应对新型电脑勒索软件的临时解决方案

安天安全研究与应急处理中心

- 1. 开启系统防火墙
- 2. 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)
- 3. 打开系统自动更新,并检测更新进行安装

Win7、Win8、Win10的处理流程

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



选择启动防火墙,并点击确定

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)				

©**‴**安天 确定 取消 点击高级设置 💣 Windows 防火墙 ← → ~ ↑ 🔐 > 控制面板 > 系统和安全 > Windows 防火増 使用 Windows 防火墙来帮助保护你的电脑 控制面板主页 Windows 防火墙有助于防止黑客或恶意软件通过 Internet 或网络访问你的电影 允许应用或功能通过 Windows 防火墙 ✓ 专用网络(<u>R</u>) 💡 更改通知设置 ▼ 来宾或公用网络(P) 🎈 启用或关闭 Windows 防火墙 💡 还原默认值 公共场所(例如机场或咖啡店)中的网络 💡 高级设置 Windows 防火墙状态: 启用 对网络进行疑难解答 传入连接: 阻止所有与未在允许应用 活动的公用网络: ₩ 网络 ◎‴安天 Windows 防火墙阻止新 通知状态:

点击入站规则,新建规则

💣 高级安全 Windows 防火増					↔
文件(F) 操作(A) 查看(V) 帮助	力(<u>H</u>)				
🗢 🄿 🖄 🖬 🖬 🔒 🛛 🖬					
🔐 本地计算机 上的高级安全 Wind	入站规则				操作
🗱 入站规则	名称	组	^	配置文件 ^	入站规则
III 出站规则	🔮 aapt			公用	🗽 新建规则
11 注法女王规则	🕑 aapt			所有	▼ 按配置文件筛选
	🔮 aapt			公用	▼ 按状态筛选
	🔮 aapt			公用	▼ 按组筛选
	V aapt			所有	
	🖉 aapt		◎煮安天	公用	Q 刷新
	v aapt				

选择端口、下一步

💣 新建入站规则向导	>	<
規则类型		
选择要创建的防火墙规则类型		
步 骤 :		
● 规则类型	要创建的规则类型	
● 协议和端口		
● 操作	召 房 (2) 控制程序连接的规则。	
● 配置文件	● 港口 (0)	
● 名称	○ 编口 Q/ 控制 TCP 或 UDP 端口连接的规则。	
	○ 預定义(2):	
	"播放到设备"功能	
	控制 Windows 体验功能连接的规则。	
	目定入规则。	
	© <i>≦</i> 安天	
	< 上一步(B) 下一步(D) > 取消	
	 新建入站规则向导 規则类型 提择要创建的防火墙规则类型 サ家 规则类型 か议和端口 操作 最低 か议和端口 # かび和端口 # 们	 新建入结规则向导 大规则类型 大規则类型 大規 な な 大 な な な な な な な な

特定本地端口,输入445,下一步

	新建入站规则向导 协议和端口 □		×
16	指定应用此规则的协议和端口。 告释 :		
	● 规则类型	此规则应用于 TCP 还是 WDP?	
ŋ	 ● 协议和端口 ● 操作 	O UDP	
と読	● 配置文件● 名称	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):	
(%			
		© <i>穒</i> 安天	
		〈上一步(图) 下一步(图) 〉 取消	

选择阻止连接,下一步

💣 新建入站规则向导		×
	11777777777777777777777777777777777777	
指定在连接与规则中指定的余1	午相心 留 的要执,行的操作。	
步骤 :	"无论"""个人"的"一名"是"正正"""""""""""""""""""""""""""""""""""""	
● 规则类型	注接付言指定宋叶可应该进行1747探1F1	
■ ● 协议和端口		
● 操作	包括使用 Irsec 保护的连接,以及木使用 Irsec 保护的连接。	
● 配置文件	○ 只允许安全连接(C) □ 回复任使田 TPree。进行身份验证的连接。连接的安全性烙依据 TPree。属性由的设	
- 名称	置以及"连接安全规则"节点中的规则受到保障。	n
A2	自定义	0
	◎ 阻止连接(K)	
備		1
1		ŝ
<		
	© <i>≦</i> ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;	
iu		
	〈上一步(B) 下一步(M) 〉 取消	

配置文件,全选,下一步

🛚 🔗 新建入站规则向导	· · · · · · · · · · · · · · · · · · ·	×
配置文件 指定此规则应用的配置文件		
步骤:		ł
● 规则类型	何时应用该规则?	N
 事 ● 协议和端口 ● 操作 		N
● 配置文件	□ 古山市(日)	B
▲ 名称	计算机连接到专用网络位置(例如,家或工作单位)时应用。	/i
	☑ 20日(0) 计算机连接到公用网络位置时应用。	4
		1
鲎		1
		5
2	© <i>煮</i> 安天	
	< 上一步(B) 下一步(M) > 取省	

名称,可以任意输入,完成即可。

100	🔗 新建入站规则向导		×
Ű,	名称		
	指定此规则的名称和描述。		
2	步 骤 :		
-	● 规则类型		
3)	● 协议和端口		
	● 操作	◆投(町)・	
1	● 配置文件	smb	В
2	● 名称	描述(可选)(<u>D</u>):	ri
ιų,			0
			4
復			J
			5
(
in			
		< 上一步(B) 完成(F) 取消	
ii I			

XP 系统的处理流程

依次打开控制面板,安全中心,Windows防火墙,选择启用



点击开始,运行,输入 cmd,确定执行下面三条命令

net stop rdr net stop srv net stop netbt

由于微软已经不再为 XP 系统提供系统更新,建议用户尽快升级到高版本系统。

版权所有:安天安全研究与应急处理中心