

针对"永恒之蓝"攻击紧急处置手册

(蠕虫 WannaCry)



2017年05月13日



第1章 隔离网主机应急处置操作指南......3

3		主	先
4	免 具		— :
4	丁升	主	_:
5	5 关务	关 445	三:
6	ACL 445	主	:

第2章 核心网络设备应急处置操作指南......19

JUNIPER	(例):	19
华三(H3C)	(例):	20
华为	(例):	21
Cisco	(例):	21
	(例):	22

第3章 互联网主机应急处置操作指南......22



作 南 第1章 主

先 主

0

下 会 付 : 💕 Tana DecryptOr 2.0 × Ocops, your files have been encrypted. # Chinese (singl) -. 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。 这和一般文件揭述有太宽上的区别。你大可在网上找找恢复文件的方法,获至 保证,没有我们的解答服务,就算老天节来了也不能恢复这些文粒。 **fillberaised or** 17 02:26:59 自然在回教包的方法。只能到她就是们的想念那么去能带着,并以从希望供,依 Time Left 發展供安全有效的恢复服务。 DOS DES 1 但这墨收费的,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 騙你的。 招輪时都可以固定金額付款,就会恢复的時,当然不是,推把付款时间越长 5/20/2017 02:26:59 你不利。 好3天之内付款费用,过了三天费用就会翻倍。 【没有、一个无容之内未有效,将会未送供复不了。 **Time Left** 财了,忘了告诉你,对半年以上没钱付救的穷人,会有活动免费恢复,能否轮 구 Send(\$300 worth of bitcoin to this address bitcein E 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 Сору Us Contact **Check Payment** Decrypt

主		:				
则	主	()。	主	份,则	动 份
o						
主		:				
则		,	以 免主	o	É	<u> </u>
二 于		,但	;其他	于	制 ,其	长中 一
	0					
从		上,360	先		制,再	



─: 免 具

免 具下 : http://dl.b.360.cn/tools/OnionWormImmune.exe



击 OnionWormImmune.exe 具, 任务 中

0



具包 关 MS17-010 丁, winxp_sp3 win10、win2003 win2016 全 列 丁。 下 :

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



下 : https://yunpan.cn/cXLwmvHrMF3WI 614d 三: 关 445 关务 击 单, , cmd, 0 入 令 netstat –an C:\WINDOWS\system32\cmd.exe - 🗆 🗙 Microsoft Windows XP [版本 5.1.2600] <C> 版权所有 1985-2001 Microsoft Corp. ٠ C:\Documents and Settings\admin>netstat -an Active Connections Proto Local Address Foreign Address State TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 0.0.0.0:445 0.0.0.0:0 TCP LISTENING 127.0.0.1:1029 0.0.0.0:0 TCP LISTENING TCP 192.168.232.137:139 0.0.0.0:0 LISTENING 0.0.0.0:445 UDP *:* UDP 0.0.0.0:500 *:* 0.0.0.0:1025 *:* UDP UDP 0.0.0.0:4500 *:* 127.0.0.1:123 UDP *:* 127.0.0.1:1900 192.168.232.137:123 UDP *:* UDP *:* 192.168.232.137:137 UDP *:* UDP 192.168.232.137:138 *:* 192.168.232.137:1900 UDP *:* C:\Documents and Settings\admin>net stop rdr Workstation 服务正在停止. -

 λ net stop rdr

net stop srv

net stop netbt





再 入 netsta –an, 功关 445 。



: 主 ACL 445

IP 全 制 Windows 共享协 关



















🔳 IP 筛选器列表







 7个
 , 加TCP
 135、139、445。
 加 UDP
 137、138。

 加全
 , 。
 。

中刚加""则,"作"卡。



新规则 属性 X
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)
云"使 加 "勾 ,单击" 加"







ń筛选 器 操作	乍属性				×
安全方法	常规				_
○ <u>许可(N</u>	1				
)				
安全方法	;重(Ⅳ); 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(<u>O</u>)	
接受不	安全的通讯,但	始终用 IPsec 响应(<u>C</u>)		
如果尤	;法建立安全连接	,则允许回退到不到	安全的通信(<u>W</u>)		
使用会	话密钥完全向前	保密(PFS)(<u>K</u>)			
		确定	取消	应用(<u>A</u>)	
"	" 卡,	个	""		"
击	1 /	I		,	0
	亙] "	卡下 "	77	中。"	
卡下	""	,, 中。	击"关"。	· -	
		•			



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	
送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(E):	-
名称	
◎阻止	
添加(<u>D</u>) 编辑(E) 删除(B) □使用"添加向导"(<u>W</u>)	
关闭 取消 应用(A)	

4. 全则。击。



封端口 属性			? >	<
规则常规				
	计算机通讯的安全规则			
IP 安全规则(I);				
IP 節這器列表	筛选器操作	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>	
1				
`			/	
添加(D)	编辑(<u>E</u>) 册	■除(<u>R</u>) □使用]"添加向导"(<u>W</u>)	
		确定	取消	_
		W U/AL		







第2章

作 南

	于	众,为	为了 免	L	え	,	传,	利
ACL		,以	临	a				
	主 利	Ј ТСР	445		传	, 于	企事	业单位
。为了		传,				\equiv	位,	ACL
则从	TCF	P 445		0				
以下内	于	为		,	举例	何	ACL	则,以
TCP 445	传	,仅供		0		作中,	协	人
\int	务人	,					上	o

Juniper	(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

全 则

set forwarding-options family inet filter output deny-wannacry set forwarding-options family inet filter input deny-wannacry

# 三	则		
set interfaces [Ξ] unit 0 family inet filter output
deny-wannacry			
set interfaces [<u> </u>] unit 0 family inet filter input
deny-wannacry			



华三(H3C)

(例):

]

: acl number 3050

rule deny tcp destination-port 445

rule permit ip

interface [Ξ packet-filter 3050 inbound packet-filter 3050 outbound

: 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

全

qos apply policy deny-wannacry global inbound qos apply policy deny-wannacry global outbound

三 则



interface [\equiv] qos apply policy deny-wannacry inbound qos apply policy deny-wannacry outbound

华为 (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 [三]

traffic-policy deny-wannacry inbound

traffic-policy deny-wannacry outbound

Cisco

:

(例):

ip access-list extended deny-wannacry deny tcp any any eq 445 permit ip any any



interface [Ξ]
ip access-group deny-wannacry in
ip access-group deny-wannacry out

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

interface [Ξ]ip access-group deny-wannacry inip access-group deny-wannacry out

(例):

ip access-list extended deny-wannacry deny tcp any any eq 445 permit ip any any

interface [Ξ]
ip access-group deny-wannacry in
ip access-group deny-wannacry out

第3章 互 作 主 南 使 360 全卫 免 具", "NSA , 修 、关 务,包 准 出 NSA 使

22 共 23



修	,			丁。	XP、2003	1
,	具	助	关	危	务,从	NSA
击		"免	" 。			

NSA 免 具下 : 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
- 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!

- EtemalBlue (永恒之蓝)
- EternalChampion (永恒王者)
- · EtemalRomance (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)

立即修复

通过360安全卫士安装补丁