手机APP被破解，被山寨已成手机软件开发行业公害

内容来源：西安弈聪信息技术有限公司(http://www.xaecong.com)

关键词：手机APP

内容概要：

很多智能手机用户可能并没有意识到，自己下载在手机APP，可能是山寨APP或被破解的官方APP。这些APP背后的开发者之间可能没有关系，更与官方APP的软件原始创作者毫无渊源。通过打法律擦边球以破解或者仿冒市场上一些热门的APP软件，从而赚取...

正文：

很多智能手机用户可能并没有意识到，自己下载在手机APP，可能是山寨APP或被破解的官方APP。这些APP背后的开发者之间可能没有关系，更与官方APP的软件原始创作者毫无渊源。通过打法律擦边球以破解或者仿冒市场上一些热门的APP软件，从而赚取软件使用费或广告费，这种地下产业链已成软件开发、运营领域的公害。

在移动时代，APP正普遍遭遇反编译、二次打包、病毒侵袭等安全性问题。APP的安全性问题，主要可分为三种：盗版、数据篡改和山寨。以赵宇的理解，盗版首先是以反编译为前提通过修改某些资源文件或者是代码文件，之后重新打包二次分发。

目前市场上山寨APP主要危害行为分为六种：一是窃取账号，窃取用户支付账号及使用行为；二是购物欺诈，诱导用户去钓鱼网站进行支付；三是恶意扣费，私自定制扣费SP业务；四是远程控制，在用户使用后留取后门，远程控制并窃取用户手机中资料；五是窃取隐私，窃取用户通讯录，向用户推送购物广告；六是骚扰用户，每天不定时无限制的向用户推送广告购物信息，并无法关闭推送。

伴随手游业务的崛起，游戏APP产业中，个人开发者及中小型开发企业的数量正在以爆发性的趋势增长，但是对于这些资金实力和应对突发事件能力不足的开发者来说，游戏APP被破解和被捆绑病毒可能成为其致命伤。对于网络游戏和单机游戏，游戏APP被破解的最大威胁便是APP背后的原有利益链被外部第三方重构，从而破坏了公司原有的利益模式。数据篡改的另一大杀手锏便是通过修改游戏APP中的内存数据，从而将收费游戏改成免费游戏，这将直接将游戏公司的盈利模式无形中破解。

目前的APP破解链条中，上游的游戏破坏者主要是两类：一类是负责软件二次打包的打包党，这些人一般是一些个人或者小团队，通常不发布公开信息，维权者很难找到这些打包党，即使能找到，因为人员较分散，维权成本也太高，因为取证难度非常大。另一类是相关作弊软件的发行者，这类人发布具体某款作弊软件时，并不特定针对具体目标，只是对外介绍具备如加速游戏等功能，因此拿到类似软件对具体产品直接损害的证据太难。

国内大多数应用分发市场为吸引流量，并未对上传的APP采取事先审查商标、版权、病毒携带等检查，无疑也为APP破解产业提供了通道。在维权中，APP官方开发者出于时下法律不健全及长期合作需要，一般也只能与这些APP分发渠道商协商解决相关问题，而非以法律诉讼方式解决。

西安弈聪信息技术有限公司简介

西安弈聪立足陕西西安，为西安企业提供网站优化，软件开发，软件外包，电子政务，网站建设、企业网络营销咨询服务及实施为主体业务，为客户提供一体化IT技术服务。

西安弈聪现有技术架构包含PHP,asp,.NET.C++,VB,J2EE等，在MYSQL,MSSQl数据库系统，ORACLE大型数据库管理系统开发方面专长，经验丰富，是业内技术服务最全面，技术实力最雄厚的IT技术服务企业之一。

联系电话：029-89322522 4006-626-615　网址:http://www.xaecong.com 邮箱:admin@xaecong.com