



# 勒索软件的防范、处置方案培训

——积极应对勒索软件“WannaCry”的威胁

西南大学信息中心

2017年5月15日

# 目录

## CONTENTS

- 0 有备无患 做好备份工作
- 1 开启本机防火墙 阻断高危端口
- 2 关闭网络共享等服务
- 3 给操作系统打补丁
- 4 建立、完善应急处置预案

WannaCry

PART  
PART  
ONE

做好数据备份，  
否则一切=零

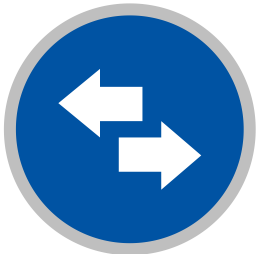


# 有备无患：做好重要数据、文件、系统的备份



## 1. 重要数据备份

条件允许的话，先断网再备份数据。



## 2. 重要文件备份

条件允许的话，可以用全新的、无病毒的U盘、移动硬盘进行备份。



## 3. 重要系统备份

建议做好重要系统的系统级备份，中毒后可启用新系统，减少对业务的影响。

## 一、开启本机防火墙 阻断高危端口

### 开启电脑、服务器的防火墙（系统自带）

1) 打开“控制面板-系统与安全-Windows防火墙”，点击左侧启动Windows防火墙。

### 把445、135、137-139统统阻断掉

2) 高级设置 -----> 进站规则-----> 新建规则  
--> 选择端口 -----> 特定本地端口，输入“445，135，137-139”  
--> 选择'阻止连接'--> 下一步--> .... 。

# 一、开启本机防火墙 阻断高危端口

## 开启电脑防火墙

1) 打开“控制面板-系统与安全-Windows防火墙”，点击左侧启动Windows防火墙。



# 一、开启本机防火墙 阻断高危端口

## 开启电脑防火墙

2) 点击“启用Windows防火墙”。

### 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)

确定

取消

# 一、开启本机防火墙 阻断高危端口

445、135、137-139统统阻断掉

3) 点击 “高级设置-进站规则-新建规则”。





# 一、开启本机防火墙 阻断高危端口

## 445、135、137-139统统阻断掉

4) 点击“选择端口 - 特定本地端口”，输入“445, 135, 137-139”。



# 一、开启本机防火墙 阻断高危端口

## 445、135、137-139统统阻断掉

4) 点击“选择端口 - 特定本地端口，输入“445, 135, 137-139”。

### 一、开启本机防火墙 阻断高危端口

#### 445、135、137-139统统阻断掉

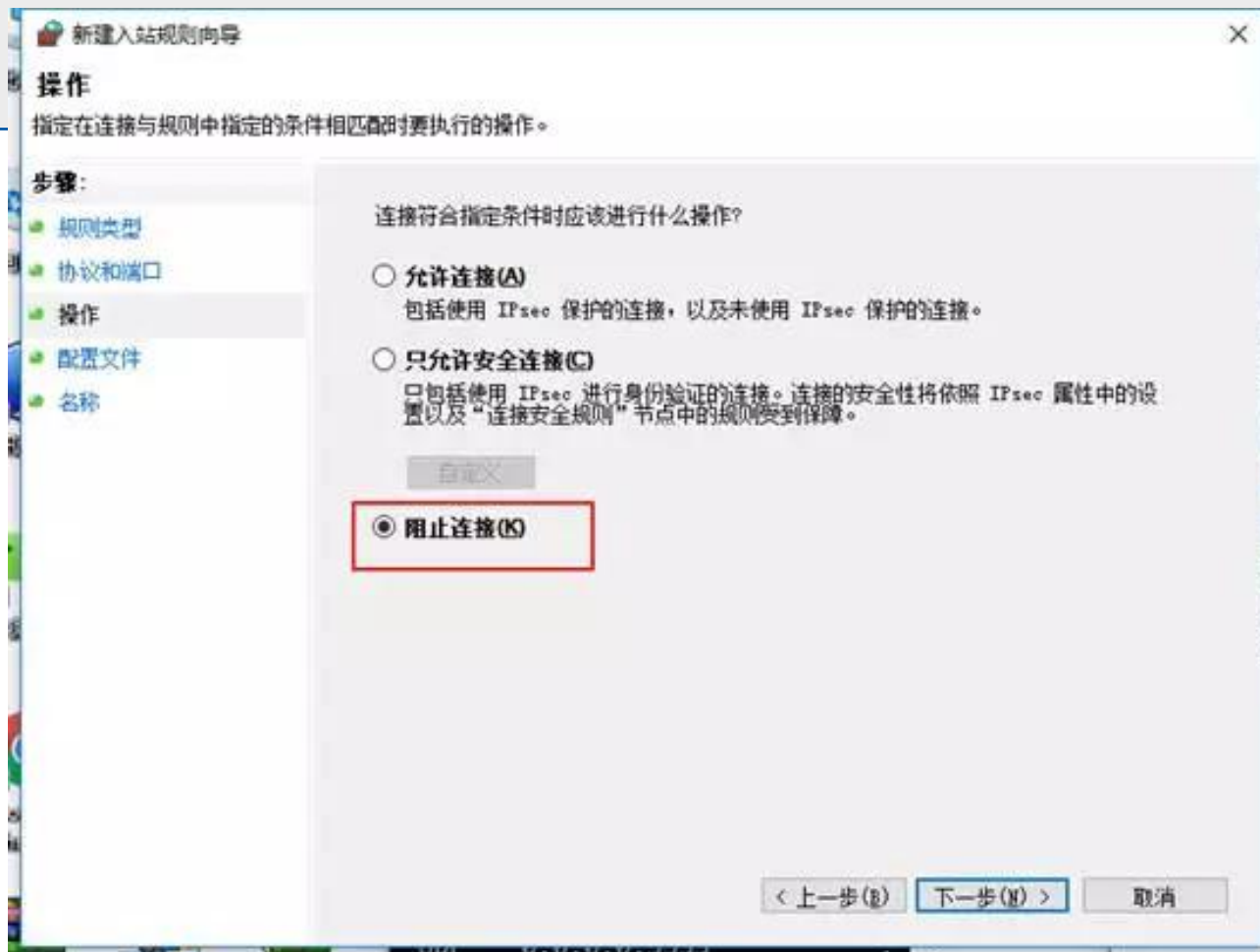
4) 点击“选择端口 - 特定本地端口，输入“445, 135, 137-139”。



# 一、开启本机防火墙 阻断高危端口

445、135、137-139统统阻断掉

5) 选择“阻止连接”--下一步....。



## 二、关闭网络共享等服务

### 关闭网络共享等服务

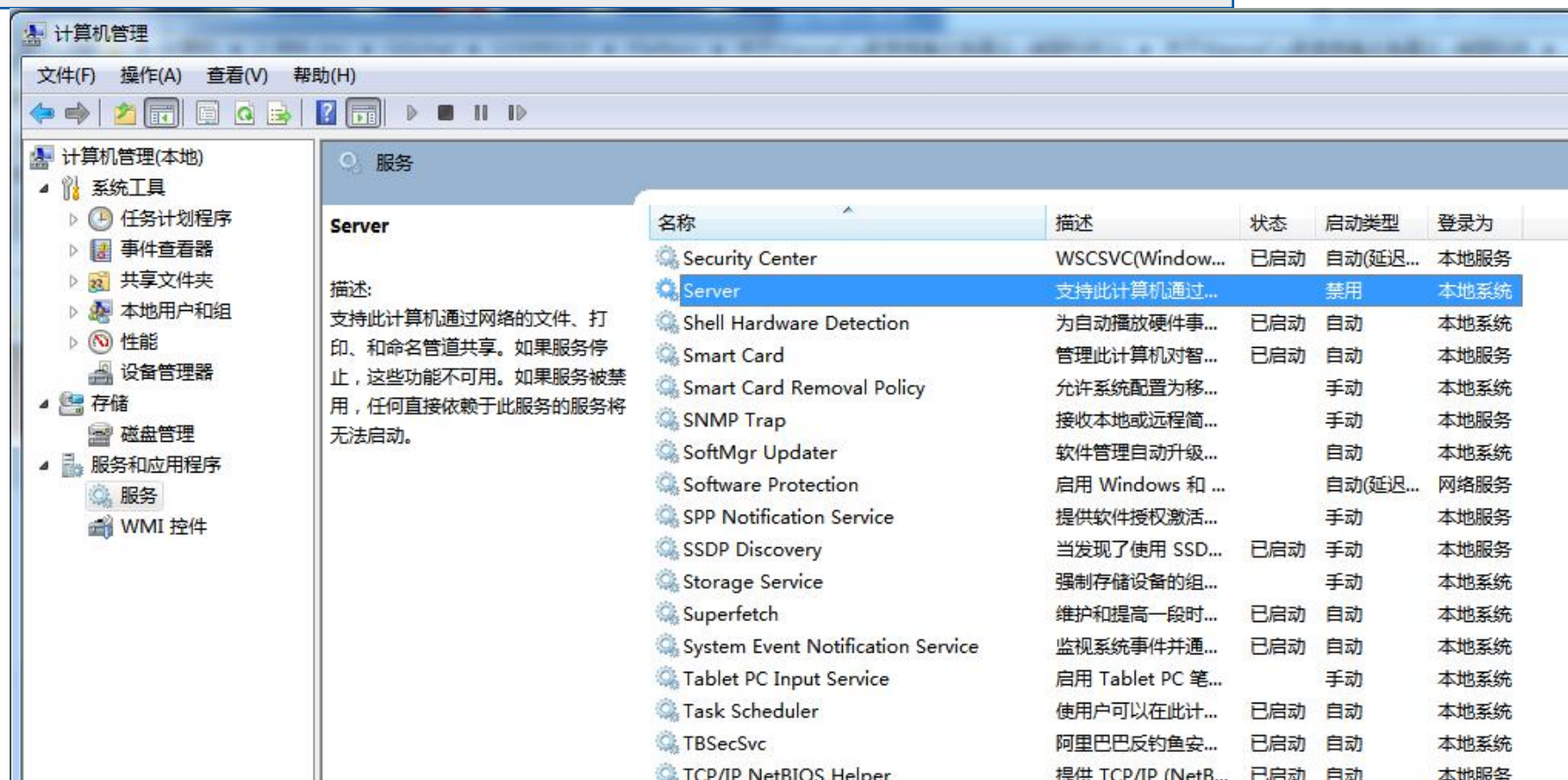
1) 右击“我的电脑”点击“管理”  
(或者如图所示的点击开始右击右栏的“计算机”)



## 二、关闭网络共享等服务

### 关闭网络共享等服务

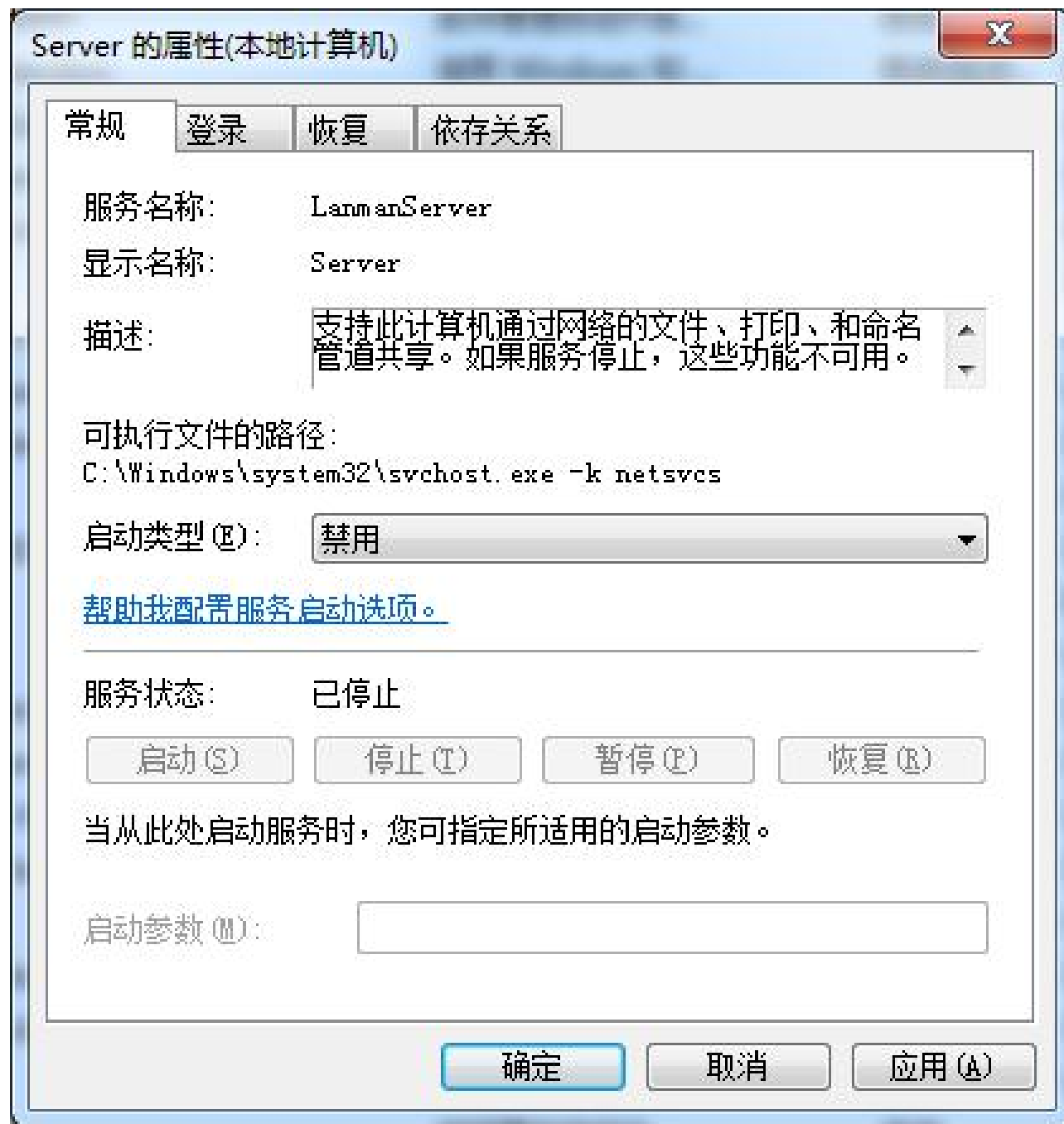
2) 点开左边菜单“服务与进程”下的“服务”。



## 二、关闭网络共享等服务

### 关闭网络共享等服务

3)在“Server”这个服务上面点右键，在“启动类型”中选择“禁用”，点“确定”。



## 二、关闭网络共享等服务

### 关闭网络共享等服务

现在各大安全公司已经推出了一些工具：

- 1、 一键检测漏洞，关闭445端口等功能。
- 2、 更多工具稍后在网络安全工作群中公布和更新。

备注：1、 工具只做辅助手段，多种方法交叉验证确保安全。

2、 关闭网络共享服务后，会影响网络共享打印机等的使用。

## 三、给操作系统打补丁

### 1、MS17-010漏洞补丁可有效阻断本次勒索病毒的攻击

1) <https://technet.microsoft.com/zh-cn/library/security/MS17-010>。

### 2、不止于“永恒之蓝” 其它漏洞也要赶紧修复

- 1) 可使用360安全卫士、腾讯电脑管家等工具下载补丁，速度相对较快。
- 2) 建议最后到微软官网检查、确认补丁已经全部打完。

小提示： 不要使用来历不明的补丁程序。



## 三、给操作系统打补丁

### 3、XP和部分服务器版的特别补丁

1) <https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>。

建议仍在使用windows xp , windows2003操作系统的用户尽快升级到window7/windows10;

windows2003操作系统的用户建议升级到windows 2008/2012/2016。

## 四、建立、完善应急处理预案

### 1、对已经中毒计算机 立即断网并隔离

- 1) 如果发现本单位的某台计算机中毒，  
**立即断网（拔网线、禁用网卡）**，隔离中毒计算机，阻止进一步扩散。
- 2) 通知本单位的所有计算机用户，断网自查。

### 2、同步通知信息中心 向本单位网络安全分管领导报告

- 1) 第一时间通知信息中心（杨彦 68367209 13996022139）。
- 2) 向本单位领导汇报，并立即启动本单位的网络安全事件应急预案，并将处置结果及时向信息中心报告（swuyy@swu.edu.cn）。
- 3) 信息中心接报后采取应急措施，并按规定向相关领导和上级部门汇报。

## 五、一点小建议

### 1、安全使用计算机

1) 不明链接不要点击，不明文件不要下载，不明邮件不要打开。

### 2、不止于“永恒之蓝” 其它漏洞也要赶紧修复

- 1) 360安全卫士、腾讯电脑管家等工具下载补丁的程序较快。
- 2) 建议最后到微软官网检查、确认补丁已经全部打完。

## 六、西南大学网络安全工作联系群

### 1、微信群

- 1)扫描二维码加入
- 2)请实名：单位名称-姓名

### 2、QQ群

- 1)二级单位信息干事QQ群 群号：  
**287894211**



西南大学网安工作群



该二维码7天内(5月22日前)有效, 重新进入将更新

谢谢