**关于防范感染勒索蠕虫病毒的紧急通知**

**各二级学院、部门：**

接教育部、省公安厅、省网信办通报，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。据公安部门通报，教育行业已有多台终端遭遇了攻击，情况严重。为控制病毒感染扩散，确保我校不发生连片式的网络安全事件，现紧急通知如下：

**一、开展漏洞扫描与修复工作。**请各二级学院和部门积极开展漏洞扫描与修复工作，组织技术力量对本单位的主管IP及学生IP进行扫描。如发现问题报告至网络与教育技术中心，并同时采取临时限制互联网访问的措施，待漏洞修复后方可恢复服务，应对方案见附件，必要时请中心技术人员处理。

**二、系统排查本单位感染终端数量。**请各二级学院和部门对本单位公共设备（如显示屏、公众终端、服务器）进行排查，如遭遇感染应立即采取应急措施，将影响降到最低。

**三、加强舆情管控。**目前大部分的媒体都片面报道教育网发生的事件。请各单位及时关注相关舆情在校园里的传播，及时普及防病毒的常识，避免造成恐慌。

**如发现此次事件相关的任何问题，请及时报告网络与教育技术中心**

联系人：吴为胜

联系电话：15107096180 邮箱：190346304@qq.com

网络与教育技术中心

2017年5月13日

**附件：**

**关于 WannaCry/Wcry 勒索蠕虫病毒的具体防范措施建议**

**个人计算机用户的预防措施：**

1、使用Widnows Vista、Windows 7、Windows 8.1、Windows 10、Windows Server 2008、Windows Server 2012、Windows Server 2016 系统的用户，请启用系统自带的更新功能将补丁版本升级到最新版本；

2、仍然使用Windows XP、Windows 8 及 Windows Server 2003 系统用户，建议升级操作系统到 Windows 7 及以上，如果因为特殊原因无法升级操作系统版本的，请手动下载补丁程序进行安装，补丁下载地址：

<http://www.catalog.update.microsoft.com/Search.aspx?q=KB401259>

3、升级电脑上的杀毒软件病毒库到最新版本。

**校园网预防措施：**

在校园网设备上阻断TCP 135、137、139、445 端口的连接请求，将会有效防止该病毒的传播，但是同时也阻断了校内外用户正常访问使用Windows系统相应文件共享机制的信息系统和网络服务。因此，必须谨慎使用下列预付措施：

1、在网络边界（如校园网出口）上阻断 TCP 135、137、139、445 端口的连接请求。这个操作可有效阻断病毒从外部传入内部网络，但无法阻止病毒在内部网络传播。

2、在校园网的核心交换设备处阻断 TCP 135、137、139、445 端口的连接请求，该操作可阻断病毒在校内的局域网间进行传播，但无法阻止病毒在局域网内传播。

3、在局域网子网边界处阻断 TCP 135、137、139、445 端口的连接请求，该操作可最大限度保护子网的安全，但是无法阻挡该病毒在同台交换机下传播。

**综上所述，阻断网络的TCP 135、137、139、445 端口连接请求只是临时措施，尽快完成各类用户Windows系统软件的升级或修复漏洞才是防范该病毒的根本措施。**