新闻稿

[即时发布]

亚信安全揭秘勒索软件攻击路径　并非所有企业都要“豪配”

此文内含：中小企业对付勒索软件的“经济型“方案

【亚信安全】-【2016 年 6 月 2 日】如果我是一名“狡猾”的黑客，肯定也会选择中小企业用户发动攻击，因为他们往往不会像大型企业那样部署复杂、难以进攻的安全解决方案，而且与消费者相比，中小企业网络中的资料“更值钱”，也更有能力支付赎金。

勒索软件入侵途径分析：“关门打狗”不适合

优选中小企业攻击，正是黑客选择攻击对象时的一种思路，也是通过网络安全人员“换位思考”之后得出的结论。当然，与个人用户相比，中小型企业还有更多的特点，比如：客户资料、投标文件、研发数据等，这些重要文件大多是需要实时共享的，但又不能被非法流转出去。一旦遭遇到勒索软件加密，只要勒索者对其施加心理压力，中小型企业的领导者只能乖乖就范。那么，勒索软件又是如何进入到企业内部的呢？

图：加密勒索软件入侵途径

- **第一步：**黑客利用社交工程(social engineering)诱饵，以及简历、订单和护照等作为邮件主题，发动垃圾邮件或定向式攻击。
- **第二步：**公司员工收到了这封内嵌看似正常网址的电子帐单邮件，点击链接而导致感染勒索软件。
- **第三步：**用户终端自动执行文档漏洞代码或.js 脚步，下载恶意软件主体，代码将加密用户重要的数据文件。
- **第四步：**当勒索提示信息已经弹出之后，用户几乎无法通过暴力破解等第三方解密方式进行破解，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。

对此，亚信安全 APT 安全专家白日表示：“多数加密勒索软件都具有闪避技术，部分 TorrentLockerr 变种更具备了自毁功能，而传统防毒软件更新一旦跟不上变化，就无法对已经进入内网的攻击进行拦截。另外，根据对全球网络威胁数据的持续跟踪，我们发现，90%以上的加密勒索软件事件是通过社交工程邮件方式发起的，还有少部分加密勒索软件事件是通过 Web 或其他方式导致的。因此，在网关层面进行有效拦截，将是中小企业最经济型的防御体系。”

Deep Edge 网关解决方案：“最经济”的防御体系

显然，像防范 APT 攻击那样，建立多层次、立体化的防御体系，以及构筑强大的数据灾备系统，都是最成功的防御手段。但这套“豪配”对于中小企业来说，不论是资金、人力、能力，还是网络架构调整、教育培训制度等多个方面，都显得不太现实。尤其是非 IT 行业的中小型企业，更不会有专门负责保护重要文件的专职人员，所以网络勒索案件才会频繁发生。

针对中小企业的网络安全防御特点，以及有效防范勒索软件的迫切诉求，白日建议用户部署亚信安全深度威胁安全网关 Deep Edge。他表示：“Deep Edge 具有极其简洁的部署和管理方式，但却包含了最重要的勒索软件攻击抑制能力。通侦测、分析和拦截功能的融合，可以针对加密勒索软件攻击路径，建立有效的‘抑制点’。”

亚信安全深度威胁安全网关 Deep Edge 隶属亚信安全深度威胁发现产品系列（Deep Discovery，DD），是一款基于内容检测的统一智能安全网关。它不仅提供了完整的下一代防火墙相关功能，针对 100 多种常用网络协议提供了虚拟补丁、APT 防护、零日漏洞检测、防恶意程序、恶意网站过滤、网站分类访问、VPN 数据过滤、垃圾邮件及恶意邮件过滤等多项高级内容安全检测及防护功能。更重要地是，Deep Edge 可以对勒索软件实现有的放矢。

- **针对“第一步”：**Deep Edge 具有 ERS（邮件信誉评估）功能，可以在源头拦截加密勒索邮件（防第一步）；
- **针对“第二步”：**Deep Edge 具有恶意邮件附件的侦测和拦截能力，可在.js 勒索脚本邮件到达用户终端之前予以拦截；
- **针对“第三步”：**Deep Edge 具有 WRS（Web 信誉评估）功能，可以实时拦截终端对加密勒索软件的外联网站访问；
- **针对“第四步”：**Deep Edge 具有 FRS（文件信誉评估）功能，可实时拦截终端对已知勒索软件的下载。

除此以外， Deep Edge 还内置 ATSE（高级威胁侦测引擎），能判别流量中的可疑加密勒索软件，通过外置定制化、可扩充的沙箱模拟分析平台 DDNA 进一步分析确认，拦截新型未知加密勒索软件。并且，Deep Edge 还可以和亚信安全深度威胁发现设备 TDA、联动，通过同步 TDA 分析出来的加密勒索软件 C&C 外联服务器黑名单，拦截勒索软件脚本的外联恶意通讯，并阻止勒索软件主题的下载。这些都能在“第三步、第四步”发挥重要作用。

勒索软件蔓延，“经济型”方案，兼顾成本与效能

面对勒索软件，大部分的保护措施都主要依赖于定期更新操作系统、软件和杀毒工具，然后定期备份重要数据。虽然这种方式可以有效抵御已知的勒索软件病毒，但是在面对未知的变种软件时却无能为力。而亚信安全深度威胁安全网关 Deep Edge 的部署，对于中小企业“捉襟见肘”的安全成本十分有利，不用“豪华配置”，就能部署周密的网络安全解决方案，实施侦测恶意文件、拦截垃圾邮件、封锁相关网址等技术，可谓最佳“经济型”解决方案。

##

关于亚信安全

亚信安全是亚信集团“领航产业互联网”版图中的重要业务板块，于 2015 年由亚信科技对全球最大的独立网络安全软件提供商趋势科技中国区业务进行收购重组，专注于产业互联网安全服务领域，是中国领先的云与大数据安全技术、产品、方案和服务供应商。亚信安全在中国北京和南京设有独立研发中心，拥有超过 2000 人的专业安全团队，以“护航产业互联网”为使命，以“云与大数据的安全技术领导者”为战略愿景，亚信安全坚持“产品、服务、运营三位一体”的经营模式，助力客户构建“立体化主动防御体系”，为国家提供网络安全与云产业安全保障，推动实施自主可控战略。更多关于亚信安全公司及最新产品信息，请访问: http://www.asiainfo-sec.com