重庆太极实业（集团）股份有限公司文件

CHONGQING TAIJI INDUSTRY (GROUP) LIMITED COMPANY

重庆太极〔2018〕2107 号　　签发人：杨靖

关于防范 Globelmposter 勒索病毒的通知

各公司、厂：

近日，多家技术机构监测发现，利用 Globelmposter 勒索病毒发起的攻击呈上升趋势。此次 Globelmposter 勒索病毒攻击的主要方式是暴力破解 RDP 远程登录密码后，再进一步在内网横向渗透。与近期其他版本勒索病毒主要针对服务器以及数据库文件加密不同，此次爆发的 Globelmposter 勒索病毒并不区分被入侵机器是否为服务器，一旦入侵成功后直接感染。Globelmposter 勒索病毒感染安装有 Windows 系统的电脑主机后，会加密 Windows 系统中的磁盘文件，且更改被加密文件的后缀名。

请各单位加强对本单位的主机及服务器进行风险排查。对

排查发现的问题，应采取必要的整改措施，避免遭遇勒索病毒破坏之后业务系统出现严重损失。各单位若遭受攻击，应立即启动预案进行处置。

联系人及电话：朱　昊：88738006

谢岱邑：89886610

附件：处置建议

重庆太极实业（集团）股份有限公司

2018 年 11 月 26 日

重庆太极实业（集团）股份有限公司　　2018 年 11 月 28 日印发

拟稿：朱昊　　校核：谢岱邑

附件

处置建议

1、对于尚未感染 Globelmposter 勒索病毒的系统，要提前备份关键业务系统，避免遭遇勒索病毒破坏之后业务系统出现严重损失。对于已经感染该病毒的系统，建议在内网下线处理，病毒清理完毕后再重新接入网络。

2、对于内网中其他未中毒的电脑，建议使用由数字和特殊字符组合的复杂密码，避免攻击者暴力破解成功。同时，及时修复操作系统补丁，避免因漏洞导致攻击入侵事件发生。终端用户若不使用远程桌面登录服务，建议关闭。局域网内已发生勒索病毒入侵的，可暂时关闭 135、139、445 端口（暂时禁用 Server 服务），以减少远程入侵的可能。

3、各单位须根据自身实际情况，采取必要的安全手段、制定有效的管理制度，防止病毒入侵网络及设备。