# 网络安全如何 Hold 住？主动发现威胁才有控制力

——趋势科技 TDA 在天津港成功抵御内网威胁攻击

天津港的现代化水平可以和很多世界级的口岸一争高下，通过广泛采用新技术、新装备、新工艺，天津港的港口现代化、信息化程度在全国港口中位居前列。天津港在促进“电子口岸”逐步形成的过程中，为客户提供了快捷、高效网络技术服务。而随着网络规模的不断扩大，业务系统的安全保障以及大量终端系统对于病毒威胁的防御工作，已经成为了 IT 部门的重点工作。

**“谍影重重”让内网安全管理遭遇瓶颈**

天津港主要负责天津港集团众多单位的 IT 系统建设和业务系统维护工作，集团共有两万多员工，终端数量超过了 2000 台。在网络规模不断壮大的过程中，物流系统、人事管理系统、调度系统以及内部公文流转系统的访问常常出现问题。经过排查，这些 IT 故障的发生多是由于终端系统的木马病毒和恶意软件造成，而一些顽固的病毒也在内部的网络中变换其攻击手段，造成了业务系统访问带宽被占用，非法流量拥堵出口的情况出现。

据天津港郭经理介绍：“为确保各个业务系统的稳定运行，IT 部门在各个服务器区、各办公区都设置了防火墙和 IPS 等安全控制设备。但这些设备对于应用层的检测功能比较弱，一些 Web 站点的木马病毒常常感染客户端系统。再加上一些终端存在应用层漏洞，例如 Office、Flash 插件、视频播放器等，这些漏洞的存在都可能让病毒的制造者偷偷地在目标电脑上执行恶意软件，最终获得电脑的控制权，并且取得网络内部的敏感资料。针对这些威胁，传统安全设备无法参与整体安全防护中，当然，最大的难点是这 2000 多台终端无法断定产生攻击的源头，定位相当困难。”

面对时刻变化的威胁攻击，天津港希望建设一套更完善、更主动、更智能的安全防御体系。实际上，在利用趋势科技提供的硬件病毒网络设备 NVW 和 OfficeScan 终端防毒软件之后，已经获取良好的投资收益。在此基础上，IT 部门评估并借鉴了趋势科技对于威胁管理解决方案中的全套对策，在多层次安全策略上增加威胁发现层，进一步把拦截、检测和遏制的各种方式组合起来。

**第一时间消除威胁　报表功能发挥特性**

通过缜密的分析和试用，以及长期以来对趋势科技 NVW 和 OfficeScan 产品的使用效果评估，在解决各个子网和终端安全的基础上，IT 部门在网络层面选择了威胁发现设备（Threat Discovery Appliance-简称 TDA）。由于集成了趋势科技“云安全”技术，TDA 全面检测和定位 2~7 层的恶意威胁，并通过威胁报表、邮件通知、专家建议等详尽功能，让天津港的网络安全管理水平得到了进一步的提升。

据了解，在部署 TDA 之前，IT 工程师都只能通过终端用户上报异常故障，才能发现已经遭遇病毒入侵的情况。并且，由于大部分终端的网络共享机制存在，一旦遭遇 Web 网站上的恶意代码、木马、邮件病毒、移动设备病毒，随时有可能造成交叉感染。而在部署 TDA 之后，发生在内网中每一次 Web 攻击、木马入侵、病毒攻击点和高危网络通讯行为都在第一时间得到解决，这也就杜绝了因为终端设备感染病毒，产生非法流量对服务器区的冲击。

据郭经理介绍，在正式部署 TDA 的半年里，管理人员都可以在第一时间知道是哪些恶意代码进入了网络。同时，对于隐藏在网络角落中的病毒变种，都可以通过流量报表和告警功能一一将他们“揪出来”。他指出， TDA 的优势在于其详细的报表功能。例如，通过报表的形式显示客户端即时通讯（IM）、P2P 文件共享（BT）、流媒体，以及未授权服务如 SMTP 中继和 DNS 欺骗现象，这些都可以直接连接到趋势科技的云安全中心，接收到“安全策略执行建议”的反馈信息，网络管理员此时就可以在发现威胁之后“有所作为”，将威胁发现转化为详细的处理措施。

**TDA 将有效帮助企业预警 APT**

对于虚拟化防毒安全以及最新火热的 APT 威胁攻击，天津港希望与趋势科技取得更加紧密的联系和培训。“学习”依旧是治理好企业网络环境安全的关键，郭经理表示，如何吸收并利用最新的防御技术，来完善企业中的虚拟化建设，如何深度挖掘网络安全设备的监视功能，实时发现攻击者所释放恶意代码的每一个细节，这两项任务将列为近期的工作要点。

根据郭经理的建议，对于大型企业的 IT 管理部门都非常有借鉴意义。一般认为，高级持续威胁（APT）只是针对政府或者大型的商业机构，但现在有研究表明，黑客对于一些企业的网络攻击都开始朝这这一方向变迁。而 APT 攻击手法重点在于“低调且缓慢”，黑客如何在不引起人注意的前提下，利用各种复杂的工具与手法，包括应用各种社交工程和在系统内植入木马程序等方式，在不被发现的前提下，能够长期隐藏下去，因此很难发现。

同样，趋势科技最近的研究中表明，一些恶意软件虽然采用了持续性攻击的设计，但利用好 TDA 和其他安全产品的功能关联，可以有效地预防此类攻击。例如，APT 的防范不能只针对一次攻击就下结论，因此从 TDA 的周报、月报中分析这些长期攻击的趋势和变化，形成“持续性观察”。还比如，企业可以用 TDA 发现恶意软件进行通讯时的特征，然后追踪到是哪些终端出现了问题，同时利用 OfficeScan 发现是那个系统文件被恶意软件给感染了，等等。

很显然地，企业信息安全威胁环境变得越来越具有挑战性。对于信息系统进行攻击的动机和方法正在发生变化，有决心有毅力的攻击者正运用着多种手段去打破安全控制。企业需要通过多种安全控管来做应对，包括实时监控和快速遏制措施等等。但你仍然需要坚信：“在较量中，上帝总是会关照那些做好准备的人。”