# 针对敲诈病毒（WanaCrypt0r2.0）的解决方案

目录

[针对“永恒之蓝”敲诈病毒（WanaCrypt0r2.0）的解决方案 1](#_Toc482484141)

[病毒背景 2](#_Toc482484142)

[病毒感染现象 2](#_Toc482484143)

[针对未中病毒系统解决方案 4](#_Toc482484144)

[针对已中病毒系统解决方案 5](#_Toc482484145)

[安全补丁下载 6](#_Toc482484146)

[打开Windows防火墙 8](#_Toc482484147)

[核心网络设备应急处置操作 15](#_Toc482484148)

## 病毒背景

5月12日起，Onion、WNCRY两类敲诈者病毒变种在全国乃至全世界大范围内出现爆发态势，中国大陆大量教育网用户和企业用户中招。

与以往不同的是，这次的新变种病毒添加了NSA(美国国家安全局)黑客工具包中的“永恒之蓝”0day漏洞利用，通过445端口(文件共享)在内网进行蠕虫式感染传播。

微软在今年3月10日已发布补丁MS17-010修复了“永恒之蓝”攻击的系统漏洞，请尽快安装此安全补丁，网址为https://technet.microsoft.com/zh-cn/library/security/MS17-010。

没有安装安全软件或及时更新系统补丁的其他内网用户极有可能被动感染，所以目前感染用户主要集中在企业、高校等内网环境下。

一旦感染该蠕虫病毒变种，系统重要资料文件就会被加密，并勒索高额的比特币赎金，折合人民币2000-50000元不等。

从目前监控到的情况来看，全网已经有数万用户感染，QQ、微博等社交平台上也是哀鸿遍野，后续威胁也不容小觑。

## 病毒感染现象

中毒系统中的文档、图片、压缩包、影音等常见文件都会被病毒加密，然后向用户勒索高额比特币赎金。

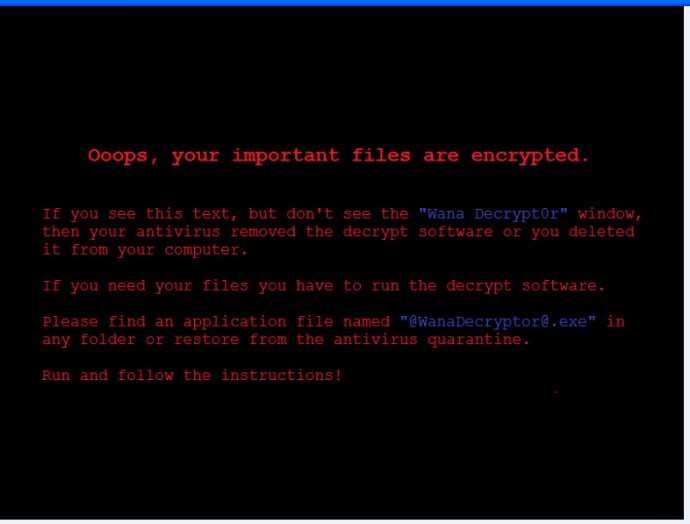
WNCRY变种一般勒索价值300-600美金的比特币，Onion变种甚至要求用户支付3个比特币，以目前的比特币行情，折合人民币在3万左右。

此类病毒一般使用RSA等非对称算法，没有私钥就无法解密文件。WNCRY敲诈者病毒要求用户在3天内付款，否则解密费用翻倍，并且一周内未付款将删除密钥导致无法恢复。

从某种意义上来说，这种敲诈者病毒“可防不可解”，需要安全厂商和用户共同加强安全防御措施和意识。



中毒后的勒索提示

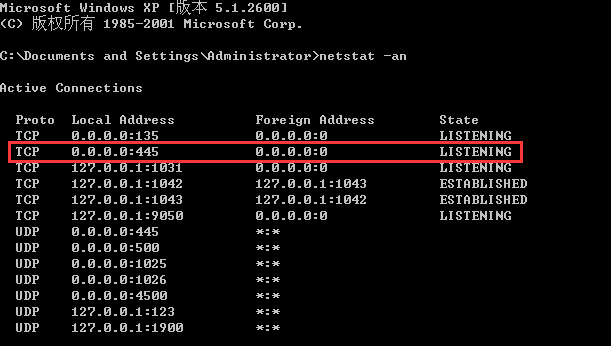


部分系统桌面变化

## 针对未中病毒系统解决方案

1. 为计算机安装最新的安全补丁，微软已发布补丁MS17-010修复了“永恒之蓝”攻击的系统漏洞，请尽快安装此补丁，请参考本文档《安全补丁下载》章节内容进行下载安装。
2. 开启Windows防火墙。请参考《打开Windows 防火墙》章节进行Windows防火墙启用。
3. 针对暂时无法安装补丁的Windows Server 2003以及Windows XP系统，可以通过关闭445端口（监控其他关联端口如： 135、137、139）来避免病毒侵害。
4. 快捷键WIN+R启动运行窗口，输入cmd并执行，打开命令行操作窗口，输入命令：netstat -an

\*用于检测445端口是否开启

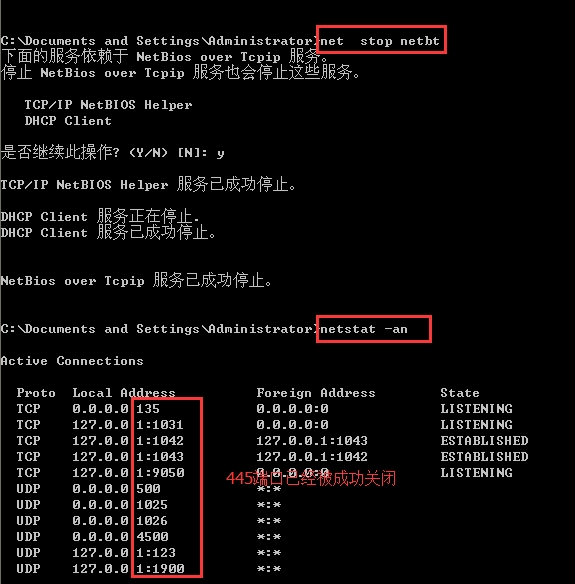


上图为未关闭445端口

1. 如445端口开启（如上图），依次输入以下命令进行关闭：

***net stop rdr  / net stop srv / net stop netbt***

功后的效果如下：



1. 强化网络安全意识：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. 尽快（今后定期）备份自己电脑中的重要文件资料到移动硬盘、U盘，备份完后脱机保存该磁盘。
3. 建议仍在使用Windows XP，Windows Server 2003操作系统的用户尽快升级到 Window 7/Windows 10，或 Windows 2008/2012/2016操作系统。
4. 若是Windows 7、Windows 8/8.1、Windows 10（不包含LTSB）以上操作系统在启用自动更新情况下对此病毒免疫。
5. 安装正版操作系统、Office软件等。

## 针对已中病毒系统解决方案

在没有解密密钥情况下，中病毒计算机中的文件恢复的成本非常高昂、难度非常大。若确定计算机已经中毒，应将该计算机隔离或断网(拔网线)，以免进行病毒扩散。若存在该计算机备份，则启动备份恢复程序。若没有重要文件，可通过对磁盘全盘进行格式化，重装系统恢复使用。

## 安全补丁下载

针对不同的系统所安装的补丁不同，请严格按照系统版本下载相对应的安全补丁对系统进行更新。

**------------------------------------------------------------------------**

以下系统版本：

Windows XP 32位/64位/嵌入式

Windows Vista 32/64位

Windows Server 2003 SP2 32位/64位

Windows 8 32位/64位

Windows Server 2008 32位/64位/安腾

对应补丁下载地址：

<http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598>

**------------------------------------------------------------------------**

以下系统版本：

Windows 7 32位/64位/嵌入式

Windows Server 2008 R2 32位/64位

对应补丁下载地址：

<http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012212>

**------------------------------------------------------------------------**

以下系统版本：

Windows 8.1 32位/64位

Windows Server 2012 R2 32位/64位

对应补丁下载地址：<http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012213>

以下系统版本：

Windows 8嵌入式

Windows Server 2012

对应补丁下载地址：<http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012214>

**------------------------------------------------------------------------**

以下系统版本：

Windows 10 RTM 32位/64位/LTSB

对应补丁下载地址：<http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012606>

**------------------------------------------------------------------------**

以下系统版本：

Windows 10 1511十一月更新版32/64位

对应补丁下载地址：

<http://www.catalog.update.microsoft.com/Search.aspx?q=KB4013198>

**------------------------------------------------------------------------**

以下系统版本：

Windows 10 1607周年更新版32/64位

Windows Server 2016 32/64位

对应补丁下载地址：

<http://www.catalog.update.microsoft.com/Search.aspx?q=KB4013429>

## 打开Windows防火墙

不同系统打开Windows防火墙的步骤不一样，请按照相应系统进行操作。

**------------------------------------------------------------------------**

以下系统：

**Windows XP**

**Windows Server 2003**

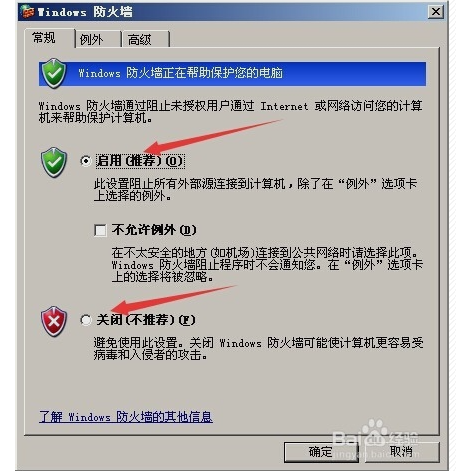
启用Windows防火墙步骤如下：



打开控制面板



在控制面板中找到Windows防火墙



将Windows防火墙由关闭改为启用

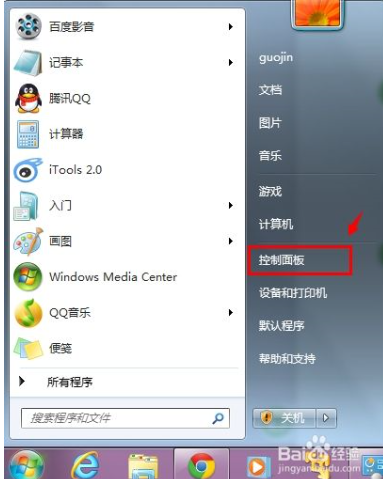
以下系统：

**Windows Vista**

**Windows 7**

**Windows 8/8.1**

启用Windows防火墙步骤如下：



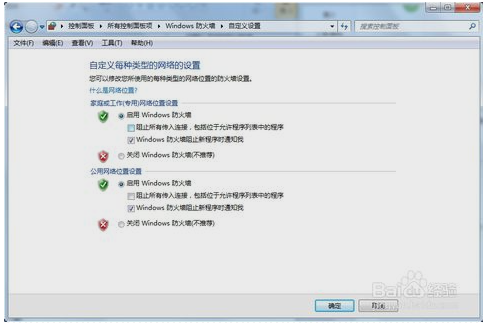
在开始中打开控制面板



在控制面板中找到Windows防火墙



在Windows防火墙控制面板中单击左侧打开或关闭Windows防火墙



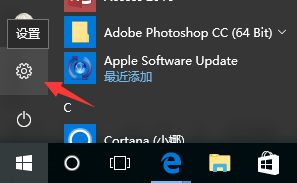
启用Windows防火墙

**------------------------------------------------------------------------**

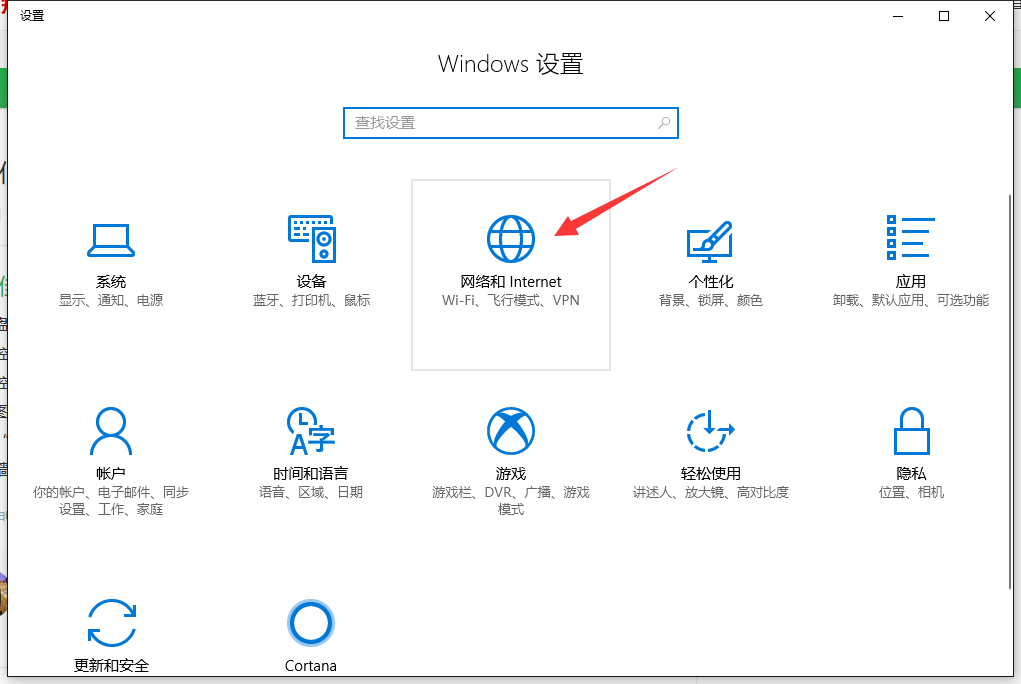
以下系统：

**Windows 10**

启用Windows防火墙步骤如下：



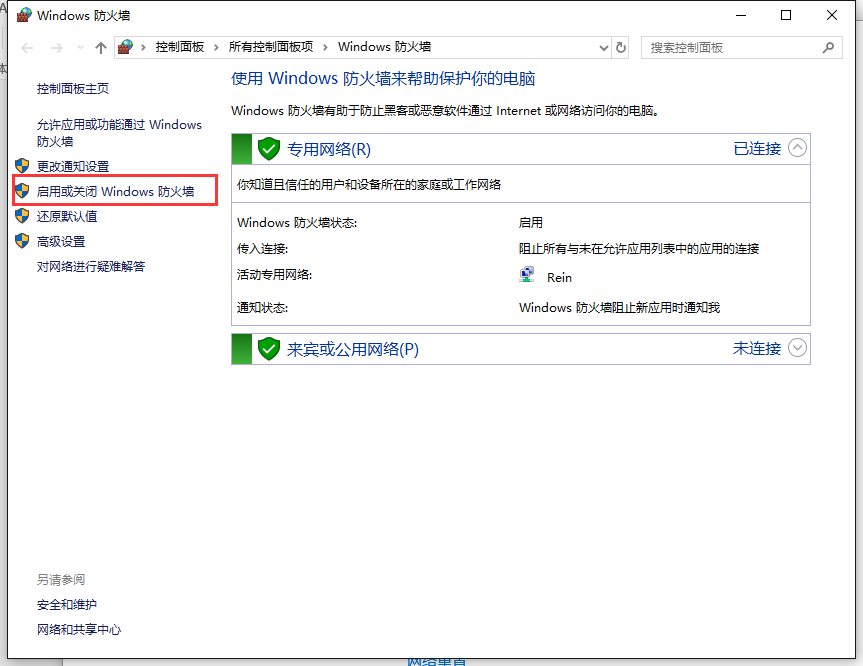
单击开始打开设置



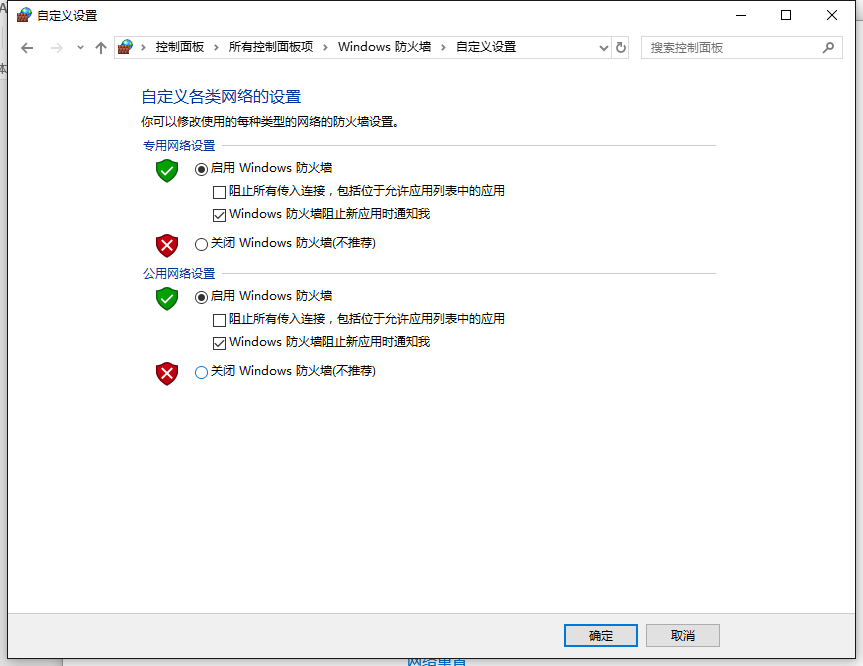
打开设置中的网络和Internet



在状态中找到Windows防火墙



在Windows防火墙控制面板中单击左侧启用或关闭Windows防火墙



启用Windows防火墙

## 核心网络设备应急处置操作

　　大型机构由于设备众多，为了避免感染设备之后的广泛传播，建议利用各网络设备的 ACL 策略配置，以实现临时封堵。

　　该蠕虫病毒主要利用 TCP 的 445 端口进行传播, 对于各大企事业单位影响很大。为了阻断病毒快速传播, 建议在核心网络设备的三层接口位置, 配置 ACL 规则从网络层面阻断 TCP 445 端口的通讯。

　　以下内容是基于较为流行的网络设备，举例说明如何配置 ACL 规则，以禁止TCP 445 网络端口传输，仅供大家参考。在实际操作中，请协调网络管理人员或网络设备厂商服务人员，根据实际网络环境在核心网络设备上进行配置。

**Juniper 设备的建议配置(示例):**

　　set firewall family inet filter deny-wannacry term deny445 from protocol tcp

　　set firewall family inet filter deny-wannacry term deny445 from destination-port 445 set firewall family inet filter deny-wannacry term deny445 then discard

　　set firewall family inet filter deny-wannacry term default then accept

　　#在全局应用规则

　　set forwarding-options family inet filter output deny-wannacry set forwarding-options family inet filter input deny-wannacry

　　#在三层接口应用规则

　　set interfaces [ 需要挂载的三层端口名称 ] unit 0 family inet filter output deny-wannacry

　　set interfaces [ 需要挂载的三层端口名称 ] unit 0 family inet filter input deny-wannacry

**华三(H3C)设备的建议配置(示例):**

　　新版本: acl number 3050

　　rule deny tcp destination-port 445 rule permit ip

　　interface [需要挂载的三层端口名称] packet-filter 3050 inbound packet-filter 3050 outbound

　　旧版本: acl number 3050

　　rule permit tcp destination-port 445

　　traffic classifier deny-wannacry if-match acl 3050

　　traffic behavior deny-wannacry filter deny

　　qos policy deny-wannacry

　　classifier deny-wannacry behavior deny-wannacry

　　#在全局应用

　　qos apply policy deny-wannacry global inbound qos apply policy deny-wannacry global outbound

　　#在三层接口应用规则

　　interface [需要挂载的三层端口名称]

　　qos apply policy deny-wannacry inbound

　　qos apply policy deny-wannacry outbound

**华为设备的建议配置(示例):**

　　acl number 3050

　　rule deny tcp destination-port eq 445 rule permit ip

　　traffic classifier deny-wannacry type and if-match acl 3050

　　traffic behavior deny-wannacry

　　traffic policy deny-wannacry

　　classifier deny-wannacry behavior deny-wannacry precedence 5

　　interface [需要挂载的三层端口名称] traffic-policy deny-wannacry inbound traffic-policy deny-wannacry outbound

**Cisco 设备的建议配置(示例):**

　　旧版本:

　　ip access-list extended deny-wannacry

　　deny tcp any any eq 445

　　permit ip any any

　　interface [需要挂载的三层端口名称] ip access-group deny-wannacry in

　　ip access-group deny-wannacry out

　　新版本:

　　ip access-list deny-wannacry deny tcp any any eq 445 permit ip any any

　　interface [需要挂载的三层端口名称] ip access-group deny-wannacry in

　　ip access-group deny-wannacry out

**锐捷设备的建议配置(示例):**

　　ip access-list extended deny-wannacry deny tcp any any eq 445

　　permit ip any any

　　interface [需要挂载的三层端口名称] ip access-group deny-wannacry in

　　ip access-group deny-wannacry out