360 企业安全针对"永恒之蓝"攻击紧急应对手册

目录

第−	一部分	}───通用环境指导	3
	—	确认主机是否被感染	3
	二、	网络层面	4
		1. 网络层 ACL 调整	4
		2. IPS 特征库更新	9
	三、	服务器层面	9
		1. 安装漏洞补丁	9
		2. 免疫工具1	.0
		3. 关闭服务1	.0
		4. 组策略调整1	.3
	四、	终端层面2	5
		1. 免疫工具	5
		2. 关闭服务	5
		3. 组策略调整	8
		4. 安装漏洞补丁4	0
	五、	周一开机及上线保障指南4	0
第二	二部分	~——针对已使用 360 企业安全产品的运维人员4	2
第三	三部分	~——互联网主机应急处置操作指南4	-2

本手册分三部分对此次"永恒之蓝"攻击提供针对性防护建议:通用环境指导,360企 业安全产品操作指导,互联网主机防护指导。

第一部分——通用环境指导

此部分针对通用 IT 环境,从已感染主机的处理,到网络、服务器、终端几个层面的防护提供建议,应对此次攻击。最后提供了"周一开机及上线保障指南",供 IT 管理员参考。

一、确认主机是否被感染

Tana DecryptOr 2.0 X Ooops, your files have been encrypted! Chinese (simpli ٠ 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。 Payment will be raised on 5/16/2017 02:26:59 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 Time Left 够提供安全有效的恢复服务。 02:22:35:15 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。 Your files will be lost on 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 5/20/2017 02:26:59 对你不利。 Time Left 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。 06:22:35:15 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: bitcoin About bitcoin 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 Copy ACCEPTED HERE How to buy bitcoins? Contact Us **Check Payment** Decrypt

被感染的机器屏幕会显示如下的告知付赎金的界面:

如果主机已被感染:

则将该主机隔离或断网(拔网线)。若文档尚未被全部加密,则应立即关机,使用 PE 盘引导进入 PE 系统后将尚未加密的文档备份转移避免损失的进一步扩大。若客户存 在该主机备份,则启动备份恢复程序。执行恢复后的主机应参照未被感染主机的防护措 施加固后再入网。

如果主机未被感染:

从以下几个层面实施防护。

二、网络层面

1. 网络层 ACL 调整

大型机构由于设备众多,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 ACL 策略配置,以实现临时封堵。

该蠕虫病毒主要利用 TCP 的 445 端口进行传播,对于各大企事业单位影响很大。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,举例说明如何配置 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。

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

set interfaces [需要挂载的二层端口名称] unit 0 family inet filter input deny-wannacry

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

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

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

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. IPS 特征库更新

多数 IPS 厂商为了应对此类攻击,会针对性的升级特征库。建议 IT 安全、运维人员及时关注厂商发布的信息,并升级特征库。

三、服务器层面

1. 安装漏洞补丁

微软针对本次事件,对支持的操作系统在安全公告 MS17-010 中已发布相应补丁修复,对于部分已停服的 Win XP、2003 也已紧急发布补丁 KB4012598 修复。请在所有服务器及终端安装依据操作系统类型不同对应安装相应的补丁。下载来源: MS17-010 Security Update:

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

KB4012598

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

or 360 云盘:

https://yunpan.cn/cXLwmvHrMF3WI 访问密码 614d

根据不用的操作系统版本,手动安装以上补丁后,可直接修复此次"永恒之蓝"攻 击的所利用的系统漏洞。 另外也可更新天擎控制中心补丁库升级到 1.0.1.2825 及以上版本,并安装其中包含的所有高危漏洞。

打补丁可能会对用户的现有业务系统、办公软件等造成影响,在生产服务器上安装前,需做好兼容性测试,避免影响业务。

2. 免疫工具

在补丁安装完成前,为避免服务器感染,手工或使用主机管理系统下发免疫工具(下载页面:http://b.360.cn/other/onionwormimmune),免疫工具将不影响当前445端口业务的运行,运行后可在任务管理器中检查其状态:

INDOWS 任务管理器											
文件(E) 选项(D) 查看(V)	关机(11) 帮助(14)										
应用程序 进程 性能 联网 用户											
映像名称	用户名	CPU 🔼									
taskmgr.exe	zzp	00									
73095b7a1a52aa072de7db	2 <mark>d System</mark>	00									
OnionWormImmune.exe	zzp	00									
ctfmon.exe	zzp	00									
vmtoolsd.exe	zzp										
explorer, exe	ICCAL SERVICE	00 =									
arg. exe	SYSTEM	00									
spoorsv.exe	IOCAL SERVICE	00									
sychost, exe	NETWORK SERVICE	00									
svchost. exe	SYSTEM	00									
wuauclt.exe	zzp	00									
svchost. exe	NETWORK SERVICE	00									
svchost. exe	SYSTEM	00									
vmacthlp.exe	SYSTEM	00									
lsass.exe	SYSTEM	00									
services.exe	SYSTEM	00 🞽									
<		>									
□ 显示所有用户的进程 (S)											
进程数: 23 CPV 使用: 2	2% 提交更改: 133M	/ 1246M									

3. 关闭服务

如果免疫工具运行遇到问题,也可选择关闭445端口相关服务:

点击开始菜单,运行, cmd, 确认。

输入命令 netstat -- an 查看端口状态

🔤 C:\V]	NDOWS\system32\cmd.exe			- 🗆 🗙					
Microsoft Windows XP [版本 5.1.2600] <c> 版权所有 1985-2001 Microsoft Corp.</c>									
C:\Documents and Settings\admin>netstat -an									
Active C	onnections								
Proto	Local Address	Foreign Address	State						
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING						
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING						
TCP	127.0.0.1:1029	0.0.0.0:0	LISTENING						
TCP	192.168.232.137:139	0.0.0.0:0	LISTENING						
UDP	0.0.0.0:445	*:*							
UDP	0.0.0.0:500	* *							
UDP	0.0.0.0:1025	*:*							
UDP	0.0.0.0:4500	*:*							
UDP	127.0.0.1:123	*:*							
UDP	127.0.0.1:1900	*:*							
UDP	192.168.232.137:123	*:*							
UDP	192.168.232.137:137	*:*							
UDP	192.168.232.137:138	*:*							
UDP	192.168.232.137:1900	*:*							
C:\Docum	ents and Settings \admir	ı>net stop rdr							
Workstat	ion 服务正在停止.			_					

输入 sc config srv start= disabled (注意 disabled 前有空格)

sc config netbt start= disabled (注意 disabled 前有空格)

输入 net stop rdr 回车

net stop srv 回车

net stop netbt 回车

如果有提问"您想继续此操作吗? (Y/N) [N]:", 输入 Y

		and the second second
	💽 🖸 C:\VINDOVS\system32\cmd. exe	- 🗆 🗙
Oni on#or	UDP 192.168.232.137:1900 *:*	
	C:\Documents and Settings\admin>net stop rdr Workstation 服务正在停止. Workstation 服务已成功停止。	
	C:\Documents and Settings\admin>net stop srv Server 服务正在停止. Server 服务已成功停止。	
	C:\Documents and Settings\admin>net stop netbt 下面的服务依赖于 NetBios over Tcpip 服务。 停止 NetBios over Tcpip 服务也会停止这些服务。	
	TCP/IP NetBIOS Helper DHCP Client	
	是否继续此操作? <y n=""> [N]: y</y>	
	TCP/IP NetBIOS Helper 服务已成功停止。	100
	DHCP Client 服务正在停止. DHCP Client 服务已成功停止。	- I
	回收站	
🛃 开始 🌖	GN C:\WINDOWS\syste	

再次输入 netsta –an , 成功关闭 445 端口。

						- WINGOWS AT	rioressional		
		3 ()	9						
	100	-	138 L				STREET, STREET,		1.100
	1000	🔤 C:\V	INDOWS\s	system32\	cnd. exe			_ [
UnionWor.		C: \Docur							
		Active (Connecti	ions					
A.		Proto	Local	Address		Foreign Address	State		
		TCP	0.0.0.	0:135		0.0.0.0:0	LISTENING		
		TCP	127.0.	0.1:1029		0.0.0.0:0	LISTENING		
		UDP	0.0.0.	.0:500		*:*			and the
		UDP	0.0.0.	0:1025		* *			
		UDP	407 0	0:4500		*:*			
		UDF	127.0.	0.1-1040		*.*			
		IINP	127.0. 127.0	0 1:1900		*:*			
		0.21	101101	011-1700					
-	-	C: Docum	nents an	nd Setting	ys∖admin	\rightarrow			
									ALC: NO
		C: Docur	nents an	nd Setting	ys∖admin	ı>			
170.5		C: \Docur	nents an	nd Setting	rs∖admin	i>ccc			
CIPERTO .									and the second
		C:\Docur	nents an	nd Setting	ys∖admin				
									100000
		_	-	-			The second second		
-							回收站		
			and the second second	in the second				New Street	
		All and the second		and the second	1.4	and the state of the second	and the second se		- and a set of
🛃 开刻	台) [C:\WINDO	∦S\syste						
State of the second second									

4. 组策略调整

另一方式是用主机 ACL 策略封堵 445 端口。请注意,2、3、4 这三种方式,做到其中

任意一个即可达到临时免疫的目的。

通过组策略 IP 安全策略限制 Windows 网络共享协议相关端口

开始菜单->运行,输入gpedit.msc回车。打开组策略编辑器

在组策略编辑器中,计算机配置->windows设置->安全设置->ip安全策略下,

在编辑器右边空白处鼠标右键单击,选择"创建 IP 安全策略"



下一步->名称填写"封端口",下一步->下一步->勾选编辑属性,并点完成

IP 安全策略向导		\times
	正在完成 IP 安全策略向导	
	你已成功地完成指定你的新 IP 安全策略的属性。	
	要立即编辑你的 IP 安全策略,请选中"编辑属性"复选框,然后 单击"完成"。	
	☑ 編辑属性(P)	
	若要关闭此向导 , 请单击"完成"。	
	< 上一步(<u>B</u>) 完成 取消	

去掉"使用添加向导"的勾选后,点击"添加"



在新弹出的窗口,选择"IP筛选列表"选项卡,点击"添加"



在新弹出的窗口中填写名称,去掉"使用添加向导"前面的勾,单击"添加"

💵 IP 筛选器列表



>

在新弹出的窗口中,"协议"选项卡下,选择协议和设置到达端口信息,并点确定。

IP 筛选器 属性		×
地址 协议 描述		
选择协议类型(P):		
ТСР 🗸		
6		
设置 IP 协议端口:		
●从任意端口(上)		
○从此端口(图):		
○ 到任意端口(1)		
◉ 到此端口(<u>O</u>):		
135		
	确定	取消

重复第 7 个步骤 , 添加 TCP 端口 135、139、445。添加 UDP 端口 137、138。添加全部完成后 , 确定。

选中刚添加完成的"端口过滤"规则,然后选择"筛选器操作"选项卡。

新规则 属性	Х
IP 筛选器列表 筛选器操作 身份验证方法 隧道设置 连接类型	
所选的 IP 筛选器列表指定了哪个网络流量将受此规则影响。	
IP 筛选器列表(L):	
名称	
添加(D) 编辑(E) 删除(R)	
关闭 取消 应用(A)

去掉"使用添加向导"勾选,单击"添加"按钮



1. 选择"阻止"

新筛选器操作 属性	×
安全方法常规	
○许可(M) ● 阻止(L)	
○协商安全(<u>N</u>):	
安全方法首选顺序(S):	
类型 AH 完整性 ESP 机密性 ESP 完整性	添加(<u>D</u>)
	编辑(E)
	删除(<u>R</u>)
	上移(U)
< >	下移(0)
接受不安全的通讯,但始终用 IPsec 响应(C)	
使用会话密钥完全向前保密(PFS)(K)	
确定取消	应用(<u>A</u>)

- 选择"常规"选项卡,给这个筛选器起名"阻止",然后"确定"。
 点击
- 确认 "IP 筛选列表"选项卡下的"端口过滤"被选中。确认"筛选器操作"选项 卡下的"阻止"被选中。然后点击"关闭"。

新规则 属性		Х
IP 筛选器列表	筛选器操作 身份验证方法 隧道设置 连接类型	
\times	选择的筛选器操作指定了此规则是否协商及如何来保证网络流量 的安全。	:
筛选器操作([):	-
名称	描述	
◎阻止		
添加(<u>D</u>)	. 编辑(E) 删除(R) □使用"添加向导"(W)	
	关闭 取消 应用(A)	

4. 确认安全规则配置正确。点击确定。

封端口 厪性			? ×
规则常规			
▲ ■ ■<	算机通讯的安全规则		
IP 安全规则([):			
IP 節這器列表	筛选 <mark>器</mark> 操作	身份验证方法	隧道终结点
☑ 端口过滤	阻止	<无>	无
□ <动态>	默认响应(仅限于	Kerberos	<无>
<			>
添加(D)	编辑(E) 删除	≹(<u>R)</u> □使用]"添加向导"(<u>W</u>)
		确定	取消

5. 在"组策略编辑器"上,右键"分配",将规则启用。

🗐 本地组策略编辑器							—	×
文件(F) 操作(A) 查看(V) 帮助(H)								
🗢 🔿 🖄 📷 🗶 🗟 😖 👔 👘 🎽 💆 🧕								
🗐 本地计算机 策略	^	名称		^	描述			策略已排
▼ 👰 计算机配置			端口					否
> 🧾 软件设置				分配(A)		1		
✔ 🛗 Windows 设置								
> 🧾 域名解析策略				所有任务(K)	>			
😅 脚本(启动/关机)				删除(D)				
> 💼 已部署的打印机				重命名(M)				
▶ 🚡 安全设置								
				馮任(K)				
				帮助(H)				
> 📄 高级安全 Windows 防火増			_					
🕲 IP 安全策略,在 本地计算机								
> ₩ 基于策略的 QoS								
>	4	<		1				>

四、终端层面

1. 免疫工具

由于批量终端的补丁安装需要一定时间,建议先用桌面管理类软件,在所有终端运行免疫工具(下载页面:http://b.360.cn/other/onionwormimmune),运行后可在任务管理器中检查其状态:

INDOVS 任务管理器		
文件(F) 选项(Q) 查看(V) 关机	(1) 帮助(1)	
应用程序进程性能联网	用户	
映像名称	用户名	CPU 🔼
taskmgr.exe 73095b7a1a52aa072de7db2d OnionWormImmune.exe ctfmon.exe ymtoolsd.exe	zzp SYSTEM zzp zzp	00 00 00 00 00
explorer.exe	zzp	00
alg. exe spoolsv. exe svchost. exe svchost. exe	LOCAL SERVICE SYSTEM LOCAL SERVICE NETWORK SERVICE	00 00 00 00
svchost. exe wuauclt. exe	SYSTEM zzp NETWORK SERVICE	00
svchost.exe svchost.exe ymacthlp.exe	SYSTEM SYSTEM	00
lsass.exe services.exe	SYSTEM	00
<		>
显示所有用户的进程(S)	结	束进程 (2)
进程数: 23 CPV 使用: 2%	提交更改: 133M	/ 1246M

2. 关闭服务

如果免疫工具运行遇到问题,也可选择关闭 445 端口相关服务:

点击开始菜单,运行, cmd, 确认。

输入命令 netstat –an 查看端口状态

🔤 C:\V]	NDOWS\system32\cmd.exe			- 🗆 🗙
Microsof (C)版权	t Windows XP [版本 5.1. 所有 1985-2001 Microsof	2600] t Corp.		
C:\Docum	ents and Settings\admin	>netstat −an		
Active C	Connections			
Proto	Local Address	Foreign Address	State	
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	
TCP	127.0.0.1:1029	0.0.0.0:0	LISTENING	
TCP	192.168.232.137:139	0.0.0.0:0	LISTENING	
UDP	0.0.0.0:445	*:*		
UDP	0.0.0.0:500	*:*		
UDP	0.0.0.0:1025	*:*		
UDP	0.0.0.0:4500	*:*		
UDP	127.0.0.1:123	*:*		
UDP	127.0.0.1:1900	*:*		
UDP	192.168.232.137:123	*:*		
UDP	192.168.232.137:137	*:*		
UDP	192.168.232.137:138	*:*		
UDP	192.168.232.137:1900	*:*		
C:\Docum	ents and Settings\admin	>net stop rdr		
Workstat	100 服穷止往停止.			

输入 net stop rdr 回车

net stop srv 回车

net stop netbt 回车



再次输入 netsta -- an , 成功关闭 445 端口。也可用 "telnet 主机名 445" 的命令

来验证终端端口已关闭。

				WINDOWS AF FIDIC	SSIVITAL	
	3€ (…)		0 4 2 1			
	100	1000		Constant of the local division of the local		A COLORED
	🔤 C:\V]	INDOWS\system32\	cad. exe			- 🗆 🗙
Oni onfor						
	C:\Docum	ents and Settin	gs∖admin>netsta	t -an		
	Active C	Connections				
	Proto	Local Address	Foreig	n Address	State	
	TCP	0.0.0.0:135	0.0.0.	0:0	LISTENING	
	TCP	127.0.0.1:1029	0.0.0.	0:0	LISTENING	
	UDP	0.0.0.0:500	*:*			
	UDP	0.0.0.0:1025	*:*			
	UDP	0.0.0.0:4500	*:*			
	UDP	127.0.0.1:123	*:*			
	UDP	127.0.0.1:1049	*:*			10000
	UDP	127.0.0.1:1900	*:*			
	C:\Docum	ents and Settin	gs\admin>			
	C:\Docum	ents and Settin	gs∖admin≻			
	C:\Docum	ments and Settin	gs∖admin≻ccc			2466
Participation .	C:\Docum	ents and Settin	gs∖admin>_			
	and the second se					
	100 m					and second second
	101					
					回收站	
		Sall and a second	And the second second second			
and the second second						Contraction of the second
TT HA						
💶 मण्डन	C:\WINDOW	S\syste				

3. 组策略调整

另一方式是用主机 ACL 策略封堵 445 端口。请注意,2、3、4 这三种方式,做到其中

任意一个即可达到临时免疫的目的。

通过组策略 IP 安全策略限制 Windows 网络共享协议相关端口

开始菜单->运行,输入gpedit.msc回车。打开组策略编辑器

在组策略编辑器中,计算机配置->windows设置->安全设置->ip安全策略下,

在编辑器右边空白处鼠标右键单击,选择"创建 IP 安全策略"



下一步->名称填写"封端口",下一步->下一步->勾选编辑属性,并点完成

IP 安全策略向导		\times
	正在完成 IP 安全策略向导	
	你已成功地完成指定你的新 IP 安全策略的属性。	
	要立即编辑你的 IP 安全策略,请选中"编辑属性"复选框,然后 单击"完成"。	
	☑ 編辑属性(P)	
	若要关闭此向导 , 请单击"完成"。	
	< 上一步(<u>B</u>) 完成 取消	

去掉"使用添加向导"的勾选后,点击"添加"



在新弹出的窗口,选择"IP筛选列表"选项卡,点击"添加"



在新弹出的窗口中填写名称,去掉"使用添加向导"前面的勾,单击"添加"

💵 IP 筛选器列表



>

在新弹出的窗口中,"协议"选项卡下,选择协议和设置到达端口信息,并点确定。

IP 筛选器 属性		\times
地址 协议 描述		
选择协议类型(P):		
ТСР 🗸		
6		
设置 IP 协议端口:		
●从任意端口(上)		
○从此端口(图):		
○ 到任意端口(1)		
◉ 到此端口(<u>O</u>):		
135		
	确定	取消

重复第 7 个步骤 , 添加 TCP 端口 135、139、445。添加 UDP 端口 137、138。添加全部完成后 , 确定。

选中刚添加完成的"端口过滤"规则,然后选择"筛选器操作"选项卡。

新规则 属性	Х
IP 筛选器列表 筛选器操作 身份验证方法 隧道设置 连接类型	
■ 所选的 IP 筛选器列表指定了哪个网络流量将受此规则影响。	
IP 筛选器列表(L):	
名称 描述	
添加(D) 编辑(E) 删除(R)	
关闭 取消 应用(A)

去掉"使用添加向导"勾选,单击"添加"按钮



6. 选择"阻止"

新筛选器操作 属性	×
安全方法常规	
○许可(<u>M</u>) ● 阻止(<u>L</u>)	
○协商安全(N):	
安全方法首选顺序(5):	
类型 AH 完整性 ESP 机密性 ESP 完整性	添加(<u>D</u>)
	编辑(<u>E</u>)
	删除(<u>R</u>)
	上移(U)
< >	下移(<u>O</u>)
接受不安全的通讯,但始终用 IPsec 响应(C)	
□ 如果无法建立安全连接,则允许回退到不安全的通信(W)	
使用会话密钥完全向前保密(PFS)(K)	
确定取消	应用(<u>A</u>)

- 洗择"常规"选项卡,给这个筛选器起名"阻止",然后"确定"。
 点击
- 确认 "IP 筛选列表"选项卡下的"端口过滤"被选中。确认"筛选器操作"选项 卡下的"阻止"被选中。然后点击"关闭"。

新规则 属性		×
IP 筛选器列表	筛选器操作 身份验证方法 隧道设置 连接类型	
X	选择的筛选器操作指定了此规则是否协商及如何来保证网络流量 的安全。	
筛选器操作(<u>F</u>):	-
名称	描述	
◎阻止		
添加(<u>D</u>)	编辑(E) 删除(R) □ 使用"添加向导"(W)	
	关闭 取消 应用(A)	

9. 确认安全规则配置正确。点击确定。

封端口 属性			? ×
规则常规			
▲ 和其他计	算机通讯的安全规则		
IP 安全规则([);			
IP 節這器列表	筛选 <mark>器</mark> 操作	身份验证方法	隧道终结点
☑ 端口过滤	阻止	<无>	无
□ <动态>	默认响应(仅限于	Kerberos	<无>
<			>
运加(D)	编辑(F) 删除	¢(R) □ /= E	"沃加向尽"(\\\)
10×04(U)····	ACOL (L)		
		确定	取消

10. 在"组策略编辑器"上,右键"分配",将规则启用。

🗐 本地组策略编辑器							_	×
文件(F) 操作(A) 查看(V) 帮助(H)								
🗢 🔿 🖄 📷 🗶 🗟 😖 👔 👘 🎽 💆 🧕								
🗐 本地计算机 策略	^	名称		^	描述			策略已排
▼ 👰 计算机配置		1	端口					否
> 🧾 软件设置		17		分配(A)		1		
✔ 🛗 Windows 设置								
> 🧾 域名解析策略				所有任务(K)	>			
😅 脚本(启动/关机)				删除(D)				
> 💼 已部署的打印机				重命名(M)				
▶ 🚡 安全设置				屋(井/市)				
				馮任(K)				
				帮助(H)				
> 📄 高级安全 Windows 防火増		l '	_			,		
🕲 IP 安全策略,在 本地计算机								
> ₩ 基于策略的 QoS								
>	4	<		1				>

4. 安装漏洞补丁

微软针对本次事件,对支持的操作系统在安全公告 MS17-010 中已发布相应补丁修复,对于部分已停服的 Win XP、2003 也已紧急发布补丁 KB4012598 修复。请在所有服务器及终端安装依据操作系统类型不同对应安装相应的补丁。下载来源: MS17-010 Security Update:

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

KB4012598

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598 or 360 云盘:

https://yunpan.cn/cXLwmvHrMF3WI 访问密码 614d

根据不用的操作系统版本,手动安装以上补丁后,可直接修复此次"永恒之蓝"攻 击的所利用的系统漏洞。

另外也可更新天擎控制中心补丁库升级到 1.0.1.2825 及以上版本,并安装其中包含 的所有高危漏洞。

打补丁可能会对用户的现有业务系统、办公软件等造成影响,在生产服务器上安装前,需做好兼容性测试,避免影响业务。

五、周一开机及上线保障指南

打补丁是最终解决方案,免疫工具、关闭端口、停止服务是临时保证主机不感染的临时 措施,只需做到一个即可达到效果。所以开机与上线的检查标准分2个等级:

● 补丁已安装

● 补丁未安装,临时措施已奏效

二者满足任意一条,该主机自身都不会感染,同时也不会感染其它主机,具备开机、上线的条件。只满足第二条的主机,需要后续跟进,直至完成补丁安装。

1. 补丁已安装检查方法:

从 Windows 控制面板中,检查已安装的补丁,确认相应补丁已安装

2. 临时措施生效检查方法:

满足以下任一条件即为合格:

A. 任务管理器检查免疫工具是否运行,可见 onionwormimmune.exe 进程。

■ Windows 任务管理器		
文件(g) 选项(g) 查看(y) 关机	(U) 帮助(H)	
应用程序进程性能联网	用户	
映像名称	用户名	CPU 🔼
taskmgr.exe 73095b7a1a52aa072de7db2d OnionWormImmune.exe ctfmon.exe	zzp SYSTEM zzp zzp	00 00 00 00
vmtoolsd.exe explorer.exe	zzp zzp	00
alg.exe spoolsv.exe	LOCAL SERVICE SYSTEM	00
svchost. exe svchost. exe	LOCAL SERVICE NETWORK SERVICE	00
svchost.exe wuauclt.exe	ZISTEM ZIP	
svchost. exe	SYSTEM	00
vmactnip.exe lsass.exe Services.exe	SISIEM SYSTEM System	
	SISIL	>
□显示所有用户的进程 (2)	结	束进程 (2)
进程数: 23 CPV 使用: 2%	提交更改: 133M	/ 1246M

B. 用同网段电脑运行以下命令,结果为"连接失败"即符合预期。

telnet <主机 IP> 445

第二部分——针对已使用 360 企业安全产品的运维人员

360 企业安全产品可增强企业内网对"永恒之蓝"的防御能力,提高 IT 安全运维的效率。天擎、天堤、天眼、虚拟化安全四类产品,均有针对性的操作建议。请参考以下各产品线的操作文档。

360企业安全产品应对永恒之蓝手册.rar

第三部分——未安装天擎的互联网主机应急处置操作指南

采用快速处置方式,建议使用 360 安全卫士的"NSA 武器库免疫工具",可一键检测修复漏洞、关闭高风险服务,包括精准检测出 NSA 武器库使用的漏洞是否已经修复,并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彻底"免疫"。

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

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

(1) 经检测,发现您的电脑存在该漏洞,请立即修复!

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



通过360安全卫士安装补丁