安徽省卫生计生委

内部传真

卫传〔2018〕76号　　签发人：高俊文

关于做好计算机勒索病毒防范工作的通知

各市及省直管县卫生计生委，委直属各单位、省属各医院，委机关各处室：

近期，多地发生计算机勒索病毒事件，病毒主要攻击开启远程桌面服务的服务器，利用密码抓取工具暴力破解获取管理员密码后对内网服务器发起扫描并人工投放勒索病毒，导致文件被加密。病毒感染后的主要特征包括windows服务器文件被加密，且加密文件的文件名后缀为*.RESERVE。为做好对勒索病毒的防范和应急处置工作，现就有关通知如下。

一、易受攻击影响的机构

攻击者主要的突破边界手段可能为 windows 远程桌面服务密码暴力破解，在进入内网后会尝试多种方法获取登陆凭证并在

内网横向传播。符合以下特征的机构更容易遭到攻击者的侵害:

（一）存在弱口令且 windows 远程桌面服务（3389 端口）暴露在互联网上的机构;

（二）内网 windows 终端、服务器使用相同或者少数几组口令;

（三）windows 服务器、终端未部署或未及时更新安全加固和杀毒软件。

目前我省受攻击单位主要集中在医疗行业。

二、应急处置建议

（一）已感染病毒的机器: 下线隔离，利用纯净备份恢复系统。

（二）未感染病毒的机器:

1. 将防毒墙、IPS/IDS 等设备的特征库升级到最新。

2. 在网络边界防火墙上全局关闭 3389 端口或 3389 端口只对特定 IP 开放。

3. 服务器开启防火墙，建议关闭 3389、445、139、135 等不用的高危端口。

4. 每台服务器设置唯一口令，且复杂度要求采用大小写字母、数字、特殊符号混合的组合结构，口令位数足够长（15 位、两种组合以上）。

5. 及时更新 windows 操作系统已发布的安全补丁。

6. 安装并及时更新杀毒软件。

7. 服务器开启关键日志收集功能，为安全事件的追踪溯源提供基础。

8.不要点击不明链接、不要下载不明文件、不要打开不明邮件。

9.如有重要文件资料，请及时做好数据备份。

请各市及省直管县卫生计生委将相关情况及时通报所辖各级医疗机构，如有问题，请及时与当地政府信息中心或公安网监部门联系解决；委直属各单位、省属各医院和委机关各处室网站、网页如有问题，请与委信息中心联系，联系人：宋忠诚　李麟，电话：0551-62242387、62242395。

安徽省卫生计生委

2018年8月31日