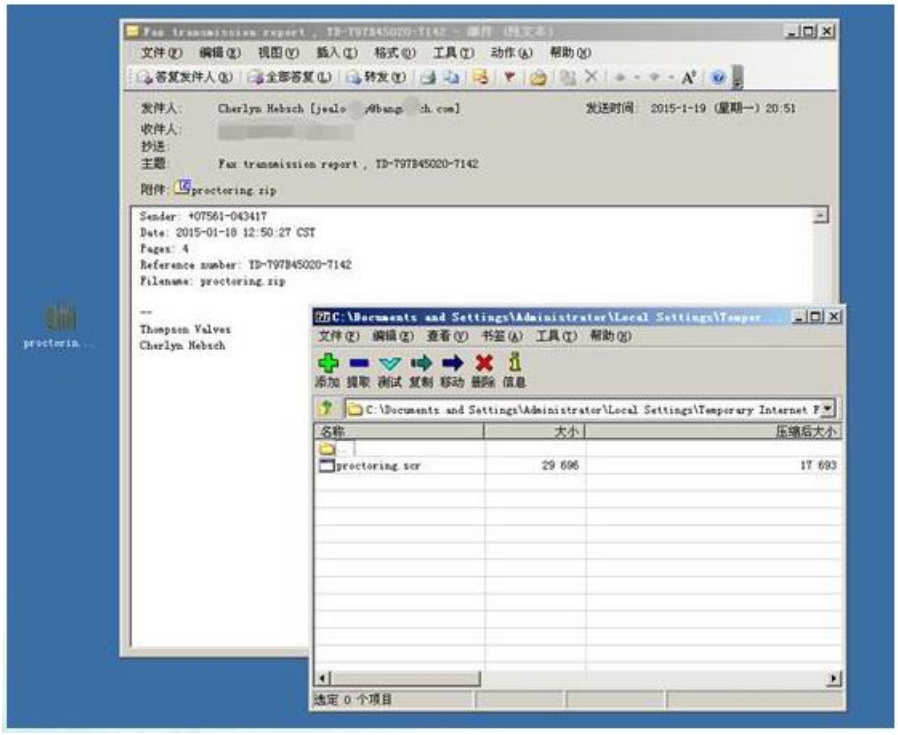
趋势科技新闻稿

[即时发布]

趋势科技安全预警：新一轮勒索软件蔓延　文件或被永久加密

[趋势科技中国]– [2015 年 1 月 21 日] 今天，全球服务器安全、虚拟化及云计算安全领导厂商趋势科技发出安全预警，新一轮勒索软件在中国开始蔓延。该病毒会伪装成邮件，病毒附件一旦被运行，用户计算机上的私人文件就会被加密导致无法打开; 如果用户不支付赎金，文件将可能永久无法解密。目前，趋势科技已经升级病毒码可对该病毒及所有变种进行拦截，并特别提醒用户不要轻易打开来源不明的邮件及附件。

据趋势科技（中国区）病毒实验室监测显示，该轮病毒会伪装成邮件附件，并随着垃圾邮件发送到用户的邮箱之中。恶意附件在点击后会打开一个 RTF 文档，文档会模仿一般的电子传真内容，让用户误以为该附件是一个正常文件。但事实上，勒索软件已经在用户打开附件之后，侵入到用户的计算机之中。



【病毒伪装成垃圾邮件的附件】

在该勒索软件感染用户计算机之后，即会在桌面显示勒索信息，警告用户如果没有在 96 小时之内支付“赎金”，计算机内的所有文件将会被永久的加密。该页面无法退出，

还会显示倒计时以强化紧迫感。如果用户点击左下角的“View”按钮，软件会列出被加密的文档，软件还具有任意恢复若干加密文件的功能，以显示其“真实”的威胁性。

【勒索软件运行后，即会在桌面显示勒索信息】

趋势科技（中国区）技术总监蔡昇钦表示：“为了降低被发现的几率，该类勒索软件会通过垃圾邮件等方式进行小规模的发送，软件不仅很难被预先发现，还使用了复杂的加密方式。我们发现，该病毒已出现大量的变种，每个用户收到的文件都是独一无二的，因此使得感染量在不断增多。鉴于病毒的快速扩展和威胁性，用户需要提高警惕。”

对于还没有感染该勒索软件的用户来说，趋势科技建议采取以下几种方式进行防护：

1. 由于病毒在进行加密操作前会访问微软系统升级官方网站，建议对以下 URL 进行暂时性的屏蔽，可有效防止计算机中文件被恶意加密：
   www.download.windowsupdate.com
2. 趋势科技最新发布的中国区病毒码已包含截止 1 月 21 日获取的所有变种，请及时更新病毒码。
3. 通过邮件网关等邮件安全产品，对附件中的.scr 文件进行拦截。
4. 不要随意点击不明来历的邮件附件。
5. 注意备份重要文件，以规避恶意软件可能带来的风险。
6. 无法访问外网的客户端，不会受该勒索软件影响。

###

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问: www.trendmicro.com.cn。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。