

2015 年,CNNIC 统计显示我国手机网民规模达 6.20 亿,手机上网人群的占比提升至 90%。随着移动端用户群体的快速扩张,除了一开始就注重移动市场的新互联网企业之外,传统企业也正不断提高对移动端的重视程度并加大投入,移动端市场的竞争呈现白热化趋势。

截止 2015 年 12 月 31 日,安卓 APP 总体数量已超过 140 万。据 Yahoo Flurry 统计^{分析},2015 年安卓 APP 整体同比增长超过 14%,其中面向细分市场的个性化 APP 爆炸性增长达 332%。新闻杂志、商务理财和旅行出游等 APP,2015 年的增长率也超过 100%。

移动 APP 已经全面覆盖衣食住行,“指尖社会”的安全风险也随着急速聚拢的财富而不断推高。

不安全的“指尖社会”

互联网的 PC 端安全经过十几年的实践,已经较为完善,但是移动端安全目前还是短板,传统的 PC 端安全防护措施无法有效保障移动端安全,作为移动端重要载体的 APP 因此安全事件频发。

大量安全事件中,APP 的安全漏洞被黑客作为攻击入口,通过侵入 APP 获取用户隐私以及企业数据库存储的数据,损坏用户和企业的利益,影响恶劣。

2015 年,APP 安全事件泄露的信息以用户的姓名、地址、账号、密码、手机号等信息为主,尤其金融理财和生活服务类的 APP 是安全事件爆发的重灾区。仅以乌云漏洞平台曝光的安全漏洞为例,2015 年,超过 10 家知名 APP 被曝存在安全漏洞可导致超 1000 万用户隐私泄露,这些安全漏洞的种类不一,漏洞的利用攻击手法也不同,但是攻击的最终指向目标都是用户隐私及企业数据。

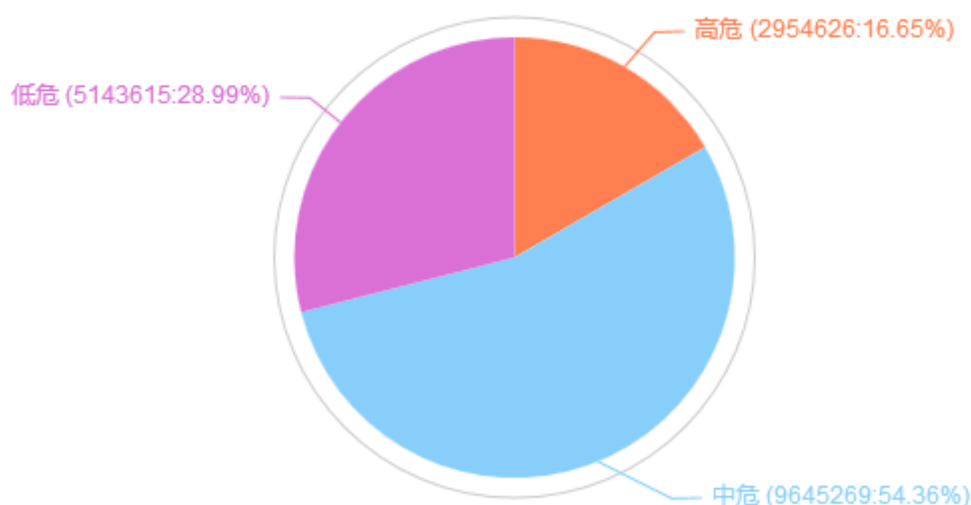
触目惊心的安全现状,超 9 成 APP 含有安全漏洞

截止 2015 年 12 月 31 日,网蛙科技对当前市场上 129 万个多类别的 APP 做了全面的漏洞扫描检测,检测结果显示,App 漏洞总量超过 1700 万个,仅程序代码中硬编码开发者密码(5744940 个)、Sqlite SQLInject 漏洞(2196703 个)与 ContentProvider SQL Injection 漏洞(1243679)三类漏洞数量就超过 918 万个。

据检测结果,129 万多个被检测 APP 中,超过 95%以上 APP 含有不同类型的安全漏洞,平均每个 APP 含 13.8 个漏洞,高危漏洞比例达 16%。

2015 年高中低危漏洞分布图

2015年高中低危漏洞分布图



1、APP 九大行业榜单产品,平均漏洞数达到 9.3 个

网蛙科技根据 2015 的 APP 年度分类排行榜,经综合考虑,选取视频、理财、音乐、电商、新闻、社交、自拍、工具以及游戏九类 APP 榜单(参考艾媒咨询、艾瑞网、互联网周刊、猎豹移动等 APP 排行榜榜单),共计 90 个 APP 产品进行了检测。

据检测结果,90 个 APP 榜单产品(以发行的最新版本漏洞扫描检测结果数据为准),漏洞总数达到 847 个,平均每个 APP 含有 9.3 个漏洞。分行业计,游戏行业所含漏洞数最高,平均漏洞数目超过 12 个,安全隐患相对较大;金融理财、电商、社交这三个行业的平均漏洞数都接近或超过 10 个,同样需要高度重视。

这些被检测的 APP 中近 70%面世时间达 3-5 年,具备成熟的市场口碑,当前用户规模和资产规模都高于同行业其他产品。它们高于普通 APP 的商业价值也更容易吸引黑产注意,如果遭遇安全事故,对 APP 有形的资产和无形的品牌都将造成严重损失。网蛙科技建议 APP 开发者们加强安全工作,切实提高产品的安全性,更好地维护 APP 用户利益和公司的品牌形象。

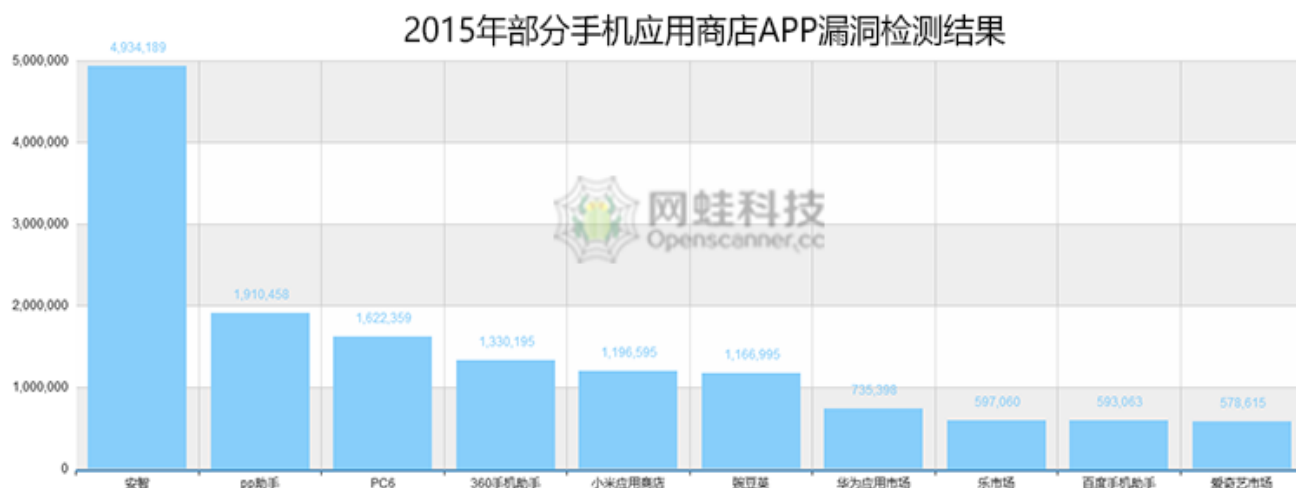
2、应用商店安全检测不到位,无法完全保障上架 APP 安全

网蛙科技对当前市场上两类应用商店的 APP 进行检测,分别为豌豆荚、应用宝、360 手机助手等知名独立第三方应用商店,以及小米应用商店、华为应用市场等终端厂商自建的应用商店。

据不完全统计,截止 2015 年 12 月,手机应用商店漏洞总数超过 1700 万,单个应用商店最高漏洞数目超过 493 万个,其中第三方应用商店漏洞数目平均达到 57 万个,终端厂商自建的应用商店漏洞数目平均达到 64 万个,第三方应用商店的安全系数相对高于终端厂商自建的应用商店。

据艾媒咨询,从当前市场 APP 下载情况来看,APP 下载渠道占比最高的为第三方应用商店(占比 54%),其次为终端厂商自建的应用商店(占比 34%),这两大类应用商店是当前用户下载 APP 的主要渠道。由于 APP 已经实质性地触及个人财产信息与隐私信息等,用户对 APP 安全性的要求不断提高,与此同步上涨的是用户对应用商店安全工作的不满情绪。截止 2015 年 12 月,超过 60%用户认为应用商店应该对商店内恶意软件的出现负审核不严的责任。2016 年,应用商店需要在安全能力提升方面做更多工作。

部分手机应用商店 APP 漏洞检测结果



3、19 类行业漏洞检测,游戏和生活服务类 APP 危险系数最高

网蛙科技对当前市场上包括金融理财、网络购物、商务办公等 19 类 APP 进行了分类漏洞统计。需警惕的是,直接涉及数据资产、用户隐私等高商业价值信息的行业,APP 检测结果显示漏洞分布数目远高于其他行业。

据检测结果,直接关联数据资产(如银行卡、移动支付等信息)的 APP 行业漏洞数目最高,游戏类 APP 漏洞数目高达 457 万,生活服务类 APP 以 250 万的漏洞数目排名第二,购物、金融理财类 APP 漏洞数目均超过 80 万;直接关联用户隐私(如姓名、联系方式信息)的 APP 漏洞数量也非常高,需要引起重视,社交、办公类 APP 漏洞数量分别达到 139 万和 100 万,而影音、教育类的 APP 漏洞数量也均超过 50 万。

近几年由漏洞引发的 APP 安全事故已经表明,无论是哪个行业,漏洞对 APP 安全都具有“一票否决权”。安全是一切发展的基础,APP 开发者需要加强安全工作,不可掉以轻心。

2015 年全行业 APP 漏洞分布图

事件中泄露的**漏洞**数据对全球众多公司造成了严重影响。

而与此相对的是,绝大部分的 APP 开发者并不具备 0-day **漏洞**挖掘能力,同时因为**漏洞**挖掘耗时久,从商业效益上说,企业自行挖掘 0-day **漏洞**的性价比不高,建议 APP 开发者与 0-day **漏洞**研究团队合作,借助专业的力量,打造更加安全的 APP 产品。

APP 安全,从防护漏洞**开始**

2015 年,云计算、物联网、大数据技术和相关产业迅速崛起,互联网移动端的发展将占据越来越重要的位置,作为载体之一的 APP 的安全更是互联网安全至关重要的一环。

国家对 APP 安全的规范工作正在不断建设与完善。2014 年 4 月至 9 月工业和信息化部联合公安部、工商总局在全国范围开展打击移动互联网恶意程序专项行动,将互联网恶意程序设为重点打击治理项目之一,督促应用商店落实安全责任。国家网信办主任鲁炜也曾公开表示,网信办将出台 APP 应用程序发展管理办法。当前 APP 市场乱象的生存空间将不断缩小,APP 开发者应提前部署应对措施。

APP 安全,是国家、开发商、广大用户三方面的需求。而随着 APP 市场发展周期的推进,错综复杂的安全情况,越来越高频的安全威胁,都预示着 APP 安全攻防战场焦点将从**漏洞**防护开始。参考互联网移动端安全发展的轨迹,APP 开发者与独立的第三方 APP 安全企业合作将成为互联网移动端安防的主流趋势。