[趋势科技新闻稿]

趋势科技推出 Smart Protection Strategy 智慧防护策略，主打“定制化智能防御战略”、“使用者全方位防护策略”以及“云端防护策略”

在高级持续性威胁逐渐兴起的情况下，企业应重新定义自己的防护策略

【趋势科技中国】– 【2013 年 4 月 9 日 新加坡讯】随着网关安全防御和传统安全防护越来越无法应付高级持续性威胁攻击（APT），全球服务器安全、虚拟化及云计算安全领导厂商趋势科技今天正式发布 **Smart Protection Strategy 智慧防护策略**来协助企业重新定义自己的安全策略，以应付日渐精密、隐匿、难缠的网络威胁。这套策略提出了全新的解决方案概念，涵盖三大主要领域：**第一、针对定制化锁定目标攻击的定制化智能防御战略；第二、针对当前 BYOD 时代的用户信息交换实现全方位防护；第三、专为数据中心而优化的云端防护。**

趋势科技全球 CEO 陈怡桦 表示：“在当前不断演变的威胁形势中，企业需强化自身的业务连续能力，才能在亚洲这个经济蓬勃发展的区域拥有最大的成长契机。当前的问题已不再是企业会不会发生安全事件，而是何时将会发生，因为网络犯罪者的手段越来越高明，越来越难缠、越来越隐匿。歹徒现在非常擅长针对企业机构当中的特定人员、系统及漏洞来发展出定制化的攻击。鱼叉式网络钓鱼邮件依然是歹徒传送恶意软件的主要媒介，同时并搭配各式各样的手法及工具（包括远程访问木马程序）来发动隐匿的攻击并且持续躲藏在您的企业之内。”

[图示：趋势科技全球 CEO 陈怡桦]

专门对付锁定目标网络攻击的定制化智能防御战略

根据最近一项针对亚太地区 1000 多位 IT 专业人员及主管的调查显示[1] ,IT 最担心的威胁是数据泄露，有将近一半的受访者认为这是一项严重问题。然而，同一份调查也指出，目前信息安全最主要的投资仍旧是防毒与恶意软件防护，其次是数据泄露防护。该报告表示，整体来说，高级持续性威胁攻击（APT）或锁定目标攻击在该地区并未受到重视，或者被视为优先级较低。

趋势科技全球技术及解决方案总监 JD Sherry 指出：“这项调查突显出企业安全意识教育在亚太区的必要性，因为一项普遍的误解认为只要能提升病毒防护能力就能解决问题。对抗与降低锁定目标攻击的风险并非单一产品或单一技术所能解决，没有所谓的林丹妙药，定制化的攻击需要定制化的智能防御。趋势科技是唯一能对付高级持续性威胁攻击（APT）的主要信息安全厂商，客户有权要求自己所购买的防护产品应该提升潜在威胁的侦测能力，给他们采取反制行动所需要的情报。”

[图示：趋势科技全球技术与解决方案总监 JD Sherry 做“全球云时代的网络防御“演讲]

企业必须采用一套新的方法来侦测并分析高级持续性威胁攻击（APT），并且快速调整其安全管理策略来对付攻击者。趋势科技的“定制化智能防御战略策略”（Custom Defense Strategy） 整合了解决方案、全球威胁情报以及专业的工具与服务，为客户提供一套完整的解决方案。

高级持续性威胁攻击(APT)或锁定目标攻击会不断渗透并躲过传统的信息安全机制 ,包括：防毒、新一代防火墙以及入侵防护系统，最近韩国各大银行及媒体所遭受的攻击正是如此。此类攻击通常是由黑客透过幕后操纵通讯服务器（Command-and-control (C&C) server[2]）从远程对已渗透的计算机下达指令。趋势科技 TrendLabs 研究人员在追踪这类幕后操纵通

信时发现了 1500 多个有效的幕后操纵通信服务器，每一网站所操纵的受害者从 1 到 25,000 个不等。

有鉴于这类攻击的行为，趋势科技 定制化智能防御战略策略提供了新的方案来应对这类幕后操纵通信手法，提供独特的定制化侦测与防护技术，并且可自动更新至网络装置、网关、服务器与端点装置等防护点，让企业迅速调整并响应这类攻击。

趋势科技“主动式云端截毒技术”（Smart Protection Network）依托于对数百万兆（Terabyte）云端威胁情报进行关联性分析，让企业获得有关特定威胁及网络黑客的信息，让他们拥有所需的情报来实施反击。在最近韩国所发生的攻击事件当中，采用定制化智能防御战略技术的趋势科技客户皆能在不法之徒造成伤害之前便预先发觉及响应。

BYOD 时代的用户全方位防护

IT 消费化趋势不仅提升了员工的生产力，也因为员工个人自备装置而带来了数据泄露与信息安全的挑战。员工不受管制地使用 Dropbox、YouSendIt 及 iCloud 等这类曾经发生安全事件的个人云端服务，已成为一项重要的资料外泄威胁。

为此，趋势科技推出了“云间 企业版”（SafeSync for Enterprise） 这套安全且架设在企业数据中心或私人云端内部的档案同步及协同办公解决方案。这套部署于企业内的解决方案既让使用多种设备 （智能型手机、平板电脑、个人电脑）的移动工作者提升生产力及协同办公，又不牺牲企业信息资产的安全性。

此外，随着趋势科技“企业安全及数据保护”（Enterprise Security and Data Protection）解决方案的推出，趋势科技更在现有的恶意软件防护平台当中纳入了整合式数据泄露防护（iDLP）功能，不论新旧客户都能享有一套完整、容易安装、集中管理的数据防护解决方案。全新的解决方案能让现有的趋势科技端点、移动装置、邮件及网关等解决方案具备完整的数据泄露防护功能。用户不论从任何地点、任何装置、任何应用程序，都能安全地存取并交换信息。

云端及数据中心安全

亚太地区有大约 20% 的企业其半数以上的服务器皆已虚拟化，这项数字预计将在 2013 年底达到 37%[3]。随着部署服务器虚拟化及迈向云端的企业越来越多，其数据中心也日趋多样化而复杂。在一个服务器工作负载横跨了物理、虚拟及云端的环境下，服务器防护必须容易管理、能够随着工作负载一起移转至云端，而且不能降低系统效能。当数据中心转型时，

企业需要的是能够提供完整安全防护、简单统一的管理控制台以及最高虚拟化投资回报的新一代服务器防护解决方案，并且要能涵盖物理、虚拟及云端服务器。

趋势科技 Deep Security™ 新一代服务器安全平台，是专为云端及虚拟化而优化，能让企业以及提供基础设施即服务（IaaS）的云端服务运营商发挥虚拟化的最高投资效益。最新的版本将数据中心防护延伸至混合云端及公共云端，能与 vCloud 及 Amazon Web Services 的 API 整合，为软件定义数据中心提供分租共享的架构。除此之外，还有趋势科技 SecureCloud™ 可提供云端数据加密，这套加密与密钥管理系统，让 IT 主管能放心拥抱虚拟化及云计算，并且知道自己最宝贵的资产，也就是数据，已受到周全的保护，不怕数据窃盗、意外泄漏，也不怕数据被任意移转至其他数据中心。如此，就能让企业重拾掌控权，获得政策导向的密钥管理，不论在任何环境都能实现最高的数据安全及法规遵从。