

做 windows 系统真跟照书
高知那左法获取链接地址并查

安

行

省

日

音

生 计 生

生 委

正 传 [2018]

关于做

传 真

各
关

程
码
密
加
和

密

市及省直
各处室：

近期，多
桌面服务
后对内网
病毒感染
密文件的
应急处置

一、易受
攻击者主
码暴力破

数家涉

委，委直

数家涉

密码破

百部六二

衣指

RESOR

通知安

被

等股其

行会登

编发人：黄俊文

国防科信院编

城名单位，非福建厦门，委编

力事件，功山主署衣书并肩编

版：同部力破解技取管理灵喜

茂放勒索病毒，是政文社搜索

windows 版本器文件被加密，且

用。为做好勒索病毒防范工

作，

内网横向传播。暴... 令... 和... 统... 特... 用... 数... 种... 供... 基...

内网横向传播。

(一) 存在暴露在互联网上

(二) 内网

(三) windows 杀毒软件。

目前我省受

二、应急处置

(一) 已感

(二) 未感

1. 将防毒墙

2. 在网络边

定IP 开放。

3. 服务器开

的高危端口。

4. 每台服务

号、特殊符号

组合以上)。

5. 及时更新

6. 安装并及

7. 服务器开

务系统下特定的机构更易于受到攻击且 windows 远端桌面服务

Android 终端。服务器使用相同或

服务器。终端未部署或未及时

病毒单位主要集中在医疗行业。

三、建议

1. 病毒的特征：下载病毒。利用特

2. 病毒的特征：

3. 针对 IDS 等设备的特征库升级直

4. 防火墙上全局关闭 3389 端口表

5. 防火墙：建议关闭 3389、445。

6. 设置唯一口令，且复杂度要求平

7. 口令位数足够

8. windows 操作系统已发布的更新和

9. 更新杀毒软件。

10. 安装日志收集功能，为安全事件

8. 不要点击不明链接、不要下载不明文件、不要打开不明文件。
9. 如有重要文件资料，请及时做好数据备份。各市、县、市及省直管县卫生计生委将相关情况及时通报所辖二级医疗机构、疾控中心或公安网部门联系解决；委直属各单位、与当地政府信息中心或公安网网页如有问题，请与委信息中心联系，联系关各处室网站电话：0551-62242387、62242395。

