



趋势科技新闻稿

[即时发布]



趋势科技“2014年第一季度信息安全报告”出炉

恶意“越权广告程序”跃居第一 万物互联出现明显信息安全漏洞

[趋势科技中国]- [2014年5月23日]近日，全球服务器安全、虚拟化安全及云安全领导厂商趋势科技发布了《2014年第一季度信息安全报告：网络犯罪发动奇袭》，文中指出，网络犯罪者处心积虑开发更多手段来攻击用户，以牟取暴利。贪得无厌的网络犯罪者本季度盯上了新的攻击目标，包括针对 POS 终端机、利用灾难事件的进阶性威胁等。此外，移动设备恶意程序与高风险 App 程序数量已在第一季度突破两百万大关，其中“越权广告程序” (Aggressive adware) 的数量更是超越去年威胁榜首“高费率服务盗用程序”。

趋势科技（中国区）业务发展总监童宁表示：“企业对于锁定目标攻击仍无良好对策，而这些攻击可能直接针对能源、金融、医疗及零售产业或重大基础建设。原因很简单，不论企业多么拼命守护其珍贵的信息，只要存在巨大的经济利益，都会成为不法分子下手的目标。”

趋势科技第一季度的主要发现包括：

- **移动设备威胁：**与去年比较，移动设备威胁在今年以更快的速度成长，恶意与高风险程序数量在今年第一季度正式突破两百万大关。其中，“越权广告程序”在数量上已经超越去年威胁榜首“高费率服务盗用程序”，原因很可能是最近国外大型电信服务商纷纷宣布降低文字增值服务的费率，不法分子认为这些服务盗用的“获利”能力，已经不如其它犯罪工具，因此将注意力转移到越权广告程序的散布，以便将触角延伸至更多用户。
- **网络犯罪与地下犯罪网络：**比特币已成为一种成熟货币且吸引更多网络犯罪者，例如今年三月出现的 BitCrypt 勒索程序，便专门盗取比特币这类数字货币的电子钱包；我们在全球也见到许多比特币交易所遭到抢劫。
- **本季度网络银行恶意程序数量比 2013 年底大幅降低：**2014 年第一季度的数据与去年同期并无太大变化，但考虑到去年年底的高额数据是网络犯罪者利用岁末购物热潮所致，因此今年的数据仍值得我们充分警惕。在区域方面，美国是遭受网络银行恶意程序攻击最严重、同时也是受勒索程序影响最严重的国家。

- **锁定目标攻击与网络攻击**：美国出现销售柜台 (POS) 系统遭渗透 (尤其是零售与旅馆业, 如知名零售商 Target) 以及韩国信用卡公司发生内部攻击的事件, 两者皆凸显出企业 (尤其是接受信用卡付款的企业) 建立“定制化防御策略”的必要性。
- **数字生活与物联网**：新一代的漏洞攻击在本季度大举入侵 App 生态体系, 即使“短暂流行”的 App 也容易遭到攻击。这些 App 专门满足用户希望以匿名方式分享、传送多媒体内容的欲望, 有造成用户个人信息外泄的风险。

除了更多的社交工程诈骗之外, 万物互联 (Internet of Everything, 简称 IoE) 市场上的多款设备也成为研究人员放大检视的焦点, 并在不少设备上发现了一些明显的漏洞。例如, Tesla Model S 电动车因大量应用移动互联网科技而获得大量媒体关注, 但也因此让该车容易遭到黑客攻击。

趋势科技经过针对一些智能电视的分析发现, 由于厂商将无线连接 Miracast 的密码直接写入到某些机型的固件中, 因此任何人只要在一定的距离范围内, 都能远程将画面播放到该电视上。此外, 监控摄影机也曾经遭攻击。所有这些针对物联网的攻击往往都不只是为了困扰用户, 而是为了非法获利。

###



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。