Petya免疫工具说明文档(必读)

# 工具介绍





Petya免疫工具是针对互联网上出现Windows操作系统的勒索病毒的免疫修复的工具。此勒索病毒利用此前披露的Windows SMB服务漏洞（[微软](http://stock.finance.sina.com.cn/usstock/quotes/MSFT.html)漏洞公告：MS17-010）和（CVE-2017-0199）RTF漏洞攻击手段，修改系统的MBR引导扇区，当电脑重启时，病毒代码会在Windows操作系统之前接管电脑，执行加密等恶意操作。

# 功能说明

* **特性一：疫苗免疫：**

通过已经捕获到的病毒文件，对病毒感染原理进行分析，了解病毒会先判断机器是否已经感染过，如果已经感染过就不进行后续流程。因此增加已经感染过的疫苗处理，加强系统对已知病毒的免疫能力。

* **特性二：操作系统关键补丁包检测**

针对Windows SMB服务漏洞（微软漏洞公告：MS17-010）的关键补丁深度检测

* **特性三：（仅针对个人PC）一键暂停微软网络共享服务**

增加系统防火墙规则

关闭TCP/UDP端口135、139、445（SMB服务相关端口）

特性三 可能带来影响说明！

1、自动启用关闭状态的PC防火墙，默认产生应用拒绝策略，可能导致本可使用的个人PC应用无法使用

2、同时自动关闭上述端口操作，在规避隐患同时会导致系统某些服务停止，例如：打印机、共享文件夹等应用。

以上请确认影响后选择操作，可在完成补丁安装后一键恢复原有端口使用状态

技术问题拨打深信服安全应急热线400-630-6430转6 寻求支持

# 支持系统

**个人PC系统：**

Windows XP （X86 / AMD64，支持特性一、特性二、特性三）

Windows 7 （X86 / AMD64，支持特性一、特性二、特性三）

Windows 8 （X86 / AMD64，支持特性一、特性二、特性三）

Windows 8.1 （X86 / AMD64，支持特性一、特性二、特性三）

Windows 10 （X86 / AMD64，支持特性一、特性二）

**服务器系统：**

Windows Server 2003 （X86 / AMD64，支持特性一、特性二）

Windows Server 2008 （X86 / AMD64，支持特性一、特性二）

Windows Server 2008 R2 （AMD64，支持特性一、特性二）

Windows Server 2012 （AMD64，支持特性一、特性二）

Windows Server 2016 （AMD64，支持特性一、特性二）