

「能为 windows 远程桌面服
试多种方法获取登陆凭证并

安徽省 卫生计生委

卫传〔20

卫生计生委 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
加密文件
和应急处
一、
攻击
密码暴力破

算机勒索病毒
卫生计生委
委直
计算机勒索病毒
密码抓
并人工
包括 w
RESER
通知如
手段可
信会尝

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
取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，
VE。为做好对勒索病毒的防
下。

内网横向传播。暴露在互联网上的计算机和服务器系统。特定应用的高危端口。数字证书组合。提供基础。

- （一）存在互联网上的计算机；
- （二）内网 Windows 终端、服务器使用相同或相似 Windows 服务器，终端未部署或未及时更新杀毒软件。

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）已感染病毒的系统：
 - 1. 将防毒墙、IPS/IDS 等设备上的特征库升级到最新版本。
 - 2. 在网络边界防火墙上全局关闭 3389 端口或 3389 端口的特定 IP 开放。
 - 3. 服务器开启防火墙，建议关闭 3389、445、135 等高危端口。
 - 4. 每台服务器设置唯一口令，且复杂度要求满足混合的复杂结构，口令位数是至少 7 位以上。
 - 5. 及时更新 Windows 操作系统已发布的补丁并及时更新杀毒软件。
 - 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，为安全事件提供基础。

待系统下特征的机构更易于识别攻击端口并且 windows 远程桌面服务 (3389) 的机构；

Windows 终端、服务器使用相同或相似 Windows 服务器，终端未部署或未及时更新杀毒软件。

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）已感染病毒的系统：
 - 1. 将防毒墙、IPS/IDS 等设备上的特征库升级到最新版本。
 - 2. 在网络边界防火墙上全局关闭 3389 端口或 3389 端口的特定 IP 开放。
 - 3. 服务器开启防火墙，建议关闭 3389、445、135 等高危端口。
 - 4. 每台服务器设置唯一口令，且复杂度要求满足混合的复杂结构，口令位数是至少 7 位以上。
 - 5. 及时更新 Windows 操作系统已发布的补丁并及时更新杀毒软件。
 - 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，为安全事件提供基础。

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。

附件仅供参考，不作为法律依据。

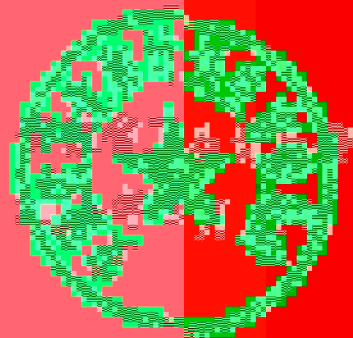
安徽省卫生健康委徽

安徽省卫生健康委信息中心网络安全中心

安徽省卫生健康委网络与信息安全处

电话：0551-62242387

电子邮箱：anws@ah.gov.cn



安徽省卫生健康委

安徽省卫生健康委

安徽省卫生健康委

安徽省卫生健康委

安徽省卫生健康委

安徽省卫生健康委

安徽省卫生健康委

安徽省卫生健康委

安徽省卫生健康委

安徽省卫生健康委

安徽省卫生健康委

安徽省卫生健康委