趋势科技发布演化的 APT 治理战略

业界首发 APT 整体解决方案白皮书 支撑“3C”战略打造零风险世界

[趋势科技中国]– [2015 年 6 月 24 日] 在不断演化的网络安全领域，会出现比高级持续性威胁（Advanced Persistent Threat，APT）更具挑战性的对手，但现在所做的事情，就是要改变。今日，全球服务器安全、虚拟化及云计算安全领导厂商趋势科技发布了演化的 APT 治理战略，以 1 个中心、4 个过程、6 个抑制点为基础，形成了“螺旋迭代”的立体化治理模式即每经历一个迭代周期，防护体系具备更强的防御治理能力。

作为趋势科技全力打造零风险网络世界的核心，趋势科技发布了业内第一份针对 APT 攻击防御治理整体解决方案的技术白皮书——《演化的 APT 治理战略》，将为“3C 理论”提供重要的技术、产品以及解决方案支撑并且有利于帮助企业用户消除数据泄露“常态化”的危险现状。

“3C 理论”旨在打造来零风险的网络世界

近年来，不论是企业级用户，还是普通的消费者，在享受 IT 技术创新带来的益处之外，也遭遇了前所未有的安全风险。黑客利用各种途径获取用户隐私信息早已不是秘密，而针对各类企业、政府及组织机构的 APT 攻击也广泛出现，涉及业务机密甚至是国家安全的数据泄露风险正在加大，以经济、商业及政治为目的的 APT 攻击正逐步显露其强大的负面影响。

IDC 最新的安全报告中显示：“大数据将会是整个 IT 安全行业发生重大转变的驱动因素，并将推动智能的信息安全模型的出现。针对防御 APT 攻击这个炙手可热的话题，越来越多的安全厂商在技术手段上更加注重检测/侦测技术，以数据为中心进行智能分析来检测威胁、分析威胁。”

对此，趋势科技(中国区)业务发展总监童宁表示：“趋势科技在 2012 年提出了覆盖‘3C 领域’的战略布局，这包括：云安全（Cloud And Data Center Security）、全面的用

户防护（Complete User Protection）、面向针对性攻击的定制化智能防御（Custom Defense From Targeted Attacks），旨在帮助客户应对 APT 高级持续性威胁、移动终端及更多的外围设备在云安全时代面临的挑战。如今，作为信息安全厂商，必须针对威胁的数量、变化和速度，寻找解决方案，为此趋势科技携手各方力量、加速跨界融合，全面实现了内外部安全产品联动机制，以帮助用户应对今天和未来的威胁变化。”

【趋势科技(中国区)业务发展总监童宁】

历经 3 年发展，趋势科技向着“打造一个交换数字信息零风险的世界”的企业愿景目标不断前进。在云安全领域，提出了以 Deep Security 为核心的无代理虚拟化安全解决方案，并持续保持着云安全全球第一的领先地位。在全面的用户防护部分，趋势科技的 PC-cillin 、OfficeScan、SMW 安全移动办公软件等安全软件已经成为了业界第一的全平台终端防护体系。在面向 APT 攻击的定制化智能防御部分，趋势科技提出了多维度深度收集系统和以大数据技术为核心智能分析系统，而在本次活动中发布的演化的 APT 治理战略正是 3C 战略发展的重要技术组成部分。

改变从“演化的 APT 治理战略”开始

趋势科技产品经理林依莹介绍：“APT 攻击是一种高级的、狡猾的伎俩，高级黑客可以利用 APT 入侵网络、逃避‘追捕’、随心所欲对相关数据进行长期访问，最终挖掘到想要的信息。而一旦被 APT 攻击事件缠身，核心数据泄密之后，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，造成了意想不到的成本影响和连带风险，更会影响到 CEO、CIO、CTO 等人的职业发展。”

【趋势科技产品经理林依莹】

为了改变网络风险失控的现状，趋势科技提出了“演化的 APT 治理战略”，这包括：1 个中心、4 个过程、6 个抑制点。即：“监控”为中心，实现威胁可视化、策略下发、以及威胁情报共享；“侦测、分析、响应、阻止”为 4 个治理过程，贯穿整个 APT 治理的生命周期；对应 APT 攻击过程的 6 个阶段分别建立抑制点，实现针对性极强的防御。

【演化的 APT 治理战略中“侦测、分析、响应、阻止”的 4 个治理过程】

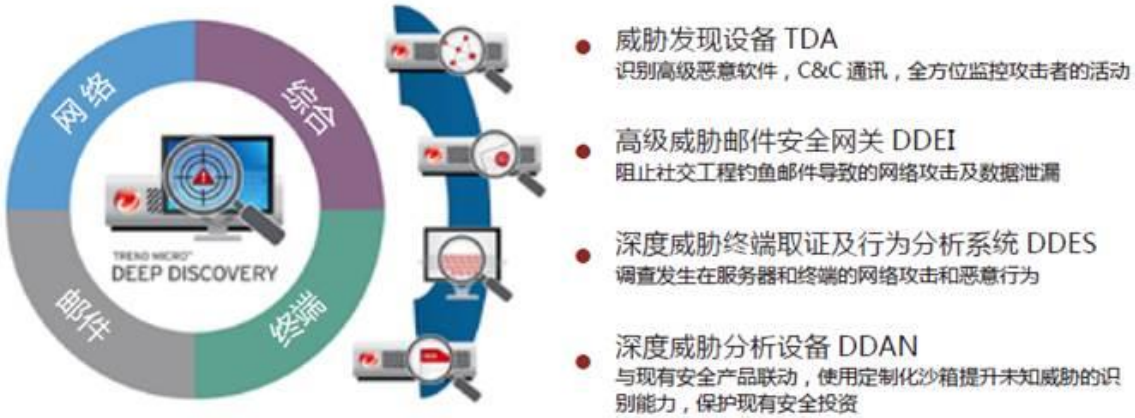
趋势科技产品经理白日表示：“演化的 APT 治理战略中所阐述的观点，是一种‘螺旋迭代’的立体化治理模式，每经历一个迭代周期，防护体系将具备更强的防御治理能力。另外，演化的 APT 治理战略包括的具体落地方案，通过趋势科技控制管理中心（TrendMicro Control Manager，TMCM）整个企业提供全方位智能的安全管控，它紧密整合了趋势科技云安全智能防护网络(TrendMicro Smart Protection Network，SPN）全球威胁情报分析系统、趋势科技深度威胁发现平台（Deep Discovery，DD）

的威胁侦测和分析能力。用户可以将 DD 系列产品部署在各层网络节点，构成安全联动的防护体系，配合最高等级的趋势科技 APT 治理专属咨询服务(TrendMicro Premium Support Program，PSP）从而达到有效治理 APT 的目标。”

【趋势科技产品经理白日】

趋势科技深度威胁发现平台（Deep Discovery 系列）全面进入中国市场

建立“抑制点”是治理 APT 攻击的关键所在，为此趋势科技在本次活动中重点介绍了深度威胁发现平台（Deep Discovery 产品系列）的全面性、有效性、开放性等特点，以及与云安全智能防护网络（SPN）、控制管理中心（TMCM）联动治理 APT 的具体方法。



【趋势科技深度威胁发现平台（Deep Discovery）】

趋势科技深度威胁发现平台(Deep Discovery)核心产品构成包括 :威胁发现设备 TDA、高级威胁邮件安全网关 DDEI、深度威胁终端取证及行为分析系统 DDES、深度威胁分析设备 DDAN，该平台能与趋势科技网络网关、服务器与终端、云和虚拟化安全产品以及第三方安全产品整合，构建完整的 APT 治理体系。在第三方安全产品整合与功能联动方面，趋势科技与 HP、IBM、Blue Coat、Palo Alto、HillStone（山石网科）已通过该平台取得了预期的合作效果。

3C 领域战略的前瞻性 ,使得趋势科技在 APT 治理领域的解决方案已经覆盖了整个 APT 攻击的生命周期，利用深度威胁发现平台（Deep Discovery），用户可在 APT 攻击的不同阶段抑制 APT 攻击可能产生的影响，保护企业核心资产免受伤害。据统计，在全球 50 大企业当中，有 48 家都信赖趋势科技的解决方案。

###

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。

趋势科技《演化的 APT 治理战略》免费下载