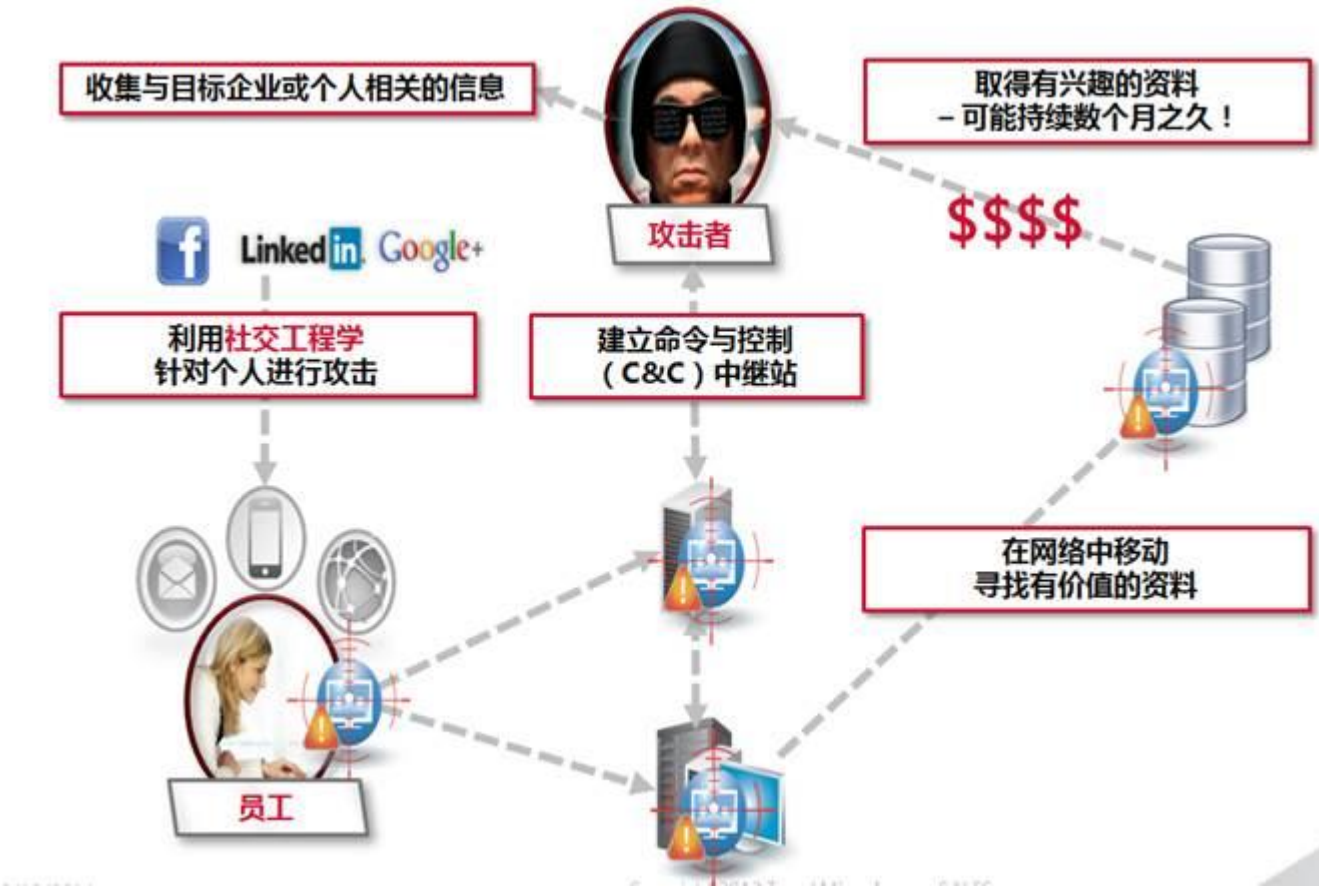
云南无线电管理机构携手趋势科技提高 APT 攻击“免疫力”

高级持续性威胁（Advanced Persistent Threat，APT）已成为最令企业和政府行业用户担心的危险，如今你可以在每一篇网络安全分析报告中都能发现它的“大名”。为了积极有效地应愈演愈烈的 APT 攻击，云南无线电管理机构与全球服务器安全、虚拟化安全及云安全领导厂商趋势科技达成深度合作，采用多层次、全方位的安全加固解决方案以及 TDA、NVWE 等云安全产品，全面提升了网络边界防范和威胁预警的能力，在符合等级保护等政策要求的基础上为政府行业用户塑造了安全管理的典范。

传统安全防护方案难以抵御 APT 攻击

APT 攻击的背后一般都是优秀技术、资金资源的黑客组织或集团，他们对某些特定的用户发起的有目的、长时间的攻击。由于其攻击前期的准备非常充足且攻击时间、次数相对于传统攻击更多，因此发起的攻击往往无法彻底防御。例如：2013 年两起针对韩国政府的 APT 攻击、国内针对金融业的“证券幽灵”等安全事件，都充分反映了 APT 这种特殊攻击的特点。作为国内政治敏感度最高的行业，政府单位历来都是黑客首选的攻击目标。最近两年，在我国政府行业发生的多起安全事件，充分证明网络安全建设已日益成为政府单位形象及社会稳定的关键。

2009 年，云南省无线电管理行政职能划入到云南省工业和信息化委员会，并成立了云南省无线电管理办公室，负责该省无线电系统建立和管理工作。2013 年，针对 APT 攻击日趋严重的网络环境，包括国家计算机病毒应急中心等多家部委级单位发文，要求政府单位做好抵御 APT 的安全工作。对于云南无线电管理机构的安全管理工作来讲，既要符合上级单位规定要求，更需要提升自身网络的威胁防范能力，那么就必须对分散在全省各分支机构的终端提供实时的威胁管理。但由于国内由于云南省无线电管理机构日常办公经常使用 U 盘等外设，同时又与云南省信息中心这个政府大网有各种数据互通，非常容易遭受到 APT 的攻击。而单纯的网络版防毒软件根本无法从 APT 攻击流程（图 1 所示）中发现和拦截危险，安全建设工作难以展开。



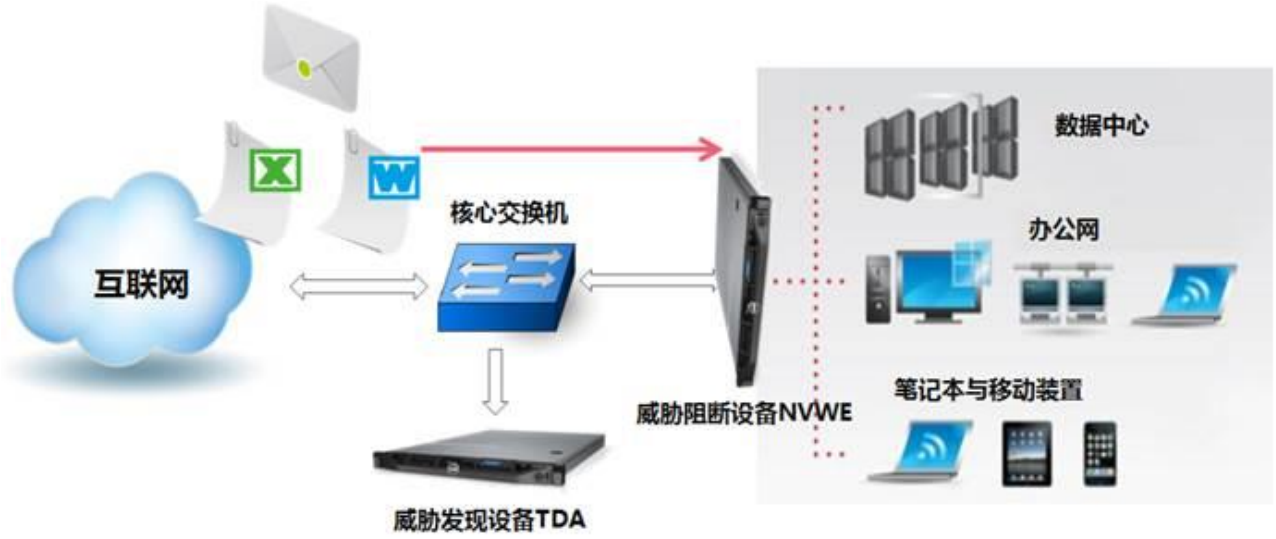
【图 1：典型 APT 性攻击流程】

结合上述需求，云南无线电管理机构决定对整体安全架构进行全面的加固，提升自身对 APT 的防御及监控能力。为此，云南无线电管理机构与多家国内外知名的安全厂家进行了长时间的技术交流及产品测试。最后，趋势科技凭借其解决方案最为符合云南无线电管理机构需求、以及在全国多个大型政府单位有丰富安全服务经验的特点，成为本次安全加固项目的实施服务商。

围绕 APT 威胁构建“发现”和“阻断”方案

结合云南无线电管理机构现有的安全架构，趋势科技采用了一套从网关到网络的全方位、多层次的 APT 疫情监控及阻断体系（如图 2 所示）。

- 威胁发现层：在全网关键边界部署趋势科技威胁发现设备 TDA，对网络中流窜的数据进行深度分析，一旦发现威胁，立刻通过控制台为用户提供预警，并配合趋势科技 EOG 服务对分布在全省各地的威胁源头进行处理。
- 威胁阻断层：为起到实时的 APT 阻断效果，在全网关键的网络边界桥接处部署趋势科技威胁阻断设备 NVWE。一旦 TDA 发现有 APT 行为出现，立刻联动 NVWE 对 APT 有害的网络行为进行实时阻断，最大限度降低 APT 的损害。



【图 2：趋势科技威胁发现和阻断方案】

据云南无线电管理机构的安全管理专责工程师陈工介绍：APT 就如疾病一样，无法彻底杜绝，能够做到“提前发现、快速修复”就是我们本次项目的目标。之所以选择趋势科技作为本次安全项目的合作伙伴，主要看重了趋势科技两方面的优势。一是趋势科技领先于业界的“云安全”技术，另一个则是趋势科技提供优质的原厂高级服务。趋势科技“云安全”技术和产品都是全球最领先的，在方案调研阶段及产品测试阶段，就已经收到了良好的效果，能够快速、准确地发现来自外界的可疑 APT 攻击并提供简单、直接的告警提示。

增强自身免疫力方可远离 APT 攻击

如今，通过使用趋势科技最新的全方位、多层次的 APT 疫情监控及阻断体系，云南无线电管理机构能够实时发现并阻断全网范围内所有的 APT 威胁事件，并能够通过趋势科技提供的原厂高级服务，快速消除 APT 威胁对云南无线电管理机构的影响。

陈工认为：“目前大部分政府单位所使用的网络防病毒系统+防火墙方案，根本无法抵御这些 APT 的攻击。必须建立一套全方位、多层次的 APT 疫情监控及阻断体系，才能保障政府单位的安全运作。而趋势科技的 APT 疫情监控及阻断体系，能够为政府单位从网关到网络提供一整套的 APT 攻击防护体系，从而全方位地监控到 APT 威胁在政府单位内部的发展情况，进而有效协助政府单位抵御 APT 攻击，为政府单位的工作顺利开展保驾护航！”