附一：教育部科技司关于防范全球爆发勒索病毒“永恒之蓝”的通知  
各省级教育行政部门、部属高校、直属单位：  
      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，确保教育行业不发生连片式的网络安全事件，现紧急通知如下：  
      一、在边界出口交换路由设备禁止外网对内部135/137/138/139/445端口的连接；在校园网络核心主干交换路由设备禁止对135/137/138/139/445端口的连接。  
      二、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进行扫描。如发现存在漏洞，应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。对winXP\2000等系统，要采取防火墙等措施，避免感染。  
      三、系统排查本单位感染终端数量。对公共设备（如显示屏、公众终端、服务器）遭遇感染，应立即采取应急措施，将影响降到最低，并汇总受影响的终端数量，报教育部科技司。  
      四、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。  
       感染情况和漏洞情况请于5月14日中午12点前报[aqtb@moe.edu.cn](mailto:aqtb@moe.edu.cn)。为避免因病毒感染造成不可挽回的损失，请及时保存备份关键数据。

附二：赛尔网关于防范感染勒索蠕虫病毒的紧急通知  
 CERNET各会员单位：  
      北京时间2017年5月12日20时起，一款名为WannaCry/Wcry的勒索蠕虫病毒在全球范围开始传播。据有关媒体报道，感染该病毒后的系统重要数据会被黑客加密，并索取一定价值的比特币后，数据才会被解密。因此该病毒可能给用户带来的危害很难估计。  
      该攻击代码利用了Windows文件共享协议中的一个安全漏洞通过TCP 445端口进行攻击，漏洞影响Windows全线的操作系统，微软2017年3月的例行补丁（MS17-010）对该漏洞进行了修补。WannaCry/Wcry勒索蠕虫病毒所利用的漏洞攻击代码是黑客组织Shadow Brokers（影子经纪人）在今年4月14日披露的Equation Group（方程式组织）使用的黑客工具包中的一个，攻击程序名为ETERNALBLUE，国内安全厂商命名为“永恒之蓝”。  
      为防范该病毒对CERNET各用户单位计算机系统的感染和传播，尽可能减少其危害和影响，建议CERNET各用户单位尽快采取相应的具体防范措施建议，见附件。  
                                               中国教育和科研计算机网CERNET  
                                                     应急响应组CCERT  
                                                       2017年5月13日