

能为 windows 远程桌面服
试多种方法获取登陆凭证并

安徽省 内部

卫传〔201

生计生委

传真

关于

签发人: 高俊

各市及省

关各处室:

近期,

程桌面服

码后对内

密。病毒展

加密文件的

和应急处

一、

攻击者

密码暴力破

勒索病毒

委直

勒索病毒

密码抓

并人工

包括 w

RESER

通知如

勾

手段可

会尝

勒索病毒防范工作的通知

属各单位、省属各医院,委

毒事件,病毒主要攻击开启

工具暴力破解获取管理员

投放勒索病毒,导致文件被

indows 服务器文件被加密,

。为做好对勒索病毒的防

下。

网
暴
露
在
今
科
杀
毒
目
二
统
1.
特
定
I
用
的
高
数
字
种
组
合
5.
6.
7.
供
基

客查
身口
有孔
Nacos
可展
真安
置康
能母
病毒
IP
防火
防火
设置
合的
更新
关健

特征的机构更暴露到
windows 远端桌面服务
终端。更多暴露使用相同或
暴露，终端未部署或未及时
主要集中在医疗行业。
暴露：下载层高，利用特
设备：
等设备的特征率先暴露
上全岛美国 3389 端口或
建设美国 9599、445、
一口令，且复杂度要求不
合结构。口令位数足够
是作系统已发布的安全补
象软件。
告收集功能，为安全事件

8. 不要点击不明链接。
件。

9. 如有重要文件资料，
请各市及省直管县级医疗机构，如有问题，
部门联系解决；委直属各
网页如有问题，请与委
电话：0551-62242387、

不要下载不明文件，不要打开不明邮件。

请及时做好信息报告。

重要者相关请就近向通源所报告。

省卫健委疫情防控信息中心网络安全网组

省各医院和委机关各处室网站。

联系：联系机：宋传斌 李晨

组。

