鄂尔多斯市信息资源中心关于做好wana 新型恶意软件爆发预警防范工作的紧急通知

市直各部门及各旗区信息化主管部门：

接自治区外网办紧急通知，要求立即部署做好wana 新型恶意软件爆发预警防范工作，具体情况及工作要求如下：

　　本次爆发的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（永恒之蓝），微软在今年3月份发布了该漏洞的补丁。

　　这次网络安全事件涉及所有使用windows操作系统的服务器和个人电脑，周六日休息问题可能没显现出来，周一上班问题可能就比较严重了，请各单位务必要高度重视，做好预警防范工作。

　　一、**服务器相关安全加固建议：**

　　1.及时更新最新的操作系统补丁。该漏洞的相关说明、补丁：https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx

　　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。

**二、网络以及个人PC机器方面安全加固建议：**

 　　1.全面控制接入交换机、核心交换机、防火墙、IPS以及出口网络设备等的安全策略，在网络设备上封堵445、135、137、138、139端口。

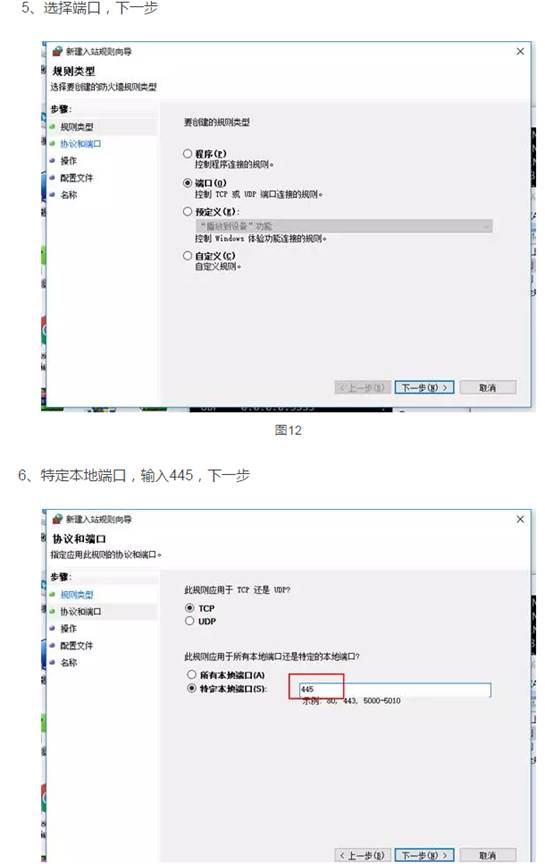
　　2.PC机处理流程

　　（1）及时更新最新的操作系统补丁。该漏洞的相关说明、补丁：

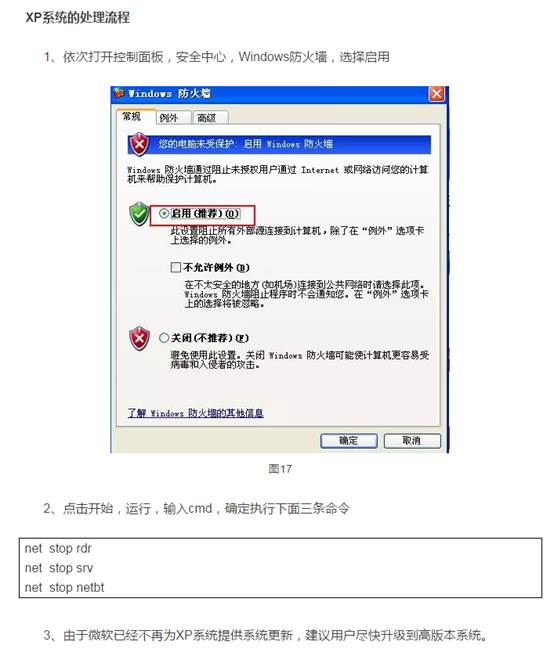
https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx

　　（2）封堵系统端口









     请各部门高度重视，立即部署开展对政务网、互联网上运行的服务器及办公电脑的排查工作，有被攻击感染情况及时上报。

鄂尔多斯市信息资源中心

2017年5月14日

(联系电话：8589600）