趋势科技新闻稿

[即时发布]

趋势科技揭秘移动互联网“地下市场” 犯罪工具“明码标价”

——趋势科技发布《中国移动互联网地下黑市调查报告》

[趋势科技中国]– [2014 年 3 月 19 日]移动互联网正在深刻地改变着这个世界。当我们将笨重的 PC 更换为各式各样的移动设备，享受数字生活的同时，网络犯罪的地下经济结构也更加完备，并由此促生出来一个被称作“移动互联网地下黑市”的地下经济新类型。

为了帮助更多的普通用户深入了解并有效防范恶意风险，让掌中的智能终端和消费意愿真正“属于自己”，作为全球服务器安全、虚拟化安全及云安全领导厂商，趋势科技近期发布了《中国移动互联网地下黑市调查报告》。

在这份近 20 页的报告中，很多不法份子的恶劣行径都第一次被详细披露，不但犯罪工具和服务“琳琅满目”，更采用了“明码标价”、“打包优惠”等销售模式。例如：每年 15000 元就能强迫用户付费的订阅服务号码、仅售 3000 元的安卓设备短信转发器源代码、2800 元人民币即可发送 100000 条信息的短信发送服务、可在 5 秒钟内劫持一部手机短信服务器、40 元就能提升 APP 商店排名的提升服务等等。

针对这些随时都对消费者构成信息泄露和资产丢失的威胁，趋势科技全球执行副总裁暨亚太区总经理张伟钦表示：”断掉地下市场这条产业链，从技术上讲难度并不大，只要能掐断核心技术来源，端掉交易市场，规范运营商销售渠道，这些损害消费利益的不法商户就没有地盘。但难就难在，这需要整个行业的协调努力，以及消费者个人防护意识的整体提升。国内 Apple 设备‘越狱’情况泛滥、安卓第三方应用商店管理不严，都为恶意程序提供了滋生的沃土。而趋势科技在 2013 年已发现将近 140 万个恶意及高风险的移动应用程序，预估这一数字在 2014 年底会到达 300 万。因此，消费者和企业比以往任何时候更需要随时掌握自己的信息安全漏洞，并且思考该如何更妥善保护个人信息及捍卫个人隐私。”

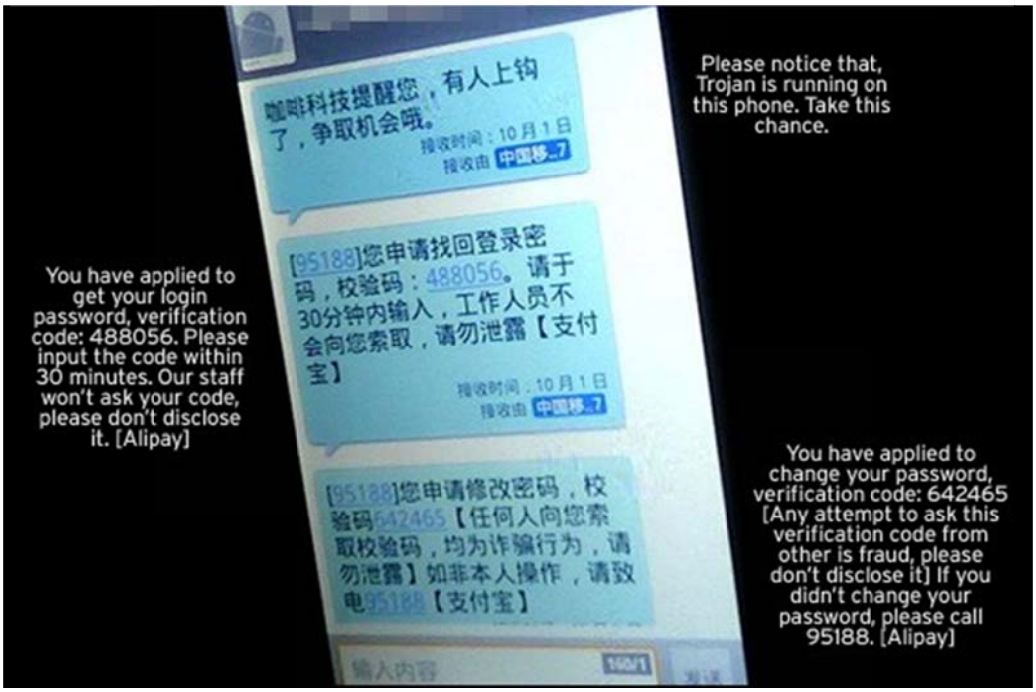
以下是报告的重点摘要：

付费服务号码

“手机吸费”是恶意 APP 的一种常见行为。此类恶意 APP 在用户手机上通过操纵短信服务来订阅手机付费服务，而在整个订阅过程中不会留下任何蛛丝马迹。所以，在用户毫不知情的情况下，用户的手机话费会被自动扣除以充当订阅费用，而这笔费用最终会落入恶意 APP 的开发者囊中。付费服务号码，又被称为“SP 短信通道”，是运营吸费 APP 的关键资源。只有配备了付费服务号码，吸费 APP 才能实现窃取话费的目的。

短信转发器

短信转发器是一种木马，旨在恶意盗取短信中的身份验证或认证码。如图 1 所示，许多运营商在站点注册、密码重置和在线付款等服务方面都会广泛使用短信进行身份验证或认证，而忘记密码的用户则通过注册手机号码从该站点收到一条包含验证码的短信，即可更改密码。而短信转发器会监控某些电话号码发送的短信，这些号码一般与在线付款服务提供商或银行有关，然后，它们会截取身份验证或验证码，并转发给网络犯罪分子。一旦掌握了受害者在特定站点的用户名，网络犯罪分子就可以轻松地更改密码并控制被盗账户了。



【图 1：短信转发器发送给网络犯罪分子的在线付款短信示例（请注意，该短信包含用户重置密码所需的验证码。)】

垃圾短信发送服务和设备

那些不请自来的“垃圾短信”是如何冲进手机的呢？网络犯罪份子通常使用三种设备包括：GSM 调制解调器（又称为“短信猫”）、Internet 短信网关、短信服务器（又称为“伪基站”）。但由于一台 16 插槽的“短信猫”每小时只能发送 9600 条短信，因此很多“顾客”会选择不法运营商提供的高速短信网关来进行群发服务。

【图 2：仅售 45000 元的短信服务器“套装”】

而对于普通用户来说，最神秘的莫过于短信服务器。如图 2 所示，一套完整的短信服务器组合包括：一台笔记本电脑、一部 GSM 手机、一个短信服务器盒、一根天线和一根 USB 数据线，而它的地下市场售价是 45000 元人民币。作为“伪基站”，它会在运行时发送大功率信号以冒充合法基站，这样就会使附近所有手机都与网络运营商的合法基站断开，转而连接到该短信服务器。此时，垃圾短信发送者可以使用“任何号码”发送短信，这包括了公共服务号码或合法的银行服务号码，非常容易让用户信以为真，并在后续的操作步骤中丢失自己的资金财产。

垃圾 iMessage 短信发送服务和软件

iMessage 是 Apple 提供的一种适用于 iOS 和 OS X® 的实时通讯（IM）服务，iPhone 用户可以将其电话号码和 Apple ID 与 iMessage 关联在一起。一般来说，某种服务越受欢迎，就越有可能成为网络犯罪的目标。要有效地发送垃圾短信，最重要的一步就是搜索与 Apple ID 关联的电话号码。为此，地下市场专门为犯罪分子推出了垃圾短信测试系统，为发送者实施精准的广告推送、发送诱骗短信提供帮助。

电话号码扫描服务

移动用户的数量正在呈爆炸式增长，一些用户的“换号”行为令网络犯罪分子无从企及。为了将未使用的电话号码从垃圾短信发送列表中过滤掉，他们可以从地下市场购买“实号“扫

描服务，这包括该号码的用户是否在线，以及该号码是否仍处于使用状态。请注意，由于受扫描软件控制的手机一小时只能扫描 400 个电话号码，因此，对存储有大量电话号码状态的数据库进行查询的服务，则在地下市场更受欢迎。

应用程序排名提升服务

一般来说，所有 APP 应用商店都会对应用程序进行排名并向客户推荐。无论应用商店采用哪种排名算法，下载次数和评论始终是确定应用程序排名的重要因素。而网络犯罪分子往往会创建数个虚拟帐户以下载某个应用程序并撰写好评，进而提升该应用程序的排名。在这项非法服务中，从 40 元人民币的 10000 次下载，到 650 元的 180000 次下载，可以说是买得越多越便宜。

针对移动互联网黑市可能对个人消费用户带来的损害，趋势科技高级安全研究员谷亮指出：“作为安全行业的一份子，我们必须主动、实时的去关注移动互联网地下市场的发展状况。如今，地下黑市拥有所有网络犯罪分子都想得到的各种服务和商品，因此，个人用户在提升警觉的同时，更应当采取积极的隐私防范措施。针对手机银行终端程序，移动支付应用，用户最好去官方网站或者具备安全检测的第三方电子市场下载，并安装有效的安全防护软件，阻止并查杀‘扣费 APP’等恶意程序的操作，防止网银账户被盗取等损失更大的事件发生。

趋势科技《中国移动网络犯罪地下市场》研究报告下载地址：
http://www.trendmicro.com.cn/pdf/pdf-20140317.pdf

###

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。