关于防范基于SMB文件共享传播的蠕虫病毒的操作措施建议

近期国内多所院校出现ONION勒索软件感染情况，磁盘文件会被病毒加密为.onion后缀，对学习资料和个人数据造成严重损失。根据网络安全机构通报，这是不法分子利用Windows主机系统基于445端口传播扩散的SMB漏洞进行病毒的主动传播。

现紧急提醒广大用户通过以下措施进行防范：

1. 网络层措施：在网络或主机防火墙上阻断对445端口的访问。
2. 终端层措施：微软在今年3月份发布了该漏洞的补丁，Win7及以上版本的系统，安装MS07-010补丁；Windows XP/2003 由于没有补丁，暂时关闭server服务。
3. 漏洞检测预防：下载各类专杀工具进行检测和加固，例如：http://dl.360safe.com/nsa/nsatool.exe
4. 校园网内已感染的计算机会携带病毒活体文件且在内网进一步传播，因此应谨慎使用USB设备或文件拷贝，及时更新病毒防护软件。
5. 针对重要业务系统立即进行数据备份，针对重要业务终端进行系统镜像，制作足够的系统恢复盘或者设备进行替换。

赛尔网络 网络运行部（CERNOC）
7x24小时联系方式：010-62784048
邮箱 cernoc@cernet.edu.cn