“僵木蠕”无处藏身：桂林移动携手趋势科技构建合规性威胁预警平台

近年来，以“僵木蠕”（僵尸网络、木马、蠕虫）为代表的网络威胁已对运营商线路租用客户造成了巨大的经济损失。为此，中国移动集团在严格遵守国家通讯管理局要求的同时，努力通过创新网络安全技术和制度的要求，指导全国各移动公司有效应对“僵木蠕”威胁。其中，桂林移动公司（以下简称：桂林移动）携手全球服务器安全、虚拟化及云计算安全领导厂商——趋势科技，采用趋势科技威胁发现设备 TDA 和 CTIS（地图威胁信息展示系统）组建了可视化威胁监控平台，通过实时展示、定位和治理移动城域网中的高风险节点，有效提升了“僵木蠕”威胁的防治能力，为实现合规目标提供了有力支撑。

“僵木蠕”分布广泛 寻找合规性突破口

据了解，桂林移动是广西地区面向中小企业客户提供宽带租赁、机房空间租赁的运营商之一。截止至 2013 年，全市已经有多家中小企业用户、家庭宽带用户、VIP 客户利用桂林移动城域网访问 Internt 的网络。同时，城域网还承载着桂林移动多个对公服务的业务系统，接入的计算机达到数万台的级别。但在最几年，国内僵尸肉机、木马主机的数量激增。面对这种规模的大型网络，如何进行有效的监管和威胁定位，是对运营商 IT 运维管理与安全防护能力的挑战。

研究表明，遭遇“僵木蠕”入侵的机器主要分布在托管主机、家庭宽带主机等安全防护手段较为薄弱的群体中。因此，国家通讯管理局在 2012 年已经针对运营商发文要求整治城域网的僵木蠕主机。针对广西地区，广西通讯管理局在《桂通管安【2012】5 号》文中提出了各运营商必须在 2012 年底完成对管辖区内僵尸、木马主机的治理，并形成常态化的管理及清理手段。而作为桂林移动的上级单位中国移动集团，也针对该情况制定了统一的集团规范《中国移动互联网安全防护技术要求 V1.0.0》，该规范明确规定了各级别移动公司必须在城域网部署对僵尸、木马主机的监控手段，提前预警及定位，降低“僵木蠕”威胁对城域网用户及移动业务的影响。

对此，桂林移动城域网安全负责人秦工表示：“僵木蠕”威胁是城域网中流窜最多的威胁之一，对用户及运行商的危害最大。但是由于僵尸、木马的技术发展非常快，其行为非常隐蔽，常规的 IDS、防火墙等安全设备根本无法发现这些威胁。同时，运营商城域网有别于常规企业的局域网，其流量非常巨大，仅桂林移动的城域网部分出口可达 6G，远远超过了常规安全设备能够承载的流量。基于上述原因，桂林移动一直无法有效落实通管局及中移动集团下发的相关法律法规，严重影响了桂林移动的安全考核上的评分。为此，桂林移动迫切希望找到一套运营商级别的“僵木蠕”威胁预警平台，提升桂林移动城域网的抗攻击能力，同时协助桂林移动遵从上级单位颁发的法律法规。

全景地图展现安全状况 威胁无处藏身

趋势科技作为全球知名的云安全厂商，一直致力于协助客户搭建多层次的安全防护体系，目前已经协助多家省级运营商搭建安全防护体系。双方在充分沟通之后，桂林移动邀请趋势科技对城域网现有安全监控体系进行新一轮的改造，以提升城域网对“僵木蠕”的防治能力。经过对城域网环境的深入分析，双方最后敲定使用趋势科技独有的 TDA 作为桂林移动城域网“僵木蠕”威胁预警平台。

据了解，TDA 作为本次“僵木蠕”威胁预警平台改造的支撑系统，以旁路监听的方式部署在桂林移动城域网核心交换机上。由于采用旁路的方式，再加上本次部署的 TDA 是趋势科技专门针对运营商网络环境提供的电信级设备，其单台设备最大吞吐量可达 1.5G，并且可以根据用户环境的变化进行按需扩展。因此，本次部署的方案解决了用户初期担忧的处理能力问题，成功踏出建设“僵木蠕”威胁预警平台的第一步。

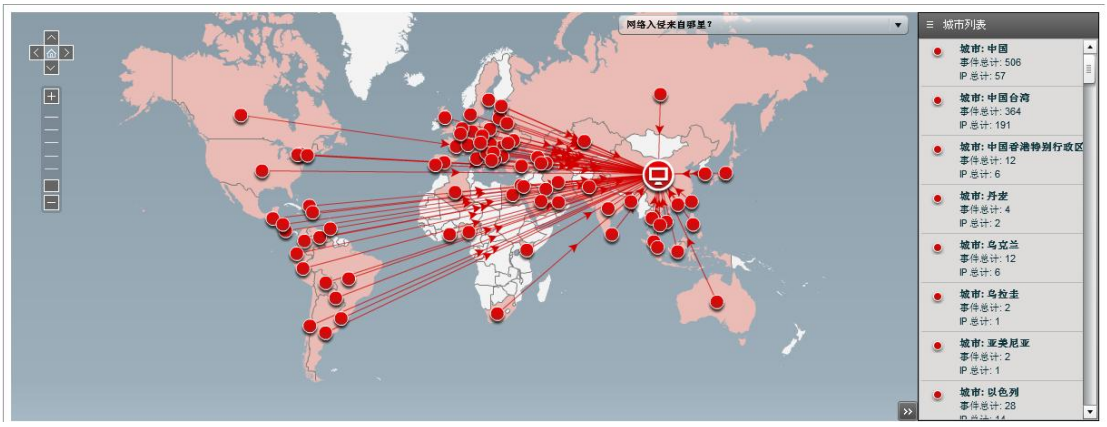
为了最大化定位城域网中的“僵木蠕”高风险节点，部署 TDA 时主要针对桂林移动托管服务器区、VIP 客户、部分家庭宽带区进行数据采集，并把采集到的数据复制到“僵木蠕”威胁预警平台中进行深度分析。由于使用了趋势科技独有的“云安全”技术，TDA 可检测各种僵尸、木马等基于应用层的威胁，如 IRC 僵尸活动、P2P 僵尸活动、挂马站点活动等。另外，当僵尸肉机、木马主机在网络中传播感染其它用户或与外界 C&C 服务器（僵尸控制服务器）通讯时，TDA 会通过深度包检测技术发现该可疑请求，并对发起连接的源头机器做标记，同时在管理控制台上通过可视化的地图展示高风险节点的物理位置、网络位置及处理建议。

如今，通过 TDA 独特的反向定位功能，桂林移动能够迅速找到了隐藏于网络中的高风险节点，并根据趋势科技整合在 TDA 报告中的解决方案，在这些高危节点尚未造成大规模病毒爆发前就把病毒处理干净。在降低“僵木蠕“威胁带来各种经济损失的同时，遵从了上级安

全单位颁发的法律法规。

顺利实现合规要求 获得集团认可

据了解，桂林移动“僵木蠕”威胁预警平台在 2012 年开始进行研究，以桂林移动重点研发项目的形式开展。经过半年的研究及实施，展示出良好的效果，并在 2013 年通过了中国移动集团对全国各个研发项目的评审。



“僵木蠕“威胁预警平台监控效果

秦工表示：在 TDA 部署完成之后，桂林移动已经按照通管局要求，制定了一套常态化的“僵木蠕”管理及清理手段，从而实现了从对”僵木蠕”威胁全生命周期的管理。如今，桂林移动整个城域网的数据都可以利用 TDA 系统，进行 2-7 层的深度扫描，不但主动、实时的抓住了城域网中的僵木蠕高风险节点，更全面降低了“僵木蠕”威胁对用户及桂林移动带来的各种损失。与此同时，TDA 还能够协助桂林移动遵从通管局及中移动集团等上级单位发布的法律法规要求，提升了每季度的安全考核分数，并成为了市级移动公司在针对“僵木蠕”防治工作成功典范。

###

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。