关于勒索蠕虫 WannaCry 病毒分析与应对建议

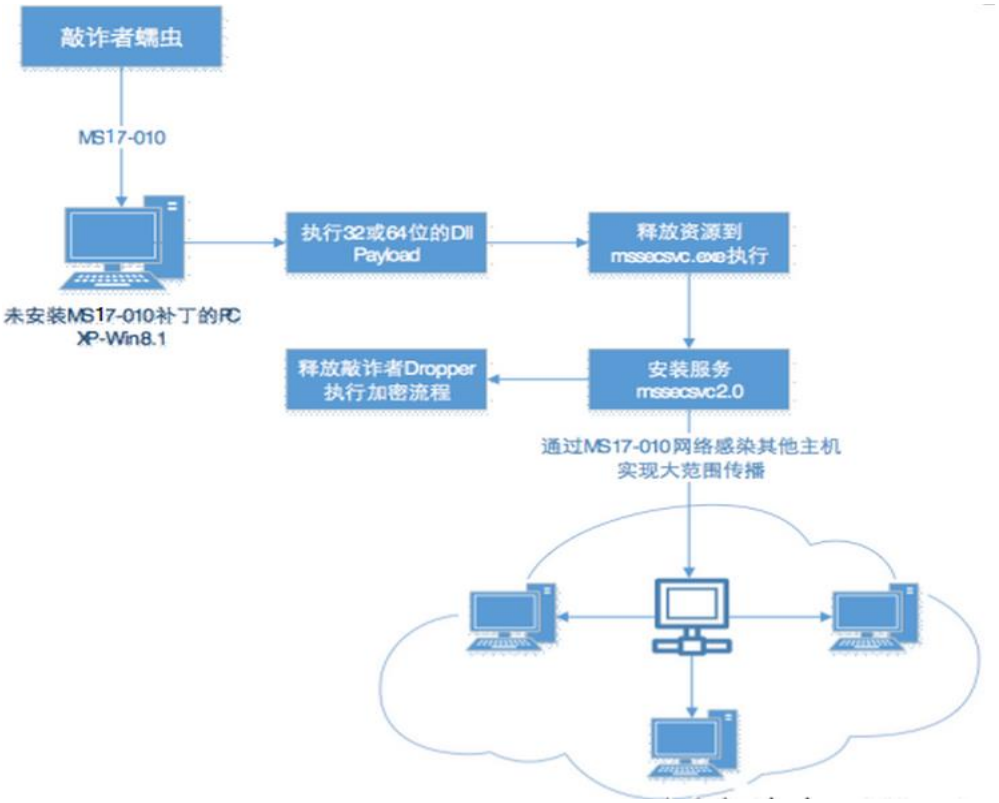
事件综述

北京时间 2017 年 5 月 12 日 20 时左右，全球爆发大规模勒索软件感染事件，此次勒索事件与以往相比最显著特点是勒索病毒结合了蠕虫的方式进行传播，传播方式采用了前不久 NSA 被泄漏出来的 MS17-010 漏洞。在 NSA 泄漏的文件中，WannaCry 传播方式的漏洞利用代码被称为“EternalBlue”，所以有报道称此次攻击为“永恒之蓝”。

该勒索软件已经攻击了 99 个国家近万台电脑。英国、美国、俄罗斯、德国、土耳其、意大利、中国、菲律宾等国家都已中招。且攻击仍在蔓延。据报道，勒索攻击导致 16 家英国医院业务瘫痪，西班牙某电信公司有 85%的电脑感染该恶意程序。至少 1600 家美国组织， 11200 家俄罗斯组织和 6500 家中国组织和企业都受到了攻击。

截至目前，受到 WannaCry 攻击的机构和用户包括，英国 NHS、西班牙的电讯公司 Telefónica、俄国内政部、FedEx 等等。中国高校也大面积遭受了攻击，据有关机构统计，目前国内每天有 5000 多台机器遭到“永恒之蓝”的攻击，教育网是受攻击的重灾区。

机理分析



WannaCry 主要利用钓鱼邮件进入受害机构的内部网络，进而以蠕虫病毒方式侵害内部网络中的其它 Windows 服务器和桌面终端。

WannaCry 利用 MS17-010 漏洞，向用户机器的 445 端口发送精心设计的网络数据包文，实现远程代码执行。勒索软件被漏洞远程执行后，会通过 Windows Crypto API 对多种类型的文件进行 AES+RSA 的组合加密，被加密后的文件扩展名被统一改为“.WNCRY”。

Windows 系统中以下所有后缀类型的文件均会被 WannaCry 进行恶意加密：.docx.docb.docm.dot.dotm.dotx.xls.xlsx.xlsm.xlsb.xlw.xlt.xlm.xlc.xltx.xltm.ppt.pptx.pptm.pot.pps.ppsm.ppsx.ppam.potx.potm.pst.ost.msg.eml.edb.vsd.vsdx.txt.csv.rtf.123.wks.wk1.pdf.dwg.onetoc2.snt.hwp.602.sxi.sti.sldx.sldm.sldm.vdi.vmdk.vmx.gpg.aes.ARC.PAQ.bz2.tbk.bak.tar.tgz.gz.7z.rar.zip.backup.iso.vcd.jpeg.jpg.bmp.png.gif.raw.cgm.tif.tiff.nef.psd.ai.svg.djvu.m4u.m3u.mid.wma.flv.3g2.mkv.3gp.mp4.mov.avi.asf.mpeg.vob.mpg.wmv.fla.swf.wav.mp3.sh.class.jar.java.rb.asp.php.jsp.brd.sch.dch.dip.pl.vb.vbs.ps1.bat.cmd.js.asm.h.pas.cpp.c.cs.suo.sln.ldf.mdf.ibd.myi.myd.frm.odb.dbf.db.mdb.accdb.sql.sqlitedb.sqlite3.asc.lay6.lay.mml.sxm.otg.odg.uop.std.sxd.otp.odp.wb2.slk.dif.stc.sxc.ots.ods.3dm.max.3ds.uot.stw.sxw.ott.odt.pem.p12.csr.crt.key.pfx.der。

防范思路

需要特别说明的是，对于已经感染 WannaCry 的计算机，目前没有理想办法实现数据恢复，因此应急防范的重点应当在于尽可能抑制该勒索软件的传播和扩散，使大量可能被感染的计算机和网络具备针对该勒索软件的免疫能力，最大程度上降低受影响的计算机数量和范围。

由于 WannaCry 是通过网络传播，且利用 Windows 系统服务中的漏洞进行感染，因此针对该类型勒索软件的紧急防范，也应该在网络传播途径和 Windows 终端系统两方面进行应对。

WannaCry 主要通过钓鱼电子邮件传入机构内部网络，因此在网络边界应当部署可以检测到该勒索软件特征的 IPS 入侵防范系统，绿盟科技在捕获到 WannaCry 的样本，对其进行分析之后，对应的检测规则已经添加到 IPS 系统的攻击规则库中，部署了绿盟 IPS 系统的客户应当尽快进行规则库升级，以实现对 WannaCry 的有效检测和阻断，这样能够抑制该勒索软件的扩散和传播。

WannaCry 利用 Windows 系统服务 445 端口存在的漏洞实现感染，无论是关闭可能存在漏洞的系统服务，还是及时安装微软最新发布的安全补丁，都能够实现针对该勒索软件的有效免疫。

截至目前，勒索病毒仍在蔓延，影响到所有联网电脑用户的文件，为避免和减少损失，请所有人员认真查看此须知！！！请各单位信息管理部负责监督落实，并及时向我部及本单位保密管理委员会统计上报损失情况！

应对措施建议

一、病毒影响范围

MS17-010 漏洞主要影响以下操作系统：Windows 2000，Windows 2003，Windows2008，Windows2012，Windows XP，Windows Vista，Windows7，Windows8，Windows10。

二、应急解决方案

对于未开机或未被感染的计算机：

第一步：断开网络（拔掉网线）；

第二步：使用 U 盘或光盘自带的 PE 系统启动电脑，将计算机中所有重要文件（尤其文档、图片、照片、压缩包、音频、视频等）备份到移动存储设备上。

第三步：开启系统防火墙，并利用系统防火墙高级设置阻止向 445 端口进行连接。

第四步：对系统进行 ms17010、ms10061、ms14068、ms08067、ms09050 补丁更新。

三、启动防火墙及阻止 445 端口处理流程

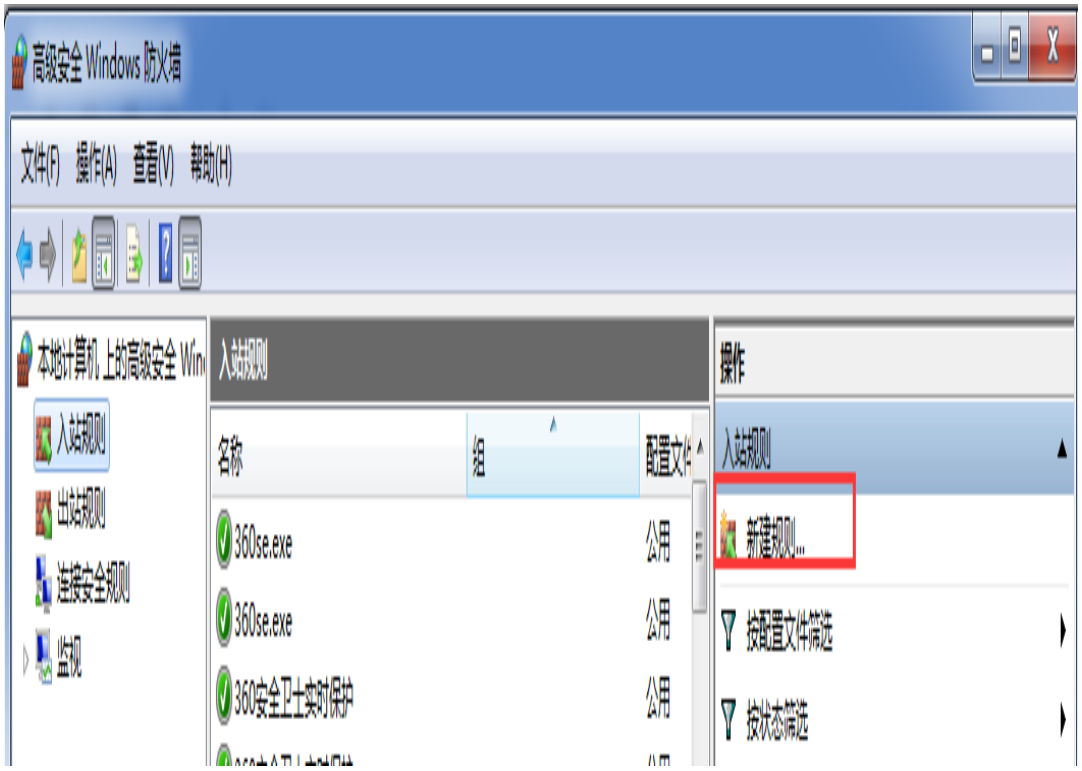
Win7、Win8、Win10 的处理流程：

1、打开控制面板-系统与安全-Windows 防火墙，点击左侧启动或关闭 Windows 防火墙

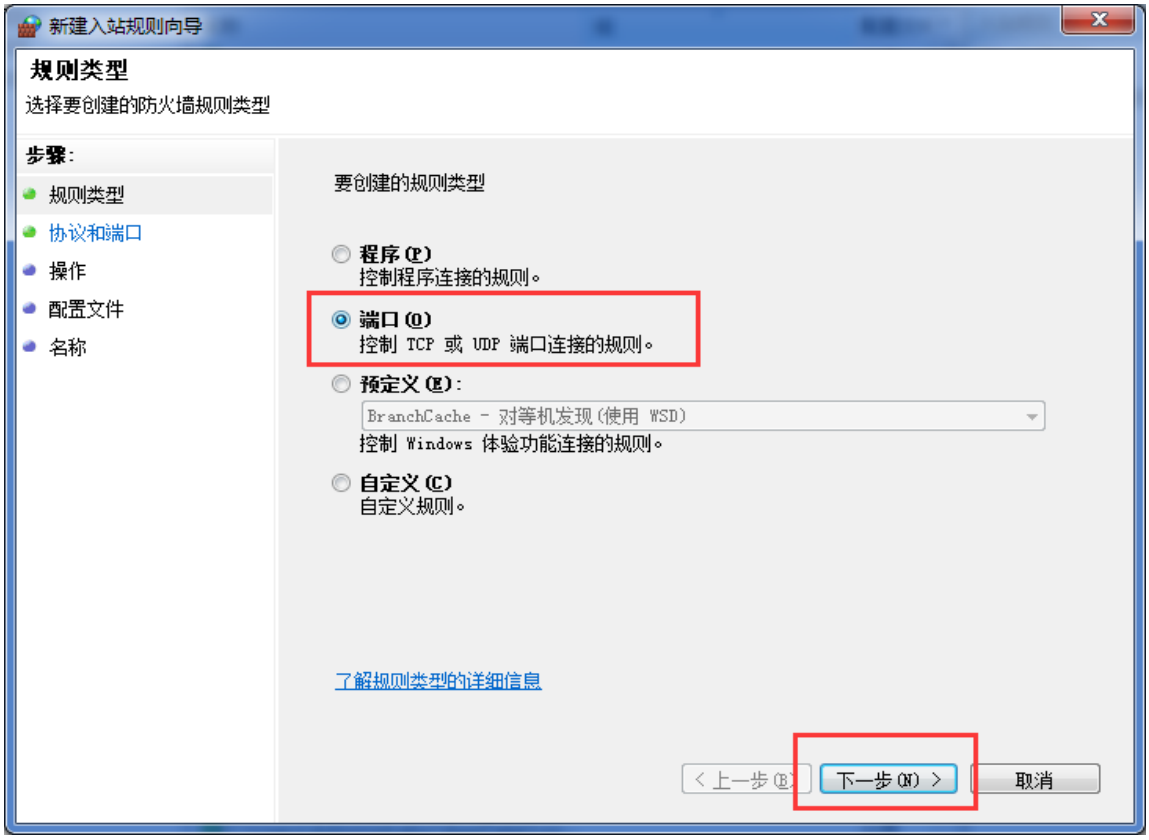
2、选择启动防火墙，并点击确定。

3、点击高级设置。

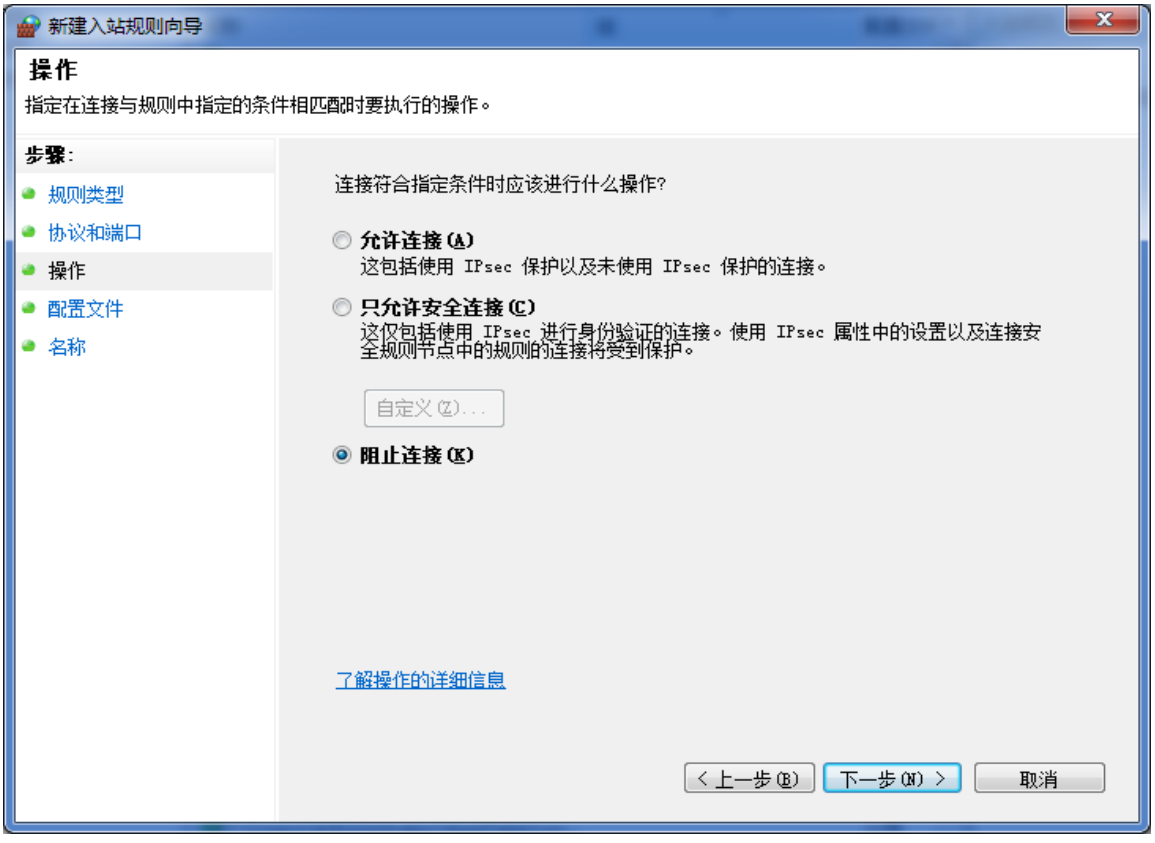
4、点击入、出站规则，新建规则。



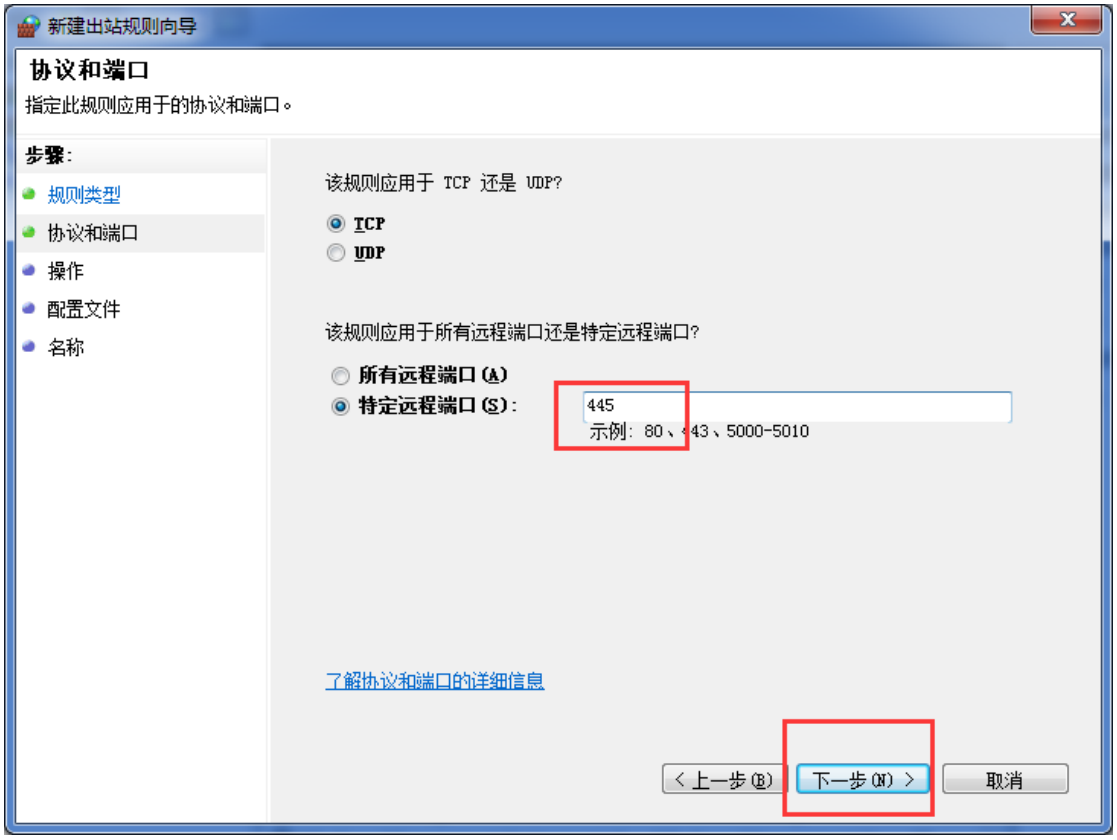
5、选择端口，下一步。



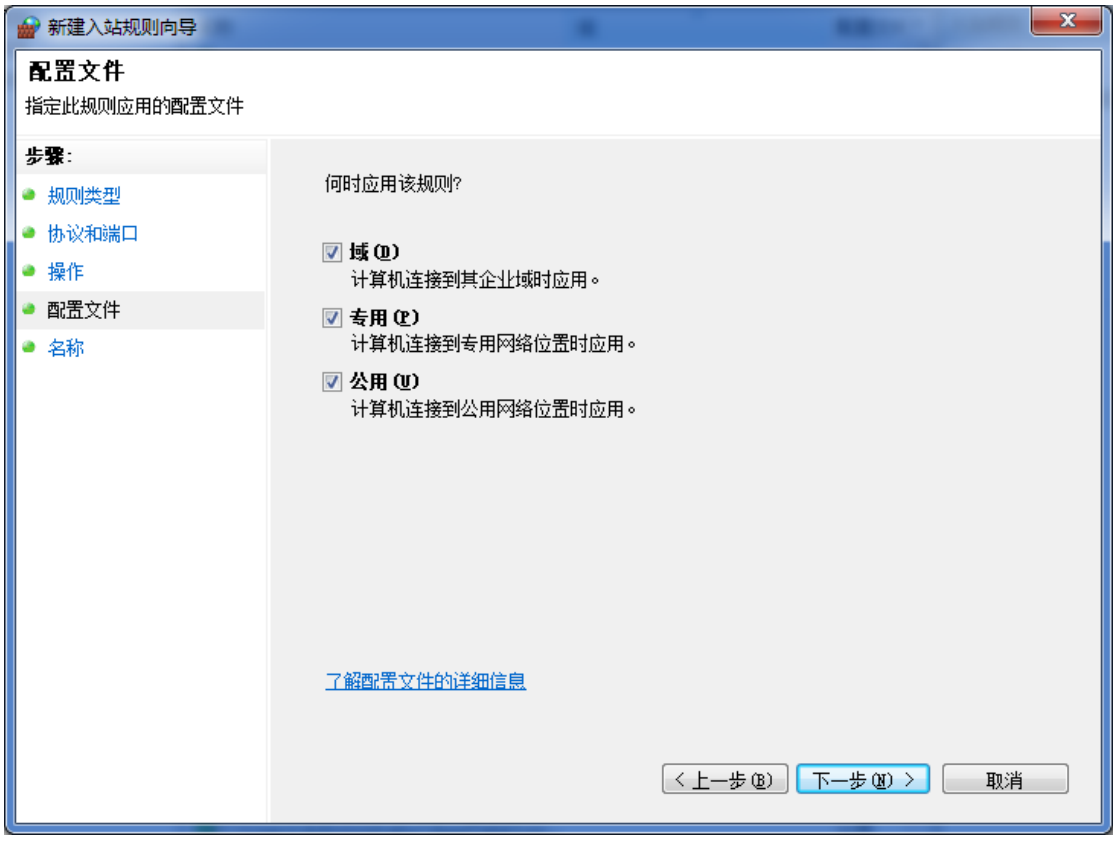
6、选择阻止连接，下一步。



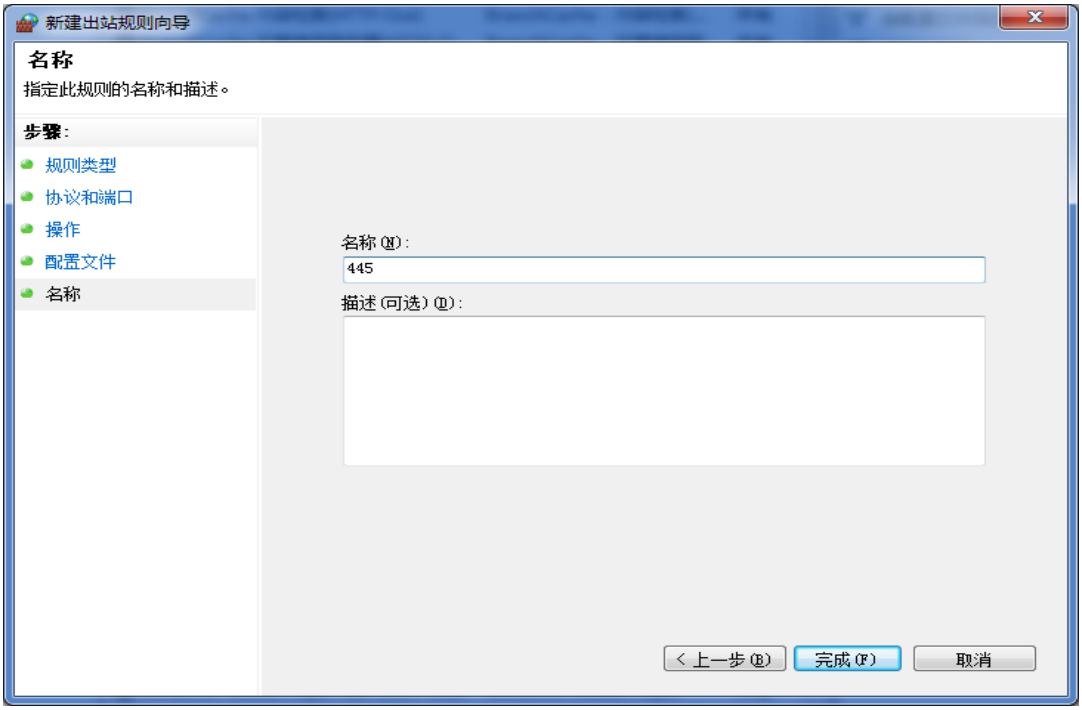
7、特定本地端口，输入 445，下一步。



8、配置文件，全选，下一步。

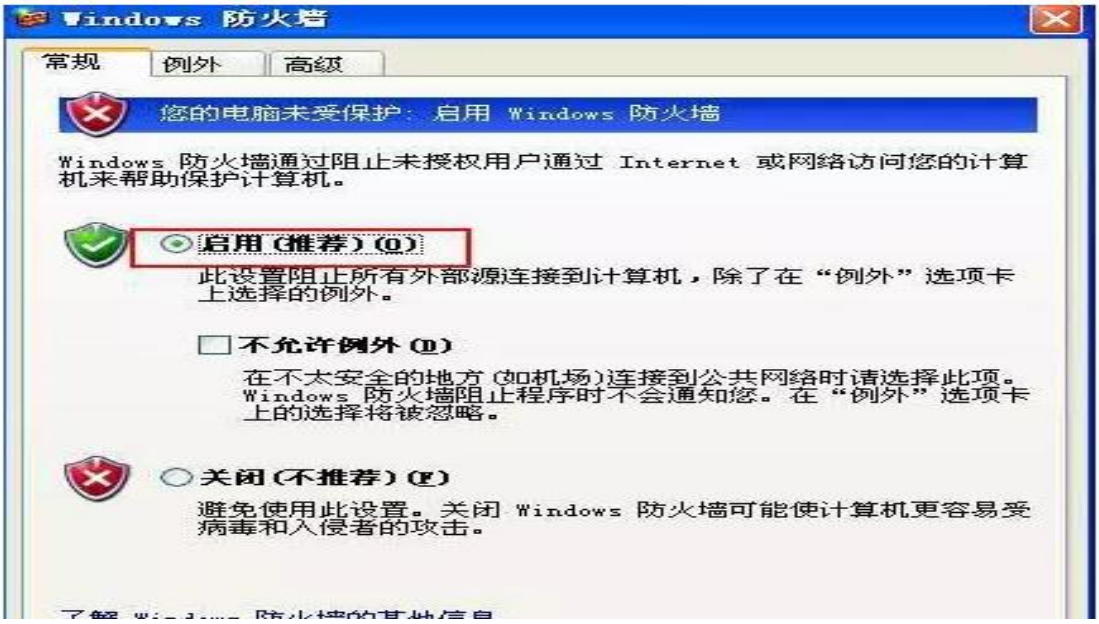


9、名称，可以任意输入，完成即可。



XP 系统的处理流程：

1、依次打开控制面板，安全中心，Windows 防火墙，选择启用



2、点击开始，运行，输入 cmd，确定执行下面三条命令

net stop rdr

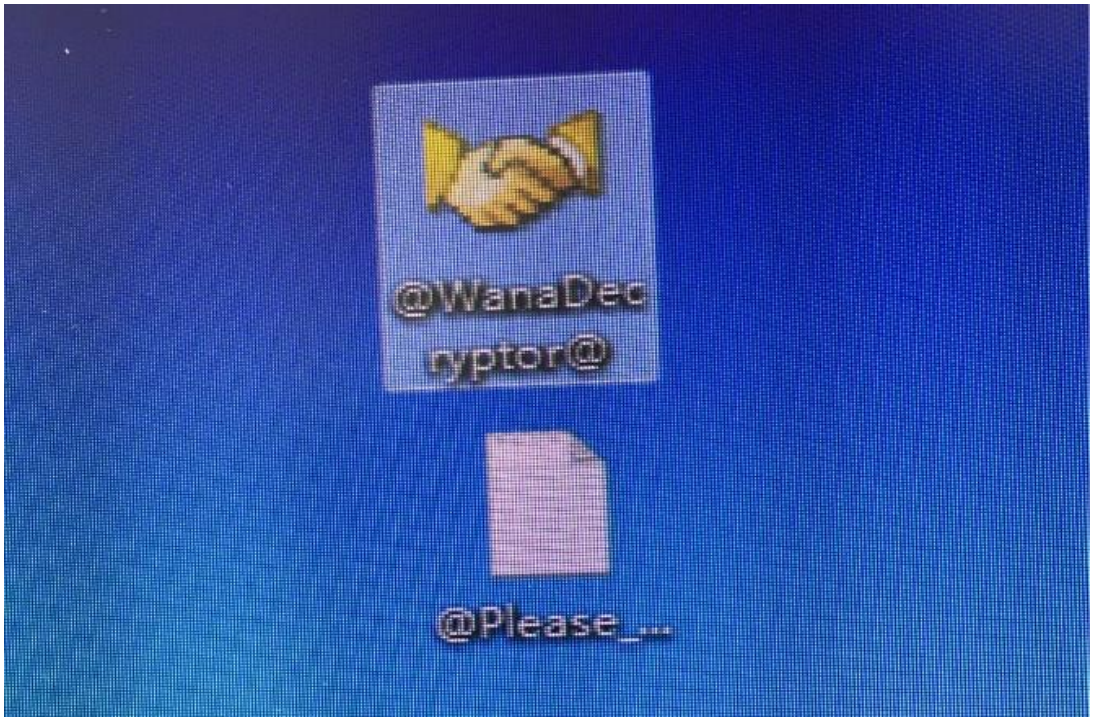
net stop srv

net stop netbt

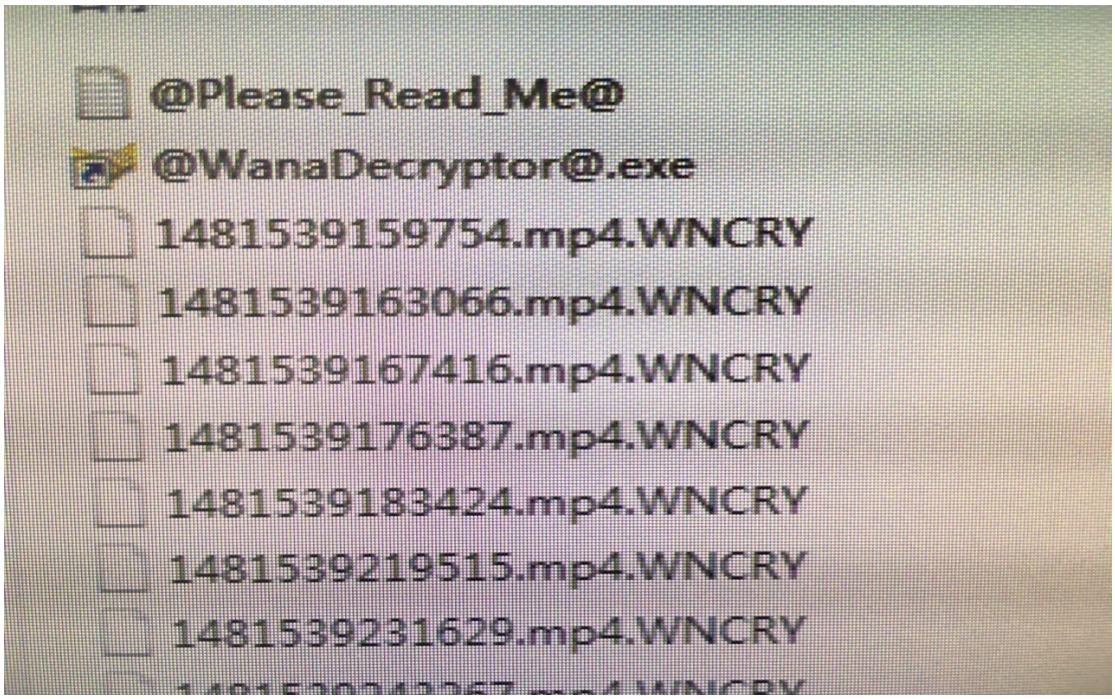
四、如何分辨是否中毒：

当系统被该勒索软件入侵后，会弹出勒索对话框：

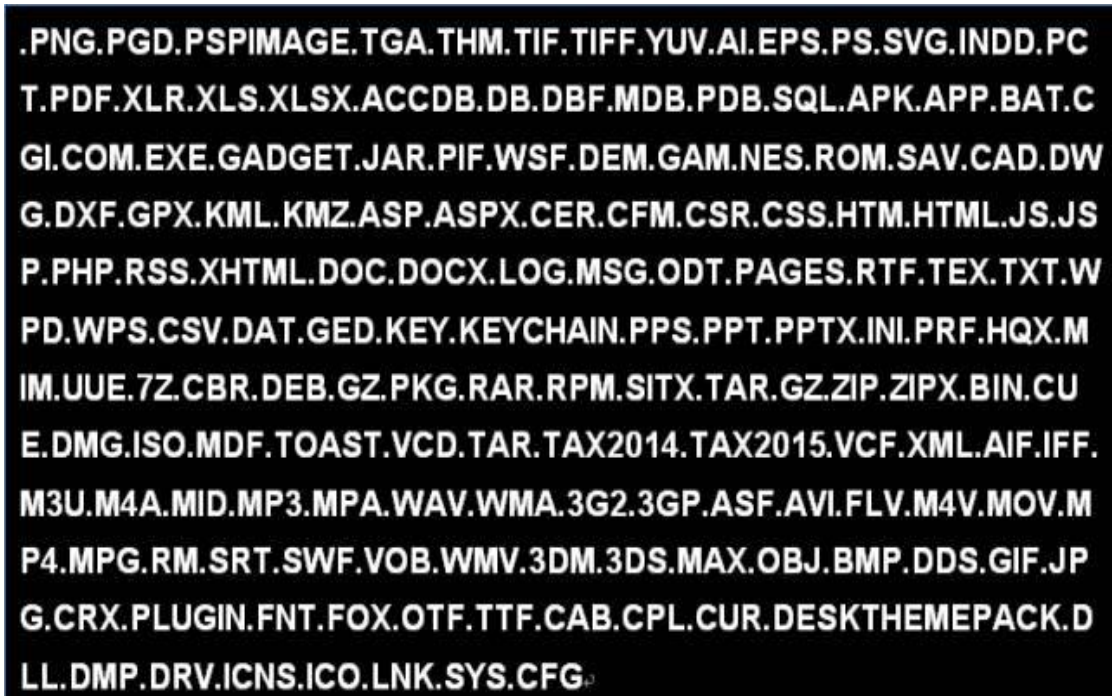
或在桌面及各个文件夹内出现以下文件：



所有被感染文件以“.WNCRY”为后缀：



该病毒目前没有专杀工具，加密文件无法暴力破解。如不幸感染病毒，系统中有重要文件的请等待解密工具，没有重要文件的可以选择格式化全盘并重做系统。该勒索软件采用包括英语、简体中文、繁体中文等 28 种语言进行“本地化”。会将自身复制到每个文件夹下，并重命名为“@WanaDecryptor@.exe”。同时衍生大量语言配置等文件，该勒索软件 AES 和 RSA 加密算法，加密的文件以“WANACRY!”开头，加密如下后缀名的文件：



微软提供免费查扫工具：

In addition, the free Microsoft Safety Scanner http://www.microsoft.com/security/scanner/ is designed to detect this threat as well as many others.

由于本次 Wannacry 蠕虫事件的巨大影响，微软总部决定发布已停服的 XP 和部分服务器版特别补丁：

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

网络和系统运维人员该怎么办？

网络边界如果已经部署 IPS 系统，运维人员应当尽快完成 IPS 检测规则库的升级，阻断 WannaCry 勒索软件从互联网进入机构内部网络的主要途径。

如果机构内部网络中部署有集中的补丁管理系统，应当尽快完成微软 MS17-010 安全补丁的统一升级，使得 Windows 计算机具备对 WannaCry 勒索软件的免疫能力。

事件思考