网络威胁不断演化　趋势科技建议：抑制 APT 攻击防范数据“吸血鬼”

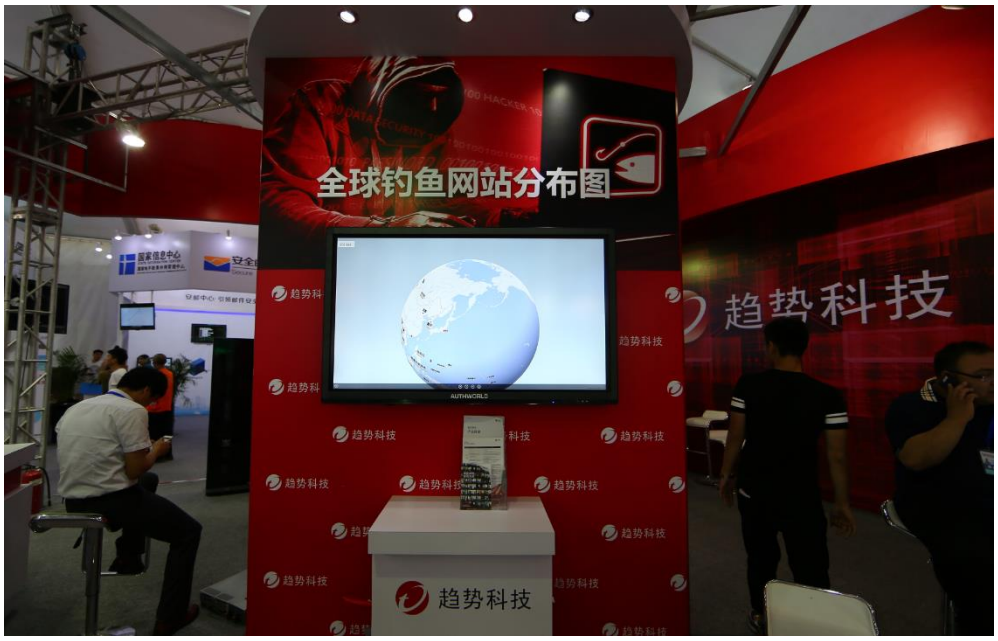
[趋势科技中国]– [2015 年 6 月 8 日] 近日 趋势科技在第二届“国家网络安全宣传周”活动中，正确引导青少年安全用网、健康用网的同时，结合宣传周的主题日，对金融、电信、政务等行业面对的网络威胁演化进行了全面展示。针对用户当前无法有效发现与阻拦 APT（高级持续性威胁）攻击的状况，趋势科技提出“知己知彼，百战不殆”的观点，详细揭秘 APT 攻击过程，并建议企业和政府用户采用定制化的解决方案建立 APT 攻击“抑制点”，确保数据安全。

万物互联，APT 攻击“入口”成倍增长

据统计，在现实世界中存在的 250 亿个物联终端，70%都存在安全漏洞，且平均每台设备上的漏洞数高达 25 个。这些设备在信息世界担任重要角色，必将会成为互联网+时代下政务、金融、电信、医疗等关键行业融合创新的有力支点。但随着网络威胁的持续演化，若掉以轻心，它们便会沦为 APT 攻击的跳板，成为用户安全防御系统的“阿喀琉斯之踵”。其中，美国连锁超市 TARGET 泄密的案例就告诉我们，随着万物互联，不仅仅是 POS 机，其它智能设备也很有可能被病毒入侵。

在趋势科技发布的《2014 年全球 APT 发展趋势报告》中指出，APT 攻击主要目的都是为了搜集情报和窃取机密信息，但有 7 成的 APT 攻击对象锁定在政府行业用户。另外，在移动支付、云计算、大数据这些全新应用环境下，数以亿计的恶意程序、成熟的地下黑色产业链、防不胜防的 APT 攻击，都如“吸血鬼”一样盯上金融、电信、医疗领域。而在这些行业中储存的公众数据、隐私数据相对集中，一旦遭遇 APT 攻击、产生数据泄露，影响范围将会极其巨大。

对此，趋势科技(中国区)业务发展总监童宁认为：“各地银行的 ATM 自助机、电信营业网点中的终端机，或是医疗行业中的智能设备，存在着操作系统服务过期、漏洞修补不及时、安全防护缺失的高危风险。另外，由于业务系统横向联系增多，数据交换过程更加频繁，一直处在‘旅行’状态的数据，一旦防护系统入口被打开，极有可能被黑客利用。因此，网络安全管理人员应该全面掌握 APT 攻击过程的全貌，做到知己知彼，借助先进的侦测与分析技术，形成针对强的定制化策略。”



【趋势科技在安全周现场设立了“炫酷”的全球钓鱼网站分布图】

拦截社交钓鱼攻击，侦测是第一步

在本届宣传周的展示环节，趋势科技在“钓鱼诈骗威胁体验区”中新设立了“炫酷”的全球钓鱼网站分布图，观众可以通过触摸屏自行旋转虚拟“地球”，直观地查看任意一个国家最新的钓鱼网站威胁的监测数据。而 APT 攻击的主要手法就包括了钓鱼网站、电子邮件、即时通信软件、社交网络或是应用程序漏洞，从而找到进入目标网络的大门。

针对网络钓鱼和 APT 攻击之间的联系，童宁表示：“APT 攻击全貌包括情报收集、单点突破、命令与控制 （C&C 通信）、横向移动、资料发掘、资料窃取共六个阶段。钓鱼攻击处在 APT 攻击的第二阶段，也是用户防范的关键所在。为此，我们建议用户建立侦测体系，采用定制化的治理策略，部署相关的威胁治理产品。全面掌握黑客的手段，对应的建立抑制点，才能做到‘知己知彼，百战不殆’。”

侦测是 APT 治理的“神经系统”，这是指企业能够在第一时间侦测到 APT 攻击者采用的恶意软件、通信以及行为等威胁。但 APT 攻击的侦测不同以往，尤其是针对政府、金融、电信、医疗卫生这些安全防护水平相对较高的行业用户，攻击者会在每次攻击时利用高度定制化的恶意程序或零日攻击恶意程序，有些感染事件可能只会出现“1”次。因此，侦测的目的在于必须对文档、URL、IP、域以及行为等可疑对象进行检查，所以利用趋势科技全球威胁情报分析系统、深度威胁发现平台（Deep Discovery， DD），清晰的侦测出 APT 攻击迹象，使预防达到“有的放矢”的目标。

防范 APT 攻击，保护公众隐私

一旦被 APT 攻击事件缠身，核心数据泄密，势必造成知识产权的流失，将在技术、业务、市场、客户等方面发生连锁反应，侵蚀企业的市场价值，这会影响企业发展战略目标的实现。但同时，企业和政府防范 APT 攻击防御意义更在于确保普通用户的隐私信息，不让普通消费者和家庭遭受到了经济损失。

因此，在公众信息安全保护方面，童宁还建议肩负社会责任的企业部署互联网反钓鱼侦测系统，他说：“互联网反钓鱼侦测服务采用了主动发现的方式，这可以帮助企业用户发现仿冒自己的网站，高效截取黑客对公众投放的钓鱼网页、手机银行钓鱼网站。用行动保护好自己，才是对公众负责的最佳表现。”

###

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。