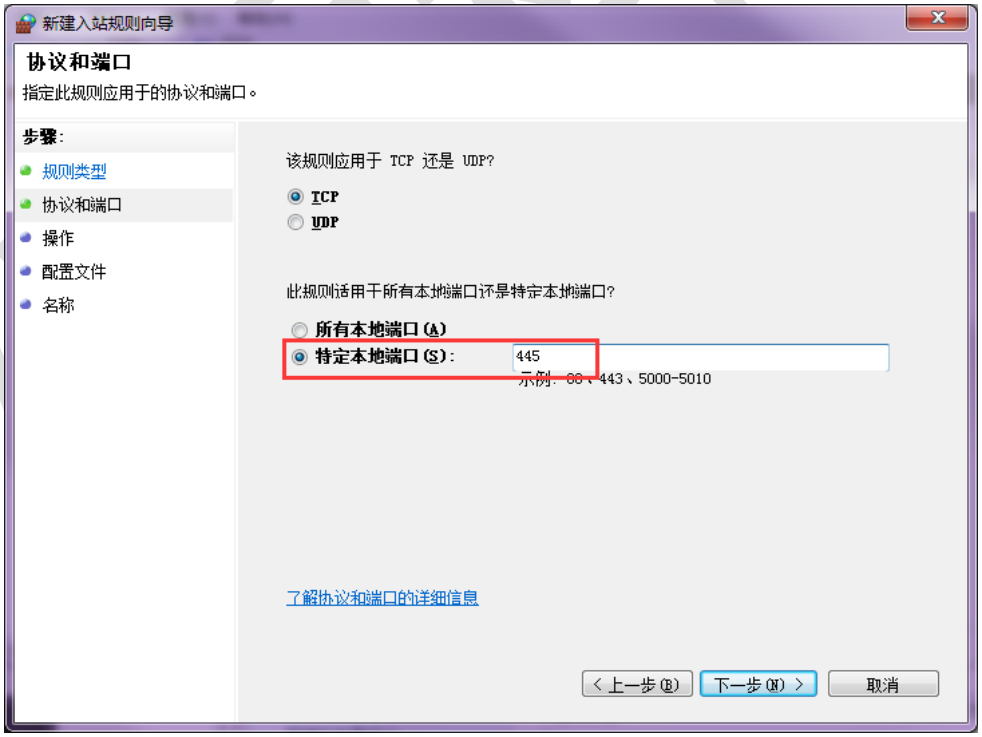
3. 点击入站规则，再点击新建规则创建防火墙入站规则：



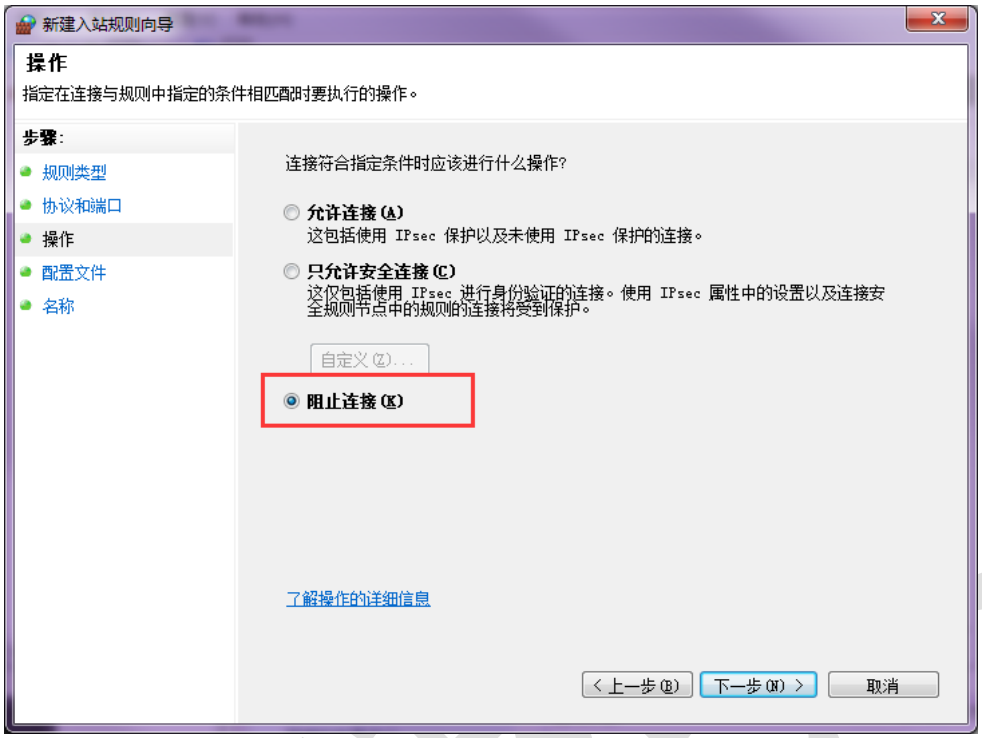
4. 在新建入站规则向导中，针对协议和端口步骤，选择对端口过滤。



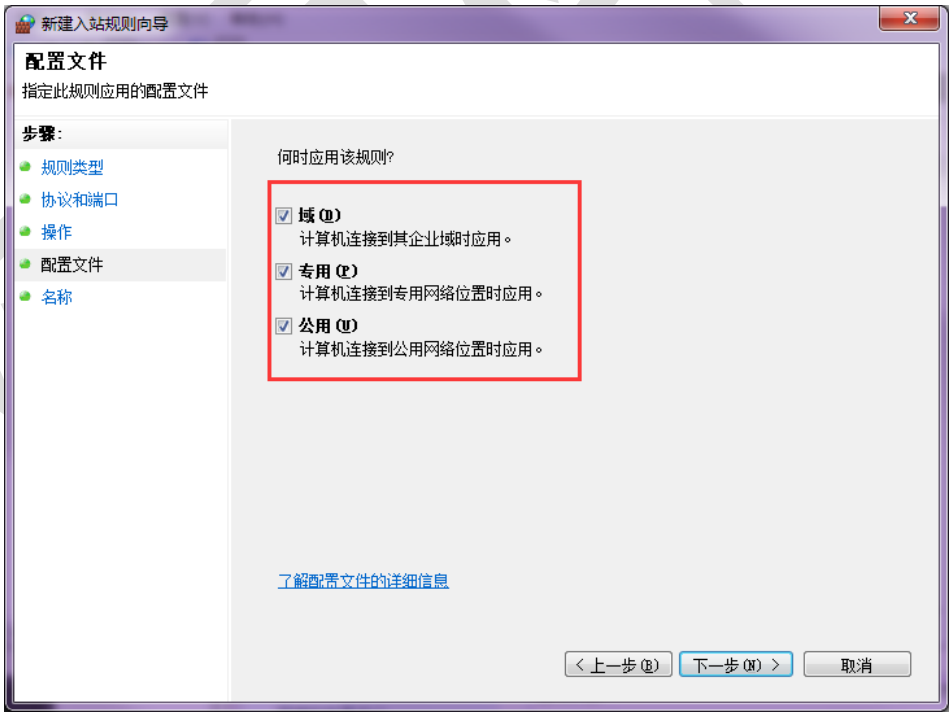
选择 TCP 协议和特定本地端口：445



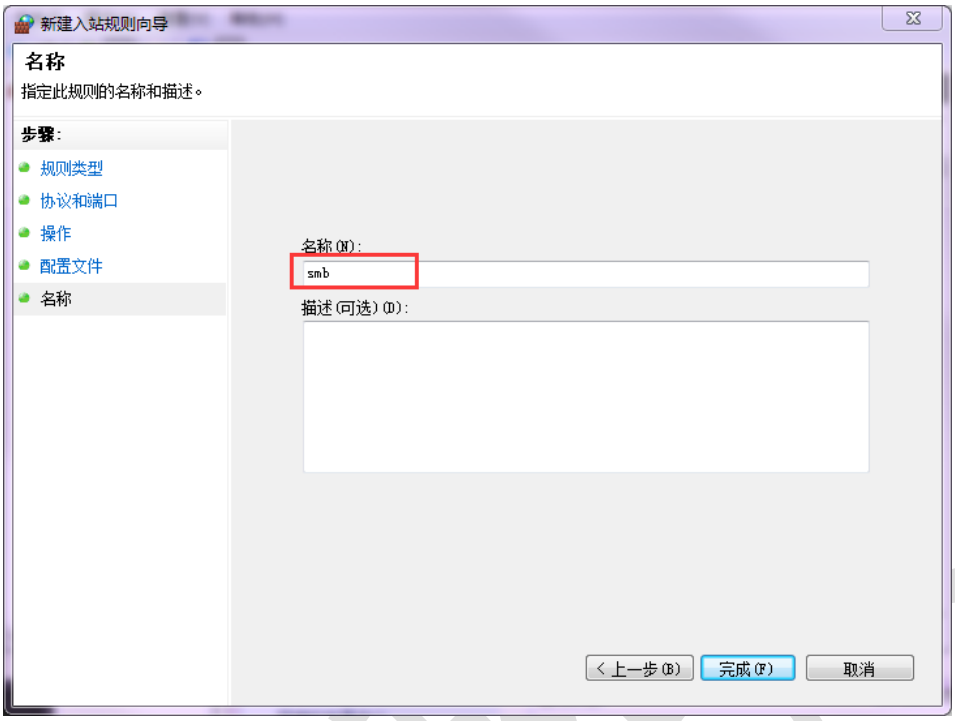
5. 在操作步骤中，选择阻止连接。



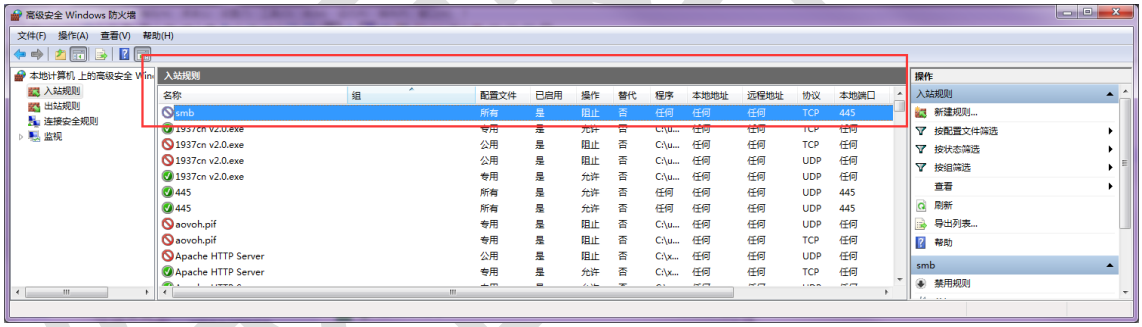
6、在应用该规则处，勾选域、专用以及公用选项。



7、填入规则名称，完成创建。



规则创建完成后，可看到入站规则中存在 445 阻断规则。

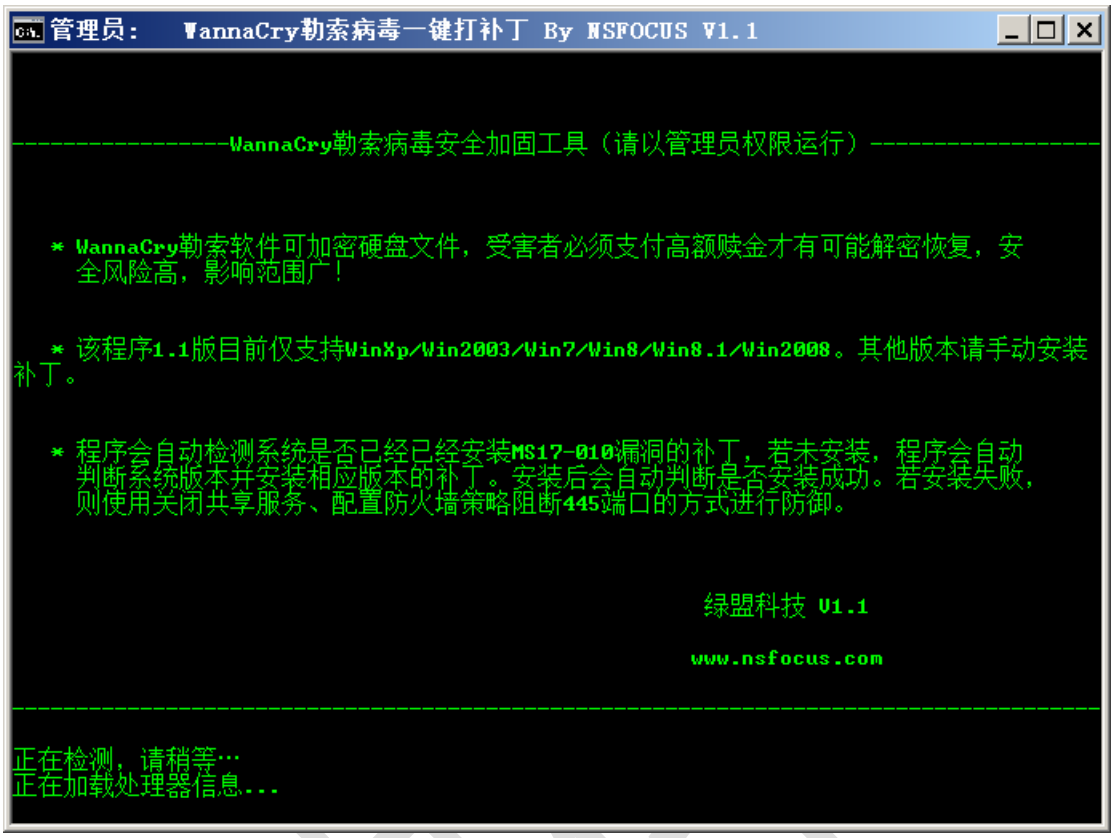


4.4.3 离线补丁升级工具

绿盟科技提供“WannaCry 勒索病毒安全加固”工具，可联系绿盟科技相关支持人员获取工具。

自动检测系统是否已经安装 MS17-010 漏洞的补丁，若未安装，则自动判断系统版本并安装相应版本的补丁。如果安装失败，工具会通过关闭 Server 服务，配置防火墙策略阻断端口进行防御。

在使用时，以**管理员权限**运行工具，对系统进行升级，运行效果如下图：



注：

- Windows 8 以上系统需要在安装后重启手动判断补丁是否安装成功。
- Windows Server 2012 及以上版本暂不支持，下一个版本进行更新；

4.5 持续监测

4.5.1 主动检测

- 在主机加固完成后，所有主机开机并使用 RSAS 再次进行扫描确认，是否受 MS17-010 漏洞的影响。详细操作过程参考 **4.2.1.1 MS17-010 漏洞扫描**小节
- 定期使用 RSAS 做漏洞扫描，针对网段主机进行风险评估，若发现新接入主机存在风险，及时通报给相关人员。

4.5.2 被动持续监测

网络中接入 NIPS，通过流量镜像分析的方式，持续对网络中的蠕虫病毒攻击监测。配置 NIPS 监测和防护策略，对网络中的蠕虫病毒攻击实时监测。

附录A MS17-010 补丁对应和下载列表

操作系统版本	对应 KB 号	补丁下载链接
Windows XP SP3 x86	KB4012598	http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-chs_dca9b5adddad778cfd4b7349ff54b51677f36775.exe
Windows XP SP2 x64	KB4012598	http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-enu_f24d8723f246145524b9030e4752c96430981211.exe http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-jpn_9d5318625b20faa41042f0046745dff8415ab22a.exe
Windows XP Embedded	KB4012598	http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-embedded-custom-chs_41935edbcd6fa88a69718bc85ab5fd336445e7f9.exe
Windows Server 2003 x64	KB4012598	http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-chs_68a2895db36e911af59c2ee133baee8de11316b9.exe
Windows Server 2003 x86	KB4012598	http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x86-custom-chs_b45d2d8c83583053d37b20edf5f041ecede54b80.exe
Windows Vista Service Pack 2	KB4012598	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-

		x86_13e9b3d77ba5599764c296075a796c16a85c745c.msu
Windows Vista x64 Edition Service Pack 2	KB4012598	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x64_6a186ba2b2b98b2144b50f88baf33a5fa53b5d76.msu
Windows Server 2008（用于 32 位系统）Service Pack 2	KB4012598	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x86_13e9b3d77ba5599764c296075a796c16a85c745c.msu
Windows Server 2008（用于基于 x64 的系统）Service Pack 2	KB4012598	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x64_6a186ba2b2b98b2144b50f88baf33a5fa53b5d76.msu
Windows Server 2008（用于基于 Itanium 的系统）Service Pack 2	KB4012598	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-ia64_83a6f5a70588b27623b11c42f1c8124a25d489de.msu
Windows 7（用于 32 位系统）Service Pack 1	KB4012212	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x86_6bb04d3971bb58ae4bac44219e7169812914df3f.msu
Windows 7（用于基于 x64 的系统）	KB4012212	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-

Service Pack 1		x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu
Windows Server 2008 R2（用于基于 x64 的系统）Service Pack 1	KB4012212	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu
Windows Server 2008 R2（用于基于 Itanium 的系统） Service Pack 1	KB4012212	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-ia64_93a42b16dbea87fa04e2b527676a499f9fbba554.msu
Windows 8.1（用于 32 位系统）	KB4012213	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8.1-kb4012213-x86_e118939b397bc983971c88d9c9ecc8cbec471b05.msu
Windows 8.1（用于基于 x64 的系统）	KB4012213	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8.1-kb4012213-x64_5b24b9ca5a123a844ed793e0f2be974148520349.msu
Windows Server 2012	KB4012214	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8-rt-kb4012214-x64_b14951d29cb4fd880948f5204d54721e64c9942b.msu
Windows Server 2012 R2	KB4012213	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8.1-kb4012213-

		x86_e118939b397bc983971c88d9c9ecc8cbec471b05.msu
Windows 10（用于 32 位系统）	KB4012606	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4012606-x86_8c19e23de2ff92919d3fac069619e4a8e8d3492e.msu
Windows 10（用于基于 x64 的系统）	KB4012606	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4012606-x64_e805b81ee08c3bb0a8ab2c5ce6be5b35127f8773.msu
Windows 10 版本 1511（用于 32 位系统）	KB4013198	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4013198-x86_f997cfd9b59310d274329250f14502c3b97329d5.msu
Windows 10 版本 1511（用于基于 x64 的系统）	KB4013198	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4013198-x64_7b16621bdc40cb512b7a3a51dd0d30592ab02f08.msu
Windows 10 版本 1607（用于 32 位系统）	KB4013429	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4013429-x86_8b376e3d0bff862d803404902c4191587afbf065.msu
Windows 10 版本 1607（用于基于 x64 的系统）	KB4013429	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/03/windows10.0-kb4013429-x64_ddc8596f88577ab739cade1d365956a74598e710.msu

Windows Server 2016（用于基于x64 的系统）	KB4013429	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/03/windows10.0-kb4013429-x64_ddc8596f88577ab739cade1d365956a74598e710.msu

附录B ACL 网络访问控制

在三层交换机上配置 ACL 规则，做好 445 端口的屏蔽操作，这里提供了常见的网络设备建议的配置方法，仅供网络管理人员参考。

Juniper 设备的配置示例：

```
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
```

华三（H3C）设备的配置示例：

```
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
```

华为设备配置示例：

```
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
```

Cisco 设备配置示例：

```
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
```

锐捷设备配置示例：

```
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
```

附录C FAQ

Q：如果有应急需求，如何联系？

A：绿盟科技应急指挥中心电话：400-818-6868，可以随时拨打或者联系客户经理，以便就近需求快速支援。

Q：WannaCry 如何进行传播？

A：利用 Windows SMB 服务存在的漏洞进行传播，只需要联网，即可远程感染。

Q：Win10 系统是否受影响？

A：不受影响。

Q：如何检测主机是否已感染 WannaCry？

A：主机侧可使用杀毒软件或专杀工具进行检测和清除。网络侧可使用绿盟远程安全评估系统（简称 RSAS）远程批量检测存在漏洞的主机。

Q：如何监测网络内是否有 WannaCry 正在传播？

A：可部署绿盟网络入侵防护系统（简称 IPS），对镜像的交换机流量进行分析，及时发现 WannaCry 的传播。

Q：处理已感染的 WannaCry 主机时需要注意什么？

A：应先将已感染的主机断网，未感染主机最好也断网，不能断网的应首先阻断 445 端口，再进行补丁安装。

Q：使用网上免疫程序时需要注意什么？

A：目前 360、安天实验室等发布了免疫工具，通过禁用 WannaCry 利用的端口、服务等方式对感染传播途径进行阻断。需要注意以下两点：1.进行免疫后，还应安装 MS17-010 漏洞补丁。2.免疫工具禁用的 TCP 445 端口可能会影响 windows 域环境，在安装补丁、杀毒后及时恢复。

Q：绿盟远程安全评估系统（简称 RSAS）是否能防护？

A：2017 年 4 月已经发布 MS17-010 漏洞扫描插件。

Q：绿盟网络入侵防护系统（简称 NIPS）是否能防护？

A：2017 年 4 月已经发布 MS17-010 漏洞扫描插件。

5.6.10 的病毒特征库中已经添加规则。

Q：绿盟 NF 防火墙系统如何防护？

A：新建安全区，新建对象 445 端口服务，设置 TCP 445 端口的阻断策略。