附件 2. 感染网络勒索病毒应急处置建议

根据多个安全组织反馈，感染此次网络勒索病毒后，电脑中重要文件将被病毒加密，并显示提示信息。

如发现勒索病毒感染情况，**应立即断开网络，第一时间上报漏洞感染情况**。

由于目前尚没有针对此次勒索病毒的可信可靠的恢复手段，恢复主机使用只能重装 Windows 操作系统。具体处置建议如下：

1）使用离线方式安装操作系统，也就是在断开网络连接的情况下进行安装。

2）操作系统安装后，第一时间启用并打开“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；关闭 445、135、137、138、139 、3389、5900 端口，关闭网络文件共享和远程桌面连接服务。

3）通过可靠方式连接网络，如将主机连接到一个路由器下后通过路由器访问网络，降低被网络环境中已感染勒索病毒主机的影响。

4）第一时间通过 Windows 系统补丁自动升级功能，将 Windows 主机系统更新升级到最新状态。

5）安装主流杀毒软件，将软件病毒库升级至最新。

对于有大量重要文档信息的个人主机和服务器，要经常性进行重要文件备份，并将备份介质离线保存（也就是将备份的硬盘断开与主机的 USB 等连接来存放）；停止使用 Windows XP、Windows 2003 等微软公司已不再提供安全更新的操作系统，及时升级操作系统补丁到最新。