趋势科技安全预警：史上“最凶残”勒索木马现身网络 解密被感染文件竟需300美元！

趋势科技最新病毒码已可防护 建议用户迅速升级

[趋势科技中国]– [2013年10月31日] 勒索木马在网络上并不鲜见，其往往会感染、加密用户电脑中的文件，并向用户骗取、勒索一定的费用。可是，趋势科技最近却监测到一个“狮子大开口”的勒索木马——Crypto Locker，并贪婪地将解密修复文档的费用提到了300美元（或相应比特币）！趋势科技建议，由于该木马可能通过聊天工具、电子邮件、恶意网站传播，或由其他病毒释放而来，因此用户务必要提高警惕。目前，趋势科技最新病毒码已经可以实现对此木马的防护，建议趋势科技TDA或防毒软件的用户尽快升级到最新版本！

据了解，以往的勒索木马曾常以“警察木马”的形象出现，这类恶意软件通常会封锁系统，并将伪造的执法单位通知单传给用户，继而要求用户支付罚金。但是趋势科技此次监测到的Crypto Locker木马并不会封锁系统，其通过聊天工具、电子邮件和恶意网站等途径进行病毒传播。当用户电脑感染木马之后，桌面会出现勒索解密费用的警告通知。而且，用户即使他们从系统内删除恶意软件，加密过的文件将仍然无法使用。因此，部分重要文件被加密的用户只好汇款并获取解密的密匙。

【受感染客户会弹出以上勒索窗口】

根据趋势科技的分析，此威胁始于一个植入程序，它会植入多个文件到受影响系统上。其中，一部分文件为无害；而另一部分被植入的文件则包含了大量的数值“垃圾”字串，并且在其中隐藏了真正的恶意程序代码。

趋势科技（中国区）技术总监蔡昇钦表示：“这个病毒的特性是感染之后不会马上发作，直到连接到黑客的 C&C 服务器并拿到加密密钥之后，才会开始加密文件或锁定桌面。此病毒会持续变种，对用户的信息安全构成了较大的风险。目前，这个勒索软件还未出现中文版本，请用户要注意不要点开不明的国外邮件。”此外，**趋势科技建议用户可以执行以下几点措施以进行防范：**

1. 从网关处阻止恶意地址的连接；

2. 不要随意点开未知发送者的邮件附件；

3. 不要随意接收并运行聊天工具中发送的文件（包括看上去是图片或 office 文档的文件）；

4. 不要随意访问未知的国外站点，特别是黄色站点或是视频下载站点；

5. 重要文档请注意备份。

目前，趋势科技中国区病毒码 10.330.60 及以后的病毒码均可检测并处理该木马，趋势科技防毒软件的用户可以升级到最新病毒码以进行防范。趋势科技 TDA 的用户则可以更新网络内容检查特征码（NCIP）到 1.11971.00，这样 TDA 便能够检测到这个勒索软件病毒相关的 C&C 查询与连接活动，即使病毒本体产生变种，TDA 也能够从网络中的 C&C 活动分辨。