天津银行携手趋势科技守护邮件安全　DDEI 沙箱技术斩断 APT 攻击入口

天津银行在业务模式向着纵深化、多元化发展的同时，为了保障业务系统与核心数据的安全，决定采用先进的网络安全技术防范新型网络攻击。为此，天津银行针对高级持续性威胁（Advanced Persistent Threat，APT）的特殊性，采用了趋势科技最新推出的深度威胁邮件安全网关 DDEI，发挥了业内领先的沙箱分析技术和全球云安全网络评估技术，实时检测并有效阻止了定向工程邮件导致的数据泄漏事件发生。

APT 攻击正在蔓延，天津银行选择“主动”应对

近年来，天津银行的业务领域持续创新，建立了集融资、结算、理财、咨询等为一体的综合性金融服务体系，尤其是在小微企业金融服务方面更抢先试水，并取得了预期效益。随着数据大集中、新一代银行、移动互联网、云计算等创新技术被更深入地结合到金融业务流程之中，如何保障业务系统与核心数据的安全，如何利用先进的网络安全技术防范最新的网络攻击，成为了天津银行信息安全管理的重点工作。

“当前，全球每天平均新增恶意程序有 200,000 个，算下来，每秒就产生 1.3 个。另外，国外几起针对金融行业的 APT 攻击案件给我们敲响了警钟。考虑到这些，我行技术人员在深入研究 APT 攻击原理的同时，开始重新评估网络中的弱点，并且着手建立能够与之对抗的解决方案。”天津银行技术工程师说到。

金融行业对信息网络的依赖‘形同鱼水’，但在当下的互联网应用环境中安全漏洞和防护弱点层出不穷。那么，在随后的网络安全评估工作，天津银行是否找到了答案？

高级恶意邮件准备“潜伏”，趋势科技出手相助

天津银行的技术人员通过对 APT 攻击的步骤和途径研究发现，在被媒体披露的 APT 攻击案件中，有超过 90%的 APT 攻击利用了社交工程钓鱼邮件。而在内部评估工作中，也证明了钓鱼邮件正在威胁着天津银行的网络和数据安全。

对此，天津银行相关技术负责人表示：“高级恶意邮件给我行带来比较严重的困扰，为此我行与趋势科技的工程师一起对网络数据进行缜密分析，发现有大量的威胁正在通过邮件这种媒介，准备悄然无息地进入网络。另外，今年大规模爆发的‘加密勒索软件’事件，更督促着我行的邮件及数据安全需要更高的防护能力。为此，我行高度重视 APT 攻击可能带来的后续影响，决定从邮件安全管理入手，建立风险防范的抑制点。”

据了解，趋势科技与天津银行在长期合作中，通过定制化的威胁解决方案、先进的云安全防护产品，不断满足着用户需求的变化，其技术创新和售后服务都得到了用户的认可。而针对这次高级恶意邮件的分析工作，不仅对邮件本身，还包括了内嵌的文档、URL、IP、域名以及后续行为等可疑对象进行检查，由此发现了传统邮件安全产品无法识别到的网络攻击。趋势科技通过定制化的虚拟沙箱对这些可疑对象进一步分析，最终发现了深度伪装的恶意代码和 C&C 通讯，最终确认新型威胁，为天津银行制定应对措施提供了依据。

针对这种情况，趋势科技为天津银行推荐了一套完整的邮件安全和 APT 防御解决方案，其中一款产品便是最新推出的趋势科技深度威胁邮件安全网关 DDEI。而在随后的测试环节，DDEI 显示出了“过人之处”，并最终成为了天津银行新一代邮件安全系统的核心。

天津银行技术工程师表示：“通过一段时间的测试发现，与其他厂商同类产品通过匹配特征库等方式识别垃圾邮件、病毒邮件相比，趋势科技的邮件安全解决方案更完整、更有效、更先进。不仅对垃圾邮件、病毒邮件进行特征的比对处理，还拥有 DDEI 先进的恶意软件检测引擎，包括了邮件附件分析、文件漏洞检测、嵌入式 URL 分析、智能文件解密以及定制化沙箱技术，这有效地阻止了传统邮件安全或终端安全产品无法检测的社交工程钓鱼邮件、定向攻击、Web 威胁、病毒、间谍软件、木马后门等高级未知恶意威胁，为我们邮件的安全和 APT 攻击防御、数据防泄露提供了可靠保障。”

“两个第一”，专为 APT 防御打造

据了解，趋势科技高级威胁邮件安全网关 DDEI 是目前国内首款针对 APT 攻击的邮件类安全网关。虽然 DDEI 在全球金融领域的成功案例很多，但天津银行却是国内第一家采用 APT 邮件防御产品的金融机构。那么，“两个第一”加在一起的效果如何呢？

从功能来看，DDEI 能够帮助天津银行的网络安全监控人员检查所有邮件及附件安全，可侦测高级恶意软件与文件漏洞攻击，可涵盖各种文件类型与内容，包括：各类 Windows 执行文件、 Microsoft Office 文件、PDF、Zip、Java、网站内容以及压缩文件。

从能力来看，作为国内第一家部署该产品的银行机构，除了在内部采用网络沙箱的智能化分析，对来自 Web 的内容和电子邮件流量进行分析，天津银行还借助趋势科技云安全智能防护网络（SPN）和大数据威胁分析情报，与云端的全球威胁库比对和共享威胁。

从效果来看，天津银行相关技术人员表示："之前我行员工经常受到垃圾邮件的困扰，在部署了传统的垃圾邮件网关后，虽然垃圾邮件数量减少，但时常还会有用户抱怨电脑受到勒索软件和邮件中的恶意 URL 攻击。之后我们部署趋势科技的 DDEI 设备，通过其定制化沙箱技术，对邮件中存在的恶意附件和 URL 可以有效地进行检测和拦截，大大减少了被感染的机率，减轻了管理员的维护压力。最重要的一点是，当 APT 攻击已经成为金融行业安全难题的时候，我们选择了主动应对，从攻击入口建立了有效的抑制点。"

###

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。