尊敬的科技网用户:

您好!

近日，国内出现一款名为 CTB-Locker 的敲诈者病毒。一旦感染病毒，计算机内的文档、图片等重要资料均会被病毒加密，同时提示受害者在 96 小时内支付大笔金额赎金，否则文件将永远无法打开。目前中国科技网网络安全应急小组已经收到个别科技网用户感染该病毒的反馈。

图: CTB-Locker 敲诈者病毒要求受害者在 96 小时内交赎金

CTB-Locker 主要利用邮件传播，解压缩后是使用了传真图标的 scr 格式可执行程序， 

，对计算机用户具有较强迷惑性，目前已有用户反映遭到此病毒感染，包括 docx、pdf、xlsx、jpg 等文件均被病毒强制添加了随

机后缀名，成为加密文件而无法打开。调查发现，由于CTB-Locker要求受害者使用比特币付款，并且需要进入TOR的网络打开一个特定网址，提交序列号后才会有支付信息，一旦中招将很难找回被病毒加密的文件。

处置建议：针对 CTB-Locker 的受害者，建议可以尝试找回“以前的版本”，具体操作方法是鼠标右键点击被病毒加密的文件，选择“以前的版本”进行还原，但前提是系统必须开启了卷影复制或者Windows备份服务。

防范建议：

一、不点击陌生人发来的exe、scr等可执行程序；

二、重要数据做好日常备份；

三、及时更新安全软件防范病毒。

中国科学院计算机网络信息中心

中国科技网网络安全应急小组

(+86)010-58812935(工作日 8：00－17：00)

58812000(非工作日值班电话)

http://cert.cstnet.cn

mail:cert@cstnet.cn