1.Shutdownanddisablethecomputernetworkserverservice.OpenCMDwithadministratorprivileges,andrun:

networkstopserver

scconfigureLanmanServerstart=disabled.

其次，打开防火墙，禁用445端口。用管理员权限打开CMD，运行以下脚本(金百安提供):

netsh防火墙设置op模式启用

。

netshadvfirewall防火墙添加规则name=&quot拒绝445&quotdir=in协议=tcp本地端口=445操作=阻止

三、对于微软不再提供补丁的WindowsXP用户，打开CMD运行(记得禁用相关服务):

netstopRDR

netstopSRV

。

netstopnetbt

第四，对于Windows7以上版本的用户，如果有外网，可以直接打补丁：

{URL:http:text:Microsoft安全公告MS17-010-critical}

带外网的懒人解决方案：

使用360NSA武器库免疫工具，下载地址：

。

另外，对于重要的文件，多留几份。

1。Win10防范流程

Win10平台比较简单，因为微软已经在3月初针对这个病毒漏洞发布了相关补丁，所以只要你的Win10已经启动了自动更新，，并已升级至最新版本(版本号高于1511)，可以成功抵御Wannacrypt病毒。

操作步骤：

1。"设置&quot&quot；更新和安全性&quot&quot；Windows更新&quot，并检查该项是否已打开；

2。点击任务栏中的Cortana搜索框，输入&quot温弗&quot并回车确认版本号高于1511；

Win10用户直接升级最新版本

二。Win7、Win8.1、WinXP处理流程

对于非Win10平台的电脑，大部分已经超过服务期限，或者由于各种原因没有打开

更新和接收安全补丁，是此次攻击的重灾区。。解决方法是手动下载ms17-010修补程序。目前微软已经紧急发布了针对不同平台的ms17-010补丁，直接链接地址如下：

WindowsXP(KB4012598)

32位：

。

64位：

Windows7(kb4012212、KB4012215)

32位：

(kb4012212)

(kb4012215)

64位：

(kb4012212)

(kb4012215)

Windows8.1(kb4012213、KB4012216)

32位：

(kb4012213)

(kb4012216)

64位：

(kb4012213)

，请直接去下载相应的补丁文件。

在搜索自己的Windows平台时，要注意版本号(如32位/64位)

再次确认平台版本号，点击对应版本的下载按钮

。

单击链接直接下载该平台的补丁程序。需要注意的是，个别平台(如Win7)会包含两个补丁，请按顺序

III下载安装。临时处置方法

如果电脑不方便安装补丁，，或者手头没有下载的补丁文件，可以考虑以下临时处置方法。临时处置方法是通过关闭系统对应端口号进行免疫，对当前版本病毒有效，但不排除病毒发生变异后被破解的可能。具体方法如下：

1。下载360NSA免疫工具

NSA军火库免疫工具

软件版本：XP版本

软件大小：125.34MB

软件授权：免费。

适用平台：winXPvistawin8win7

下载地址：

立即下载

360公司发布的NSA免疫工具，具有省时省力、操作难度低的特点。。整个工具包是125MB。双击它可以自动解压。稍后，您将进入一个主界面，并按照屏幕提示进行操作。当界面为绿色时，表示系统是安全的！360公司发布的

NSA免疫工具

2。手动关闭Windows端口445、135、137、138和139

除了现有的工具，还可以手动关闭端口号445、135、137、138和139，抵御病毒攻击。。具体操作步骤如下：

2.1关闭135、137、138端口

1。运行输入&quotdcomcnfg&quot；

2。在&quot电脑&quot选项，右键单击&quot我的电脑&quot。，选择&quot属性&quot；

3。在出现的“我的电脑属性”对话框的“默认属性”选项卡中，删除&quot在这台计算机上启用分布式&quot；

4。选择默认协议选项卡。，选择&quot用于连接的TCP/IP&quot；然后单击&quot删除&quot按钮；

5。右键单击网上邻居选择属性，然后右键单击网络选项卡。，去掉微软网络和微软网络客户端上文件和打印机共享的复选框，然后关闭共享端的135、137、138端口；

手动关闭端口

2.2关闭端口139

打开网络和拨号连接本地连接，选择互联网协议(TCP/IP)属性，进入高级TCP/IP设置“WINS设置。，有一个&quot禁用TCP/IP&quot；检查它关闭端口139；

2.3关闭端口445

&quot；开始&quot&quot；运行&quot,输入"注册表编辑"确定后定位到"HKEY_LOCAL_MACHINE\SYSTEM\currentcontrolset\Services\NetBT\Parameters&quot；，创建一个名为&quotSMB设备已启用&quot并将其设置为0，则可以关闭端口445；

注意：手动关闭端口号后，某些intranet服务(如文件和打印机共享)可能会失败。请慎重选择。写在最后的

Wannacrypt是近年来危害最大的病毒之一，仅次于当年的冲击波。最关键的是，这种病毒会影响硬盘数据，目前几乎不可能破解。目前，方法如下Wannacrypt会

在加密前自动删除原文件，你可以尝试使用一些专业的数据恢复软件进行恢复。简而言之，保持系统最新是抵御病毒的最佳方式。

根据网络安全局的通知，这是由犯罪分子利用&quot永恒的蓝色&quot从国家安全局黑客军火库泄露的。"永恒的蓝色&quot将扫描445文件共享端口打开的Windows机器，无需用户任何操作，只要打开互联网。不法分子可以在电脑和服务器中植入勒索软件、远程控制木马、虚拟货币挖矿机等恶意程序。我想提醒电脑用户：1。为计算机安装最新的安全补丁。Microsoft已发布修补程序MS17-010来修复&quot永恒的蓝色&quot进攻。请尽快安装这个安全补丁。，网址为https://TechNet.Microsoft.com/zh-cn/library/security/ms17-010；对于windowsXP、2003等微软不再提供安全更新的机器。，可以使用360“NSA武器库免疫工具&quot检测系统是否存在漏洞，关闭受漏洞影响的端口，避免被勒索软件等病毒攻击。免疫工具下载地址：/NSA/nsatool.exe。。2.关闭端口445、135、137、138和139，并关闭网络共享。3.加强网络安全意识：Don&#039不要点击未知链接，不要&#039；不要下载未知文件。唐&#039；不要打开未知的电子邮件.4.尽快(以后定期)将电脑中的重要文件备份到移动硬盘和u盘上，备份后离线保存磁盘。5.建议还是用windowsxp。，windows2003操作系统的用户应尽快升级到Windows7/Windows10或windows2008/2012/2016操作系统。