**网络信息中心针对勒索病毒应对方案**

机层防护措：
　　1、临时措施：用单机版防火墙关闭windows终端的的135、139、445端口；
　　启用并打开“Windows防火墙”，进入“高级设置”，在入站规则里禁用“文件和打印机共享”相关规则。
　　2、针对windows 2003以上系统需要升级最新的MS17-101补丁；
　　3、针对windowsXP 以及 2003，建议升级操作系统版本
　　4、针对windows服务器照样受到蠕虫影响，建议采取以上3点措施；

主动防御层面：
　　1、开展针对病毒及APT的监测工作，防范带有恶意行为的可执行文件传入内网，包括开展针对邮件、U盘文件以及其他互联网下载文件等；
　　2、针对内网进行网络区域隔离，屏蔽445、135、139端口的互相访问；
　　3、采用终端防病毒措施；

主动检测层面：
　　扫描内网，发现所有开放445 SMB服务端口的终端和服务器，对于Win7及以上版本的系统确认是否 安装了MS17-010补丁，如没有安装则受威胁影响。

其他：
1、如不幸中招，不要给黑客缴纳赎金；
2、电脑端的Windows Update记得开启；
3、不要轻易点击来路不明的网站和文件等；
4、重要资料及时备份在移动硬盘或云端

注意：

补丁链接：http://its.stiei.edu.cn/s/11/t/122/53/f3/info21491.htm