“证券幽灵”恶意威胁现身　趋势科技率先预警

金融行业应做出应急响应　谨防成为韩国金融行业 APT 攻击事件的“翻版”

[趋势科技中国]– [2013 年 7 月 30 日] 近日,趋势科技 （中国区） 网络安全监测实验室（CRTL）最新监测到数起针对国内金融行业的 APT（Advanced Persistent Threat，高级持续性威胁）攻击事件。该威胁变化多端，会导致用户重要信息数据泄露。趋势科技通过检测 BKDR_CORUM 家族、TSPY_GOSME 家族、TROJ_JNCTN 家族及 China Pattern 通用检测 TROJ_GENERIC.APC 等恶意病毒，目前将此威胁命名为“证券幽灵”。趋势科技特别提醒金融行业用户需要做出应急响应，评估内部网络风险，谨防韩国金融行业 APT 攻击事件的“翻版”。

CRTL 研究表明，“证券幽灵”恶意威胁拥有了更加典型的 APT 攻击特点，瞄准银行、证券等更具攻击价值的企业网络，并主要针对 IT 管理人员的终端、域控、DNS 服务器、网络安全和业务管理软件服务器。其感染途径可以通过网络共享、或由其他病毒及被篡改后的第三方软件传播释放，但“证券幽灵”进入企业内网后不会立即大规模传播，反而会潜伏下来，并寻找其他更具价值的数字信息和替代者。

趋势科技（中国区）技术总监蔡昇钦表示：“该威胁极具‘智能’，针对金融行业 IT 管理人员和网络服务节点服务器进行攻击，并寻找网内软件的漏洞进行全网控制。由于遭受攻击的人员和服务器节点权限极大，病毒攻击的特征将被视为正常通信和授权操作，其后续可能造成的数字资产泄露危害不可估量。一旦全面触发，金融用户将面临历史上从未遭遇过的沉重打击。已经部署趋势科技 TDA 的用户，将能从威胁预警和趋势科技报告信息中第一时间发现该病毒的网络恶意通信行为和感染源。而其他企业，特别是证券和基金类公司，建议管理员应立即启动 IT 风险管理流程、有针对性的排查此次 APT 攻击释放的恶意程序代码。”

据了解，该病毒”藏匿颇深并比较狡猾，还具有：隐藏文件真正路径、为恶意 DLL 文件找“替身”、恶意软件完整性监测、伪造软件版本信息、免杀和清除日志等特性。此前，趋势科技在事前通过 TDA 的启发式侦测与沙盒动态分析提示，监测出韩国 APT 攻击相关邮件

中的恶意附件，并使用定制化防御策略，帮助趋势科技的韩国客户事先发觉并采取防护措施，成功抵挡了黑客攻击。而趋势科技 TDA 防御体系，也将会为其在国内金融用户防范 APT 过程中扮演相同的角色。

趋势科技作为全球服务器安全、虚拟化及云计算安全领导厂商，已经携手国内金融客户成功拦截多次 APT 攻击的趋势科技，帮助用户摆脱了以特征码为主的传统安全产品的局限性。而针对“证券幽灵”恶意威胁，用户也不必在后面“苦苦追赶”。**趋势科技建议：使用趋势科技防病毒客户端的客户，升级到最新病毒码，便能自动清除目前该恶意软件的所有变种。而未采用 TDA 产品和非趋势科技防病毒客户端的用户，需要针对以下关键信息进行“自查”，或者可以使用趋势科技提供的 ATTK 扫描病毒并收集信息，寻求趋势科技工程师的帮助。**

最新一轮的金融行业 APT 攻击威胁汹涌袭来，趋势科技提供的以下技术细节可以帮助用户查找“证券幽灵”存在的可能性：

一、部分特征表现

- 利用反向连接技术连接到控制服务器的 443 端口，实现后门功能；
- 使用安全软件，在目标计算机上创建用户，并打开共享，再利用远程计划任务启动；
- 通过 Winlogon 的 Notify 和 Service 方式自启动，部分变种会替换系统的 DLL；
- 在文件系统中创建 Junction，将系统 DLL 复制成和恶意 DLL 同名，用于混淆用户 ；
- 在注册表中创建 briefcase.server 的键值，用于记录状态、配置和备份信息。

二、如何判断是否受到威胁：

- 使用趋势科技 TDA 能有效发现内网中被入侵的计算机和病毒的网络行为；
- 目前我们发现感染该恶意软件的主要是金融行业的用户，特别是证券和基金公司。建议这些公司进行检查；
- 对网络流量进行分析，发现异常的网络流量，特别是非工作时间的网络访问或者周期性地访问相同的网站；
- 对内网的通讯进行分析，找到异常的端口通讯；
- 对域登录记录进行分析，找到异常的登录或者密码猜测行为；
- 如果怀疑受到威胁，建议将检查重心放在服务器网段和对服务器有管理权限的 IT 人员。特别是域控、文件服务器、安全软件服务器等；
- 检查计算机是否存在 HKCR\Briefcase.server 注册表项目；
- 检查系统中是否有被重命名的系统文件，是否有异常的 reparse point 到 System32 目录。