“勒索软件”猖獗如瘟疫蔓延　趋势科技建议“多管齐下”进行治理

黑客单次勒索金额高达 2000 元　不支付“赎金”将可能导致文件永久被锁

[趋势科技中国]– [2015 年 5 月 20 日] 近期，趋势科技在国内再次收到大量勒索软件新变种的感染报告，病毒会将自身伪装成邮件附件进行传播。邮件附件一旦被运行，用户计算机上的所有文档会被加密，用户需要按照要求支付“赎金”，否则文件将有可能永远无法打开。由于这种网络欺诈金额巨大，且防范困难，趋势科技提醒个人消费者与企业务必要留意此类威胁的演变，并采用定制化的治理策略进行化解。

勒索软件威胁巨大 传统网络安全防护手段濒临失效

作为一种有着持续影响力的欺诈手段，勒索软件在西方国家早已经“臭名昭著”，它们以“绑架（非法加密）”用户文件为手段，直接敲诈用户巨额钱财，并且这种流行“瘟疫”正从西方国家迅速扩展到国内。犯罪分子勒索的金额常常高达 600-2000 元，即使支付了这些费用，黑客也可能会进行后续的勒索，获取大量非法收益后销声匿迹。

【受害者只有支付“赎金”才能恢复文件】

一旦勒索软件进入到终端，文件被黑客加密，就几乎无法通过第三方手段进行解密。趋势科技中国区技术总监蔡昇钦指出：“犯罪份子使用了标准机制对受害者的数据进行加

密，其复杂的加密方式，几乎无法通过暴力破解等第三方解密方式进行破解，用户只能被迫支付‘赎金’，外连到黑客不断变化的 C&C 服务器才能拿到解密的密钥。“

【犯罪分子会通过加密编译器对软件进行加密】

更加可怕的是，勒索软件可以轻松绕过传统防毒软件的防线。经过对勒索软件代码的分析，趋势科技安全研究人员发现，犯罪分子使用了加密编译器对软件进行了加密，这使得很多根据静态特征码工作的防毒软件对这种病毒失效。采用多种反病毒引擎的可疑文件分析服务网站 VirusTotal 分析结果显示，在加密编译之后，网站检测到的可疑文件数量从 49 个（总数为 51 个）下降为 1 个！这意味着绝大多数经过编译后的勒索软件都无法被传统防病毒软件发现。

那么，在勒索软件不断蔓延的情况下，用户应该如何应对呢？作为全球服务器安全、虚拟化及云计算安全领导厂商，趋势科技分别针对普通消费者和企业级用户提供了有效的治理方案。

个人用户：养成良好习惯，安装云安全防毒软件

任何一个普通用户，都可能受到勒索软件的威胁，所以用户都需要养成良好的网络使用习惯。首先，不要轻易打开来陌生人的电子邮件，也不要随意点击电子邮件中的不明链接。其次，当打开邮件附件时，要注意查看附件扩展名，exe、scr 等可执行文件都具备高度的风险性，一定要谨慎下载。

另外，个人用户可以安装 PC-cillin 2015 等具备勒索软件防护功能的防护软件，阻挡勒索程序进入到终端。PC-cillin 2015 可以根据勒索软件的恶意行为，自动检测邮件和恶意网址包含的勒索软件，确保重要文件不被黑客“加密”。

针对个人用户对文档管理的“好习惯”，蔡昇钦建议：“用户最好能养成定期备份重要文件的好习惯，备份的最佳做法是采取 3-2-1 规则，即至少做三个副本，用两种不同格式保存，并将副本放在终端以外的介质上。”

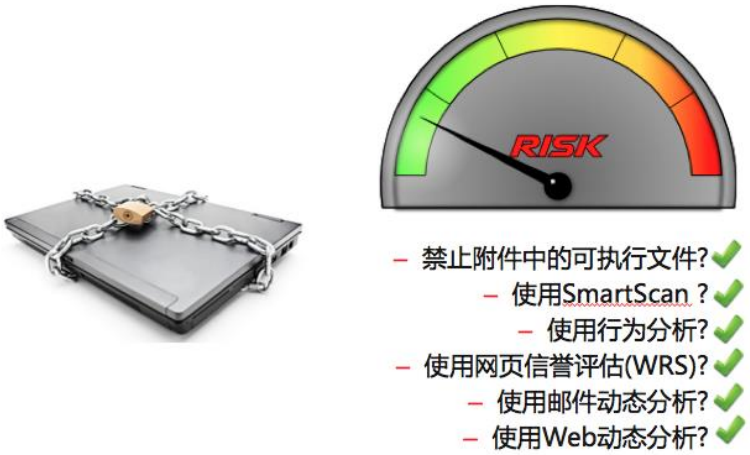
企业用户：采用定制化防御，“多管齐下”方能有效治理

勒索软件威胁的影响范围正在变得越来越大，不仅个人用户（特别是那些电脑上存储有重要文件的用户）需要加深对该类型软件的防范意识，企业用户更要有所应对，研发文档、销售数据、数据库文件一旦被加密，损失和影响都将超出您的预期。

趋势科技的研究人员发现，在地下黑客经常光顾的“地下市场”，一些勒索软件的加密编译器不但标定了不同的价码，而且还可以根据不同需要定制化的加工“加密编译器”。这样一来，几乎每个用户收到的文件都是独一无二的，这使得感染量在不断增多。另外，犯罪分子往往会将其伪装成垃圾邮件的附件发送到用户的邮箱，如果用户终端在疏于防范的企业内部，黑客很有可能会以此形成“单点突破”、发动 APT 攻击，即使企业“服软”后交付赎金，也会造成无可挽回的重要信息泄露。

对于更复杂的企业网络环境，蔡昇钦表示：“有效应对此类威胁的重要手段之一，便是采用动态的沙盒分析技术。这项技术可以克服基于特征码检测的不足之处，其运作原理可以先检查整个文件结构、寻找篡改和恶意代码注入的迹象，然后在受害者相同环境的沙盒中模拟可疑文件，以此了解勒索软件的作用域、行为和影响。”

为此，趋势科技建议企业用户采用定制化治理策略，通过趋势科技全球云安全智能防护网络（TrendMicro Smart Protection Network，SPN）或部署本地支持 SPN 的深度威胁发现平台（Deep Discovery， DD）产品，实时掌握全球各地相同的勒索软件攻击，发现勒索软件采用的 C&C 恶意链接，实现有效地侦测和阻断。其中，DD 系列中 TDA 采用了“三层式”的侦测方法，第一层是初步侦测，第二层是沙盒模拟分析，第三层是事件关联，目的就是为了发掘这种隐匿性的攻击活动。而作为定制化防护策略的重要产品之一，用户可以采用趋势科技推出的深度威胁邮件安全网关 Deep Discovery Email Inspector，检测和阻止勒索软件通过邮件途径进入到网络。



【“多管齐下”可有效降低勒索软件带来的风险】

若要防范勒索软件被 APT 攻击利用，单一的安全产品很难奏效。因此，用户还需要使用行为分析、网页信誉评估、邮件动态分析等技术来检测邮件中的未知样本，在实时监控系统中的发现恶意行为，这是有效治理的前提，更是防威胁于未然的基础。

###

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。