安天蠕虫式勒索软件WannaCry免疫工具使用说明

# 一 概述

本工具为安天CERT响应WannaCry勒索蠕虫病毒紧急发布的防护工具，提供禁用系统服务、设置ipsec本地组策略等功能，能阻断通过SMB漏洞MS17-010向本机传播WannaCry勒索软件，但不能阻断WannaCry在本机上的运行。

提示1：建议将该工具刻录至光盘后在电脑中运行，避免重复感染。

提示2：本工具不能直接阻断WannaCry在本地运行！请及时更新补丁并安装防护软件保证系统安全！

工具会阻断部分端口的连接，请在使用前确认是否会影响其他应用。

# 二 功能介绍

## 2.2设置组策略免疫

### 2.2.1常规型组策略设置

* 功能介绍  
  该策略适用于Windows Vista及之后系统，仅阻止445端口的连接，推荐Windows Vista及之后系统的用户优先使用。
* 使用说明  
  点击“设置免疫”，工具会自动关闭445端口，重启后设置生效。  
  点击“取消设置”，会重新开启445端口。

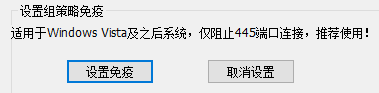


图2-1常规型策略界面

### 2.2.2增强型组策略设置

* 功能介绍  
  该策略为增强型策略，可以关闭135/137/138/139/445端口。
* 使用说明  
  点击“设置增强免疫”，工具会自动关闭135/137/138/139/445端口，重启后设置生效。  
  点击“取消设置”，会重新开启135/137/138/139/445端口。

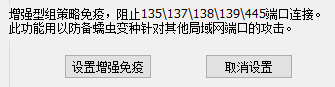


图2-2 增强型组策略免疫界面

### 2.2.3禁用服务免疫

* 功能介绍  
  适用于Windows XP系统，设置后会关闭部分系统服务，有可能影响其他系统功能。
* 使用说明  
  点击“设置免疫”，工具会自动关闭部分系统服务，重启后设置生效。  
  点击“取消设置”，会重新开启部分服务。

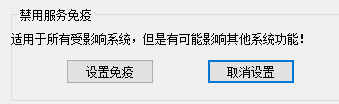


图2-3 禁用服务免疫功能截图

### 2.2.4官方补丁下载

* 功能介绍  
  可以链接到微软官网下载漏洞补丁。
* 使用说明  
  点击“官方补丁下载”，将会启动浏览器并访问微软官方网站，用户可通过网站下载适配的补丁程序。  
  注：漏洞补丁由微软官方提供，与工具无关。