**关于防范基于SMB文件共享传播的蠕虫病毒攻击安全预警通告**

 安天安全研究与应急处理中心（Antiy CERT）发现，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，我国大量行业企业内网大规模感染，教育网受损严重，攻击造成了教学系统瘫痪，甚至包括校园一卡通系统。

经过安天CERT紧急分析，判定该勒索软件是一个名称为“wannacry”的新家族，目前无法解密该勒索软件加密的文件。该勒索软件迅速感染全球大量主机的原因是利用了基于445端口传播扩散的SMB漏洞MS17-101，微软在今年3月份发布了该漏洞的补丁。

该漏洞的相关说明、补丁：

<https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx>

2017年4月14日黑客组织Shadow Brokers（影子经纪人）公布的Equation Group（方程式组织）使用的“网络军火”中包含了该漏洞的利用程序，而该勒索软件的攻击者或攻击组织在借鉴了该“网络军火”后进行了这次全球性的大规模攻击事件。

  安天CERT在2017年4月14日发布的《2016年网络安全威胁的回顾与展望》中提到“网络军火”的扩散全面降低攻击者的攻击成本和勒索模式带动的蠕虫的回潮不可避免等观点。结果未满1个月，安天的这种“勒索软件+蠕虫”的传播方式预测即被不幸言中，并迅速进入全球性的感染模式。

  安天依托对“勒索软件”的分析和预判，不仅能够有效检测防御目前“勒索软件”的样本和破坏机理，还对后续“勒索软件”可能使用的技巧进行了布防。安天智甲终端防御系统完全可以阻止此次勒索软件新家族“wannacry”加密用户磁盘文件。

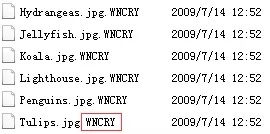
**事件分析:**

 经过安天CERT紧急分析，判定该勒索软件是一个名称为“wannacry”的新家族，目前无法解密该勒索软件加密的文件。该勒索软件迅速感染全球大量主机的原因是利用了基于445端口传播扩散的SMB漏洞MS17-101，微软在今年3月份发布了该漏洞的补丁。2017年4月14日黑客组织Shadow Brokers（影子经纪人）公布的Equation Group（方程式组织）使用的“网络军火”中包含了该漏洞的利用程序，而该勒索软件的攻击者或攻击组织在借鉴了该“网络军火”后进行了些次全球性的大规模攻击事件。

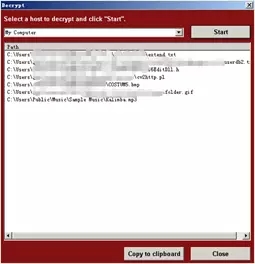
        当系统被该勒索软件入侵后，弹出勒索对话框：



        加密系统中的照片、图片、文档、压缩包、音频、视频、可执行程序等几乎所有类型的文件，被加密的文件后缀名被统一修改为“.WNCRY”。



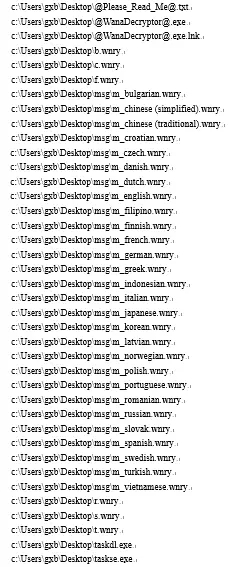
        攻击者极其嚣张，号称“除攻击者外，就算老天爷来了也不能恢复这些文档” （该勒索软件提供免费解密数个加密文件以证明攻击者可以解密加密文件，“点击 <Decrypt> 按钮，就可以免费恢复一些文档。”该勒索软件作者在界面中发布的声明表示，“3天内付款正常，三天后翻倍，一周后不提供恢复”）。现实情况非常悲观，勒索软件的加密强度大，没有密钥的情况下，暴力破解需要极高的运算量，基本不可能成功解密。



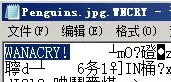
        该勒索软件采用包括英语、简体中文、繁体中文等28种语言进行“本地化”。



该勒索软件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：

|  |
| --- |
| **.PNG.PGD.PSPIMAGE.TGA.THM.TIF.TIFF.YUV.AI.EPS.PS.SVG.INDD.PCT.PDF.XLR.XLS.XLSX.ACCDB.DB.DBF.MDB.PDB.SQL.APK.APP.BAT.CGI.COM.EXE.GADGET.JAR.PIF.WSF.DEM.GAM.NES.ROM.SAV.CAD.DWG.DXF.GPX.KML.KMZ.ASP.ASPX.CER.CFM.CSR.CSS.HTM.HTML.JS.JSP.PHP.RSS.XHTML.DOC.DOCX.LOG.MSG.ODT.PAGES.RTF.TEX.TXT.WPD.WPS.CSV.DAT.GED.KEY.KEYCHAIN.PPS.PPT.PPTX.INI.PRF.HQX.MIM.UUE.7Z.CBR.DEB.GZ.PKG.RAR.RPM.SITX.TAR.GZ.ZIP.ZIPX.BIN.CUE.DMG.ISO.MDF.TOAST.VCD.TAR.TAX2014.TAX2015.VCF.XML.AIF.IFF.M3U.M4A.MID.MP3.MPA.WAV.WMA.3G2.3GP.ASF.AVI.FLV.M4V.MOV.MP4.MPG.RM.SRT.SWF.VOB.WMV.3DM.3DS.MAX.OBJ.BMP.DDS.GIF.JPG.CRX.PLUGIN.FNT.FOX.OTF.TTF.CAB.CPL.CUR.DESKTHEMEPACK.DLL.DMP.DRV.ICNS.ICO.LNK.SYS.CFG** |

注：该勒索软件的部分版本在XP系统下因文件释放未成功而未加密用户文件。



**临时解决方案:**

* 开启系统防火墙
* 利用系统防火墙高级设置阻止向445端口进行连接（该操作会影响使用445端口的服务）
* 打开系统自动更新，并检测更新进行安装

**安全建议：**

1.及时更新最新的操作系统补丁。

2.关闭操作系统不必要开放的端口如445、135、137、138、139等，关闭网络共享。

3.定期备份重要文件数据。请各用户对自己所用系统和数据进行排查和备份，消除隐患。

**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

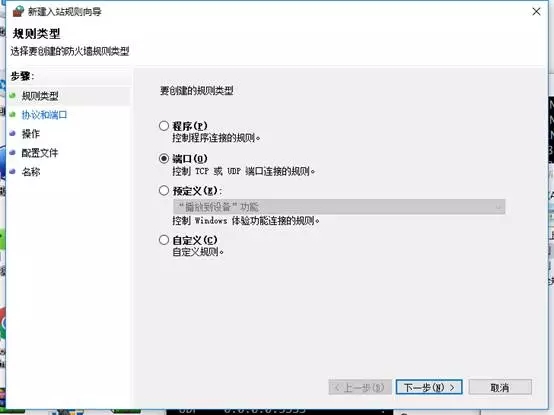


3、点击高级设置

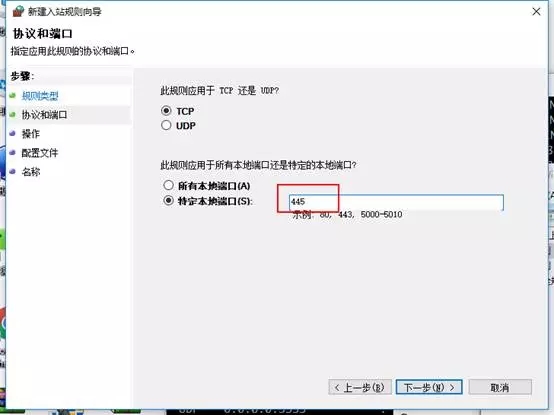
4、点击入站规则，新建规则



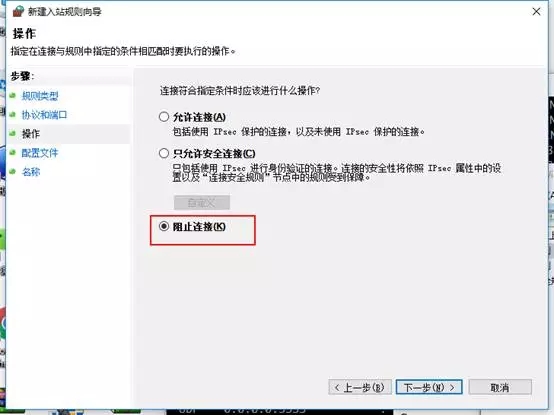
5、选择端口，下一步



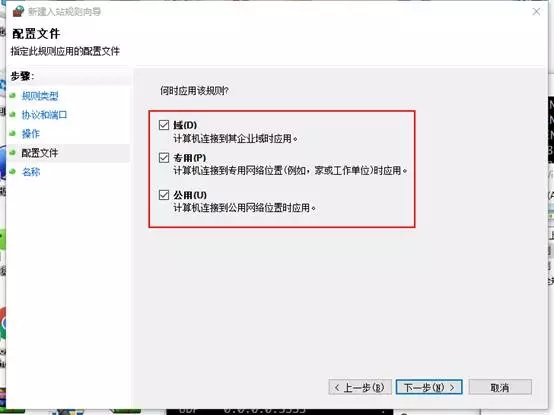
6、特定本地端口，输入445，下一步



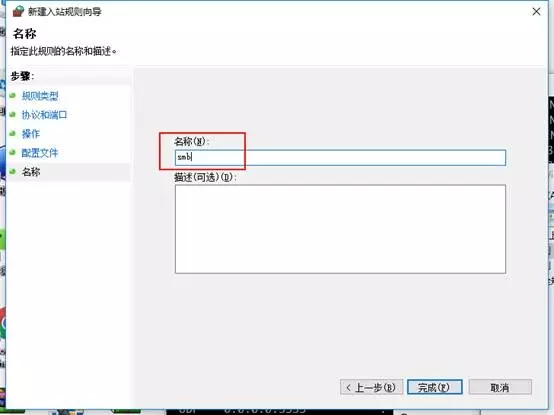
7、选择阻止连接，下一步



8、配置文件，全选，下一步

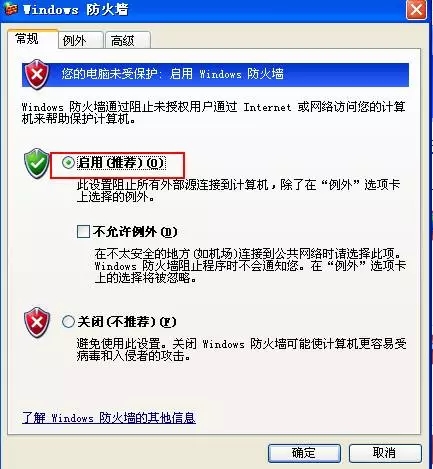


9、名称，可以任意输入，完成即可。



**3.2  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 |

3、由于微软已经不再为XP系统提供系统更新，建议用户尽快升级到高版本系统。

请下载NSA武器库免疫工具，用以检测个人计算机是否存在安全漏洞，下载地址：

http://dl.360safe.com/tools