jaq.alibaba.com

ALIBABA JAQ 2016
Annual Security Report

阿里聚安全2016年报

Content

2016年阿里聚安全先达到一个小目标，比如查杀病毒1个亿
每天新增近9000个新移动病毒样本，每10秒生成1个
广东省仍旧是用户感染病毒最多的省份
Android用户面临以往最大的风险
钓鱼诈骗木马使Android用户资金受损最大
移动安全时代双因素认证不再安全
真正威胁企业安全的高级移动病毒出现——DressCode恶意代码
Android病毒展现更多面的恶意行为
Android病毒攻击呈现出更隐秘的特性
89%的热门应用存在仿冒
移动病毒和仿冒相辅相成，广东省两者都占首
社交行业仿冒应用量最高，但游戏和影音的传播性更强
盗版软件、短信劫持、流氓行为、恶意扣费是仿冒应用主要恶意行为
金融行业银行类仿冒居多，某银行仿冒应用全部具有短信劫持行为
游戏行业仿冒应用分析
阿里聚安全移动安全扫描器创新迭代快速，帮助企业提高前置安全感知能力
18个行业的Top10应用中98%的应用都存在漏洞，但Webview远程执行代码漏洞迅速下降
逐利是黑产本性，游戏行业漏洞上升较快
安全闭环的Apple生态系统比Android系统表现出更安全的态势
可能永远不会修复的漏洞影响9亿安卓用户
折断的翅膀——WLAN芯片引入大量提权漏洞
对于移动安全漏洞，企业需要更多关注NDAY漏洞
只要接入网络就可能被攻击
与操作系统和软件无关的硬件漏洞攻击出现—— Drammer
PEGASUS——三叉戟攻击链，最复杂精密的iOS APT攻击
iOS可公开利用的漏洞持续披露用户面临更大风险
互联网业务风控或将成为下一个风口
羊毛党、黄牛党在2016年成为互联网业务发展过程中最大的毒瘤
在干草堆里捞针，数据、算法、算力为王
自动注册为王，细化防御才能精确打击
暗号谍战——滑动验证的混淆加密切换
2016年移动欺诈损失超数亿美金
大规模图搜索和实时计算成为风控系统核心竞争力
快速接入与快速自动响应是营销反作弊系统重要指标
创造纵深的有适应力的数字化业务系统

Preface

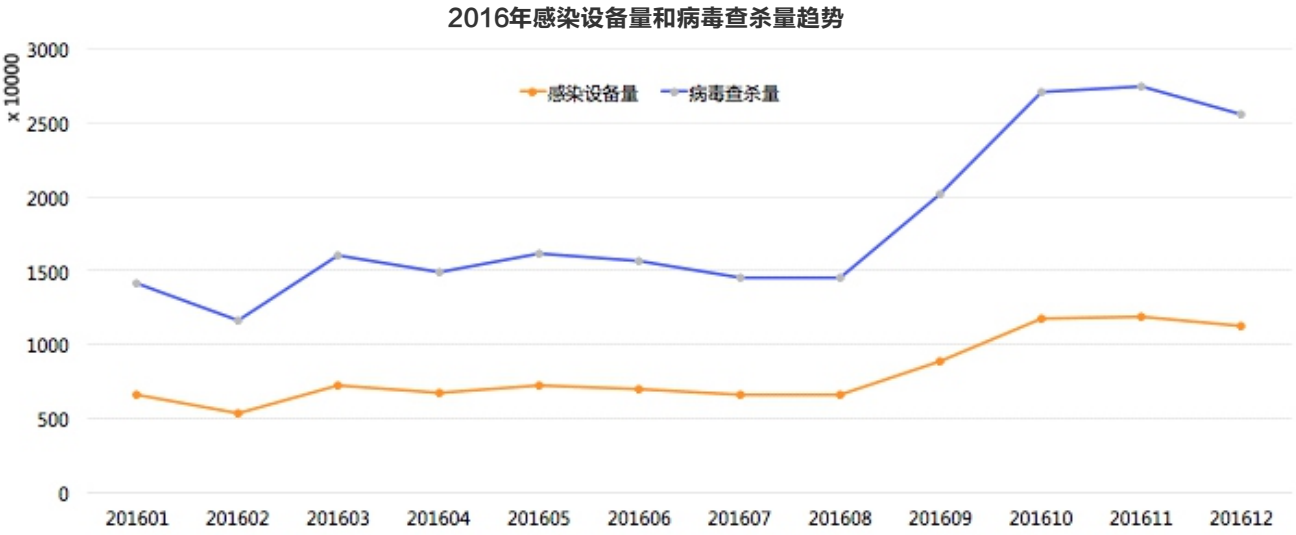
我们正处于一个科技创新涌现的时代，沟通、协作及业务模式的变革速度变得十分惊人，在传统企业进入边界模糊、用户海量、终端不可控的互联网业务时，传统的安全边界防护策略已经不再是有效的方法，原来依赖的安全控制效果已经大大降低。作为专注于互联网业务安全的阿里聚安全，正以新的安全模型全面着保护互联网企业用户。本报告重点聚焦在2016年阿里聚安全所关注的移动安全及数据风控上呈现出来的安全风险，在移动安全方面重点分析了病毒、仿冒、漏洞三部分，帮助用户了解业务安全端安全方面应该注意的风险，之后会描述阿里聚安全在业务安全防控方面做的一些努力和观点，帮助企业在建设互联网业务安全时，考虑安全策略和防护应该往哪部分倾斜。

Part / 01

2016年阿里聚安全先达到一个小目标，比如查杀病毒1个亿

2016年度，Android平台约10台设备中就有1台染毒，设备感染率达10%，阿里聚安全病毒扫描引擎共查杀病毒1.2亿，病毒木马的查杀帮助用户抵御了大量的潜在风险。

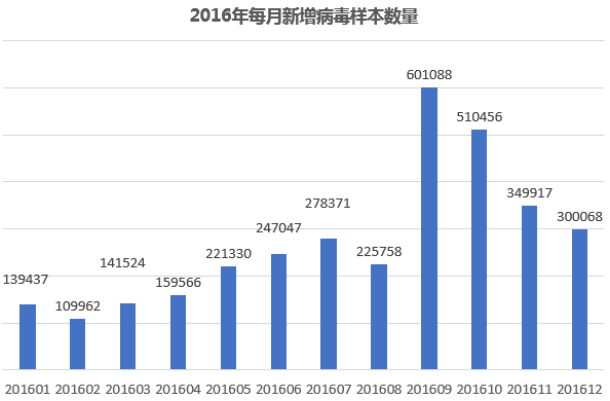
(注：根据国外的病毒定义标准，将软件获取部分手机硬件信息、游戏软件包含支付插件等行为也定义为恶意软件，因此2016年我们为了更贴合中国国情，认为在移动应用病毒里统计“弱风险”类型病毒意义不大，本次及下面的统计取消了“弱风险”类型的统计)



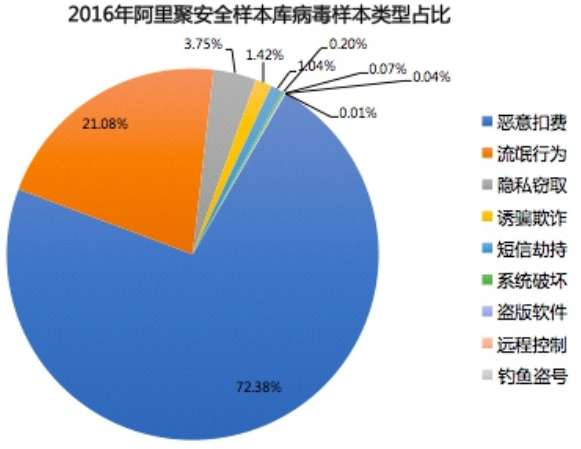
Part / 02

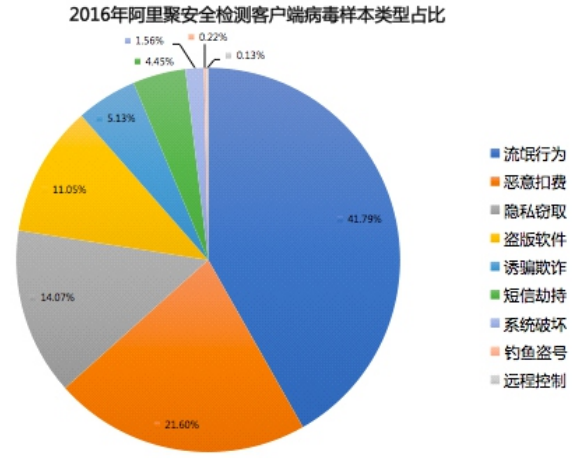
每天新增近9000个新移动病毒样本，每10秒生成1个

阿里聚安全移动病毒样本库2016年新增病毒样本达3284524个，平均每天新增9000个样本，这相当于每10秒生成一个病毒样本。我们也看到在9月份后病毒样本有比较明显的增加趋势。虽然原生Android系统的安全性越来越高，但移动病毒利用多种手法如重打包知名应用、伪装成生活类、色情类应用等传播，在每天新增如此多病毒的恶意环境下，Android用户必须时刻警惕在官方场合下载应用。

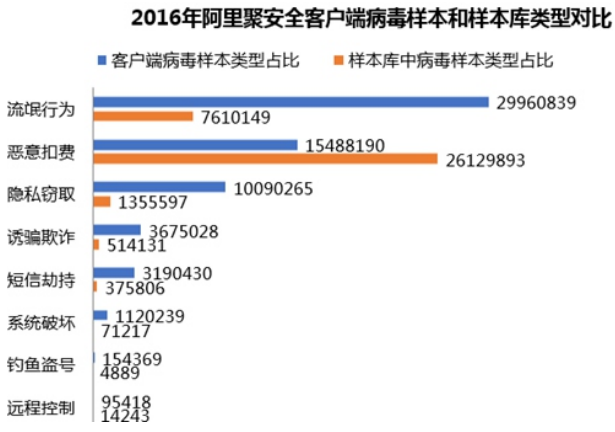


2016年，我们发现“恶意扣费”类在病毒样本量占比最高，达72%。该类病毒应用未经用户允许私自发送短信和扣费指令，对用户手机的资费造成一定风险，而在客户端检测到样本的“流氓行为”占比最高，“恶意扣费”其次。





对比客户端病毒样本和样本库类型，虽然“恶意扣费”的样本数非常庞大，但在客户端感染的数量已经成反比，这是因为国家着重针对影响范围大、安全风险较高的移动互联网恶意程序进行专项治理，“恶意扣费”类恶意程序治理效果显著，而“流氓行为”、“隐私窃取”、“短信劫持”及“诱骗欺诈”类病毒还是以较少的样本数占领了大多数客户端，尤其是黑产用于诈骗的“短信劫持”和“诱骗欺诈” 病毒基本是以1：10的比率影响用户端。此外干扰用户正常使用软件，影响用户体验，随意添加广告书签、广告快捷方式或锁屏等行为的“流氓行为”类病毒也占据大量用户客户端，此类病毒一般用于恶意广告推广为主。

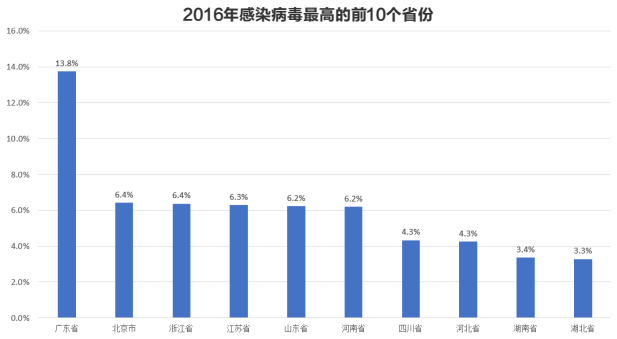


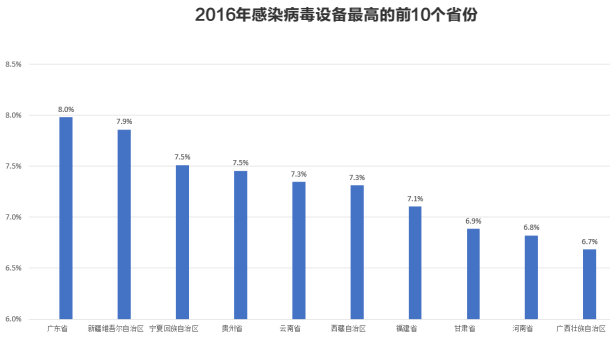
Part / 03

广东省仍旧是用户感染病毒最多的省份

相对比2015年，2016年广东是受病毒感染用户量最多的省份，其全年的设备感染量约占全国总感染量的13.8%。这受各省用户自身的安全防范意识、经济等因素影响，移动设备的强劲消费，一人持有多部手机的现象逐渐普遍，都使得这些省普遍呈高染毒感染趋势。

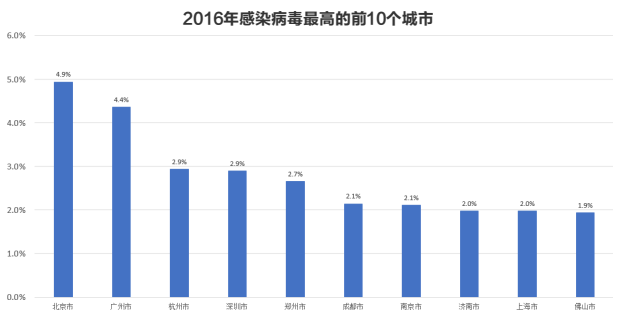
2016年设备中毒比例最高的省份集中在广东、新疆、宁夏和贵州，其中广州的总设备量基数较大,中毒比例最高达到8%，比全国平均值高2%。

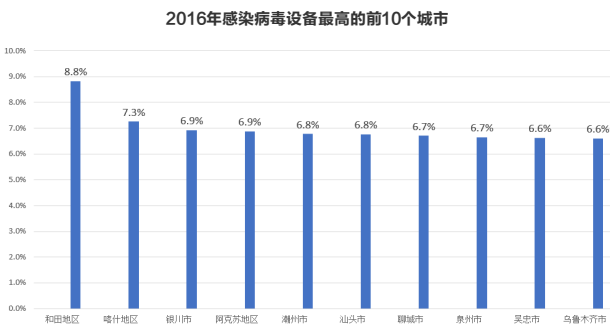




移动互联网产品发展较为发达的城市北京、广州、杭州依然领跑感染病毒最高的城市，全年的设备感染量约占全国城市总感染量的4.9%、4.4%和2.9%。

排名前10的感染病毒设备比例最高城市分别是和田地区、喀什地区、银川市、阿克苏地区、潮州市、汕头市、聊城市、泉州市、吴忠市和乌鲁木齐市。主要集中在西部和广东沿海等较不发达的城市。





Part / 04

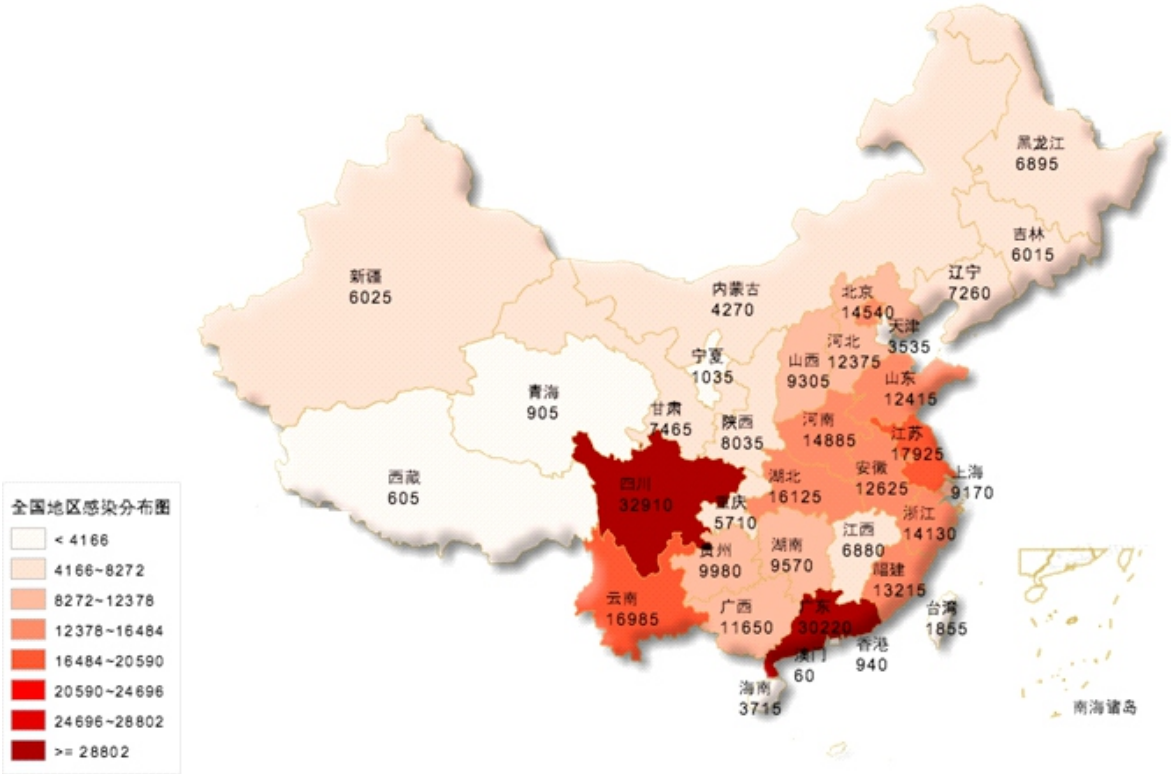
Android用户面临以往最大的风险

Android的86.2%的市场占有率，使得黑产毫无迟疑的专注Android系统，Android用户面临以往最大的安全风险。阿里聚安全在10月份发现“九头虫”恶意代码，该代码来自国内某“公司”，该灰产团伙通过广告投放商赚取广告推广费，和推广应用获取安装费。“九头虫”病毒一旦发作，设备将不断弹出广告，并自动下载、安装、启动推广应用，最终设备衰竭而死，用户非常困难通过常规的卸载手段清除病毒。

“九头虫”病毒通过重打包知名应用、伪装成生活类、色情类应用分发，利用多家知名root sdk对设备提权，可轻松提权上万种机型，成功提权后获得设备最高权限，随后向系统分区植入多个恶意App，删除设备其他root授权程序、su文件，并替换系统启动脚本文件，实现“起死回生”同时保证病毒具备root权限，将自身插入某杀软白名单中，并禁用掉多家杀软，致使设备安全防护功能全线瘫痪。

对2016年初到2016年10月的监测统计数据显示，“九头虫”病毒累计设备感染量高达33万。从感染地区分布图中可以看出四川、广东是感染重灾区。

全国地区感染分布



Part / 05

钓鱼诈骗木马使Android用户资金受损最大

除了隐藏恶意代码，伪装成合法的应用程序进行广告推送等常用恶意软件使用的技巧，攻击者使用更复杂的技术，针对用户进行诈骗，敲诈等行为，获取利益最大化。2016年移动电信诈骗案件呈持续高发态势，比如清华大学教授被诈骗1760万元、罗庄徐玉玉电信诈骗猝死，造成恶劣社会影响。

攻击手段上，“情景构建”式攻击在最近几年最为流行。攻击者通过地下产业链获取待攻击对象的个人信息和隐私，随后细化攻击“剧本”，实施连环诈骗，最典型的场景就是冒充教育局、公安局、检察院人员。

随着病毒与反病毒的博奕，移动电信木马技术也随之发生了变化，最新版本恶意代码核心功能全部native实现。以“最高人民检测院”剧本为例，诈骗过程如下：首先向受害者发送带恶意应用下载连接短信，短信内容以“案件号”、“xxx罪”、“电子凭证”诱骗用户点击；一旦受害者点击恶意程序后，攻击者获得手机控制权，随后将设备信息上传病毒C&C端，诈骗团伙得知用户已上线，实施接下来的电话诈骗；诈骗者主动给受骗者电话，恐吓受害者因涉嫌犯罪需要接受调查，并叫受骗者拨打检查院或公安局电话自己确认；防范意识薄弱的受害者可能会直接相信对方，但即便被害人具备足够的防范意识，诈骗者依然有办法逼其就范，他们会劫持受害者手机的报警电话，在被害者拨打110确认时，电话那头依然是诈骗者。环环相扣，使受害者信以为真，最终落入攻击者的圈套。

Part / 06

移动安全时代双因素认证不再安全

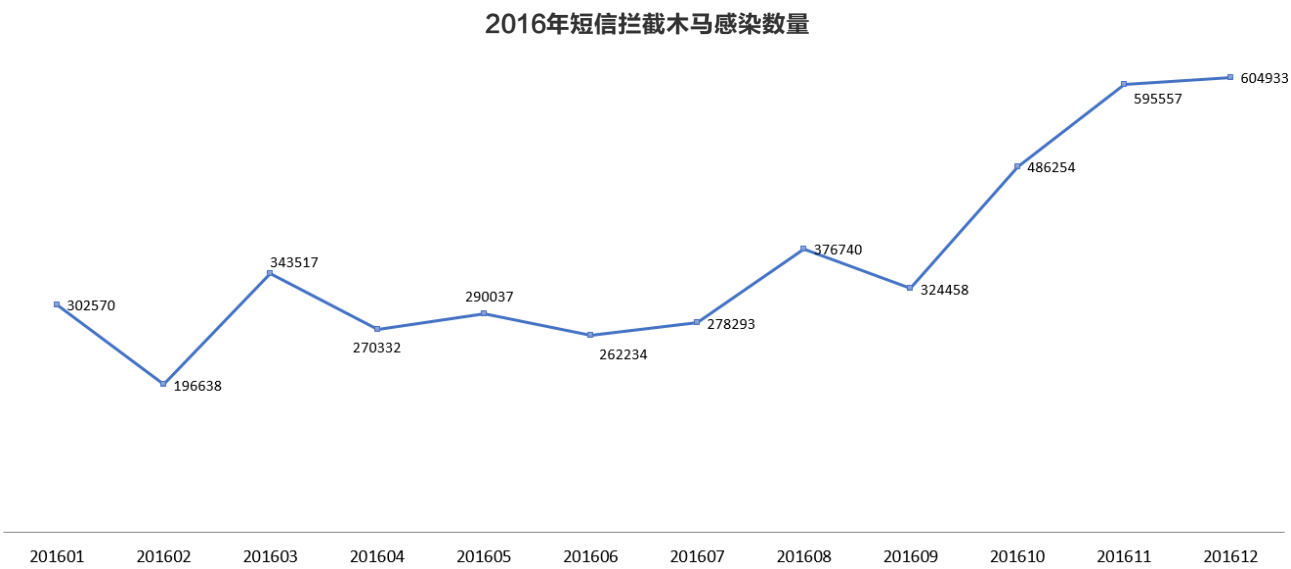
为了保证用户在移动支付中的安全性，目前，各大银行实施双因素认证即在支付过程中进行身份认证和基于手机动态密码的验证。在除了银行以外的第三方支付平台等都支持移动支付业务，并且大多都提供了银行卡绑定业务，在支付过程会验证用户账户和手机短信验证码，以确保安全。

双因素短信验证码、个人隐私数据（第三方支付App账号密码，银行卡号、手机号码、支付密码）是银行、第三方支付App、金融系统等与用户进行交易的重要介质，同时也是攻击者成功盗刷用户的关键媒介。

2013年至今黑产之手蔓延到移动支付，直接危害个人用户资金损失。目前，短信拦截马持续了将近4年的威胁和攻击， 短信截取木马类威胁事件已成固定的攻击模式：

1. 制马团伙编写木马；
2. 分发转卖团伙，卖给黑产团伙，并配置控制端信息；
3. 通过伪基站投放，伪装成银行、运营商和商户等号码发送带短链接的诈骗短信；
4. 用户点击短链接种马，木马上传用户短信、联系人，并进行拦截短信；或用户点击短链接，进入钓鱼界面，被诱导填写个人隐私（身份证、银行卡号、手机号、密码），随后下载安装木马，实施短信拦截；
5. 黑产洗料团伙，对拦截马上传的隐私数据过滤，筛选出可利用的整套个人信息（身份证、银行卡号、手机号）；
6. 转账洗钱，利用用户信息和短信动态验证码盗刷账户资金。

阿里聚安全监视到2016年短信拦截木马持续高位，严重影响用户安全，尤其临近年底，随着各种节日的到来，可以看到有比较高的升势。



Part / 07

真正威胁企业安全的高级移动病毒出现——DressCode恶意代码

“DressCode”的恶意代码利用典型SOCKS代理反弹技术突破内网防火墙限制，窃取内网数据。在PC端通过代理穿透内网绕过防火墙的手段非常常见，但病毒通过手机终端为跳板实现对企业内网的渗透还是第一次出现。病毒感染手机后，通过链接C&C服务器，接收恶意指令，这些指令可对内网的FTP服务器进行攻击，进而窃取企业敏感数据。8月底 CheckPoint官网发布报告《DressCode Android Malware Discovered on Google Play》，首次披露Google Play上存在40多个、第三方市场存在400多个应用感染了DressCode恶意代码；9月底Trendmicro官网发布报告《DressCode and its Potential Impact for Enterprises》，对DressCode代码片段、SOCKS代理攻击内网模型进行详细分析。 该病毒对内网安全带来极大威胁，企业需要非常严格的限制不可信的智能终端设备接入公司内网。[1][2]

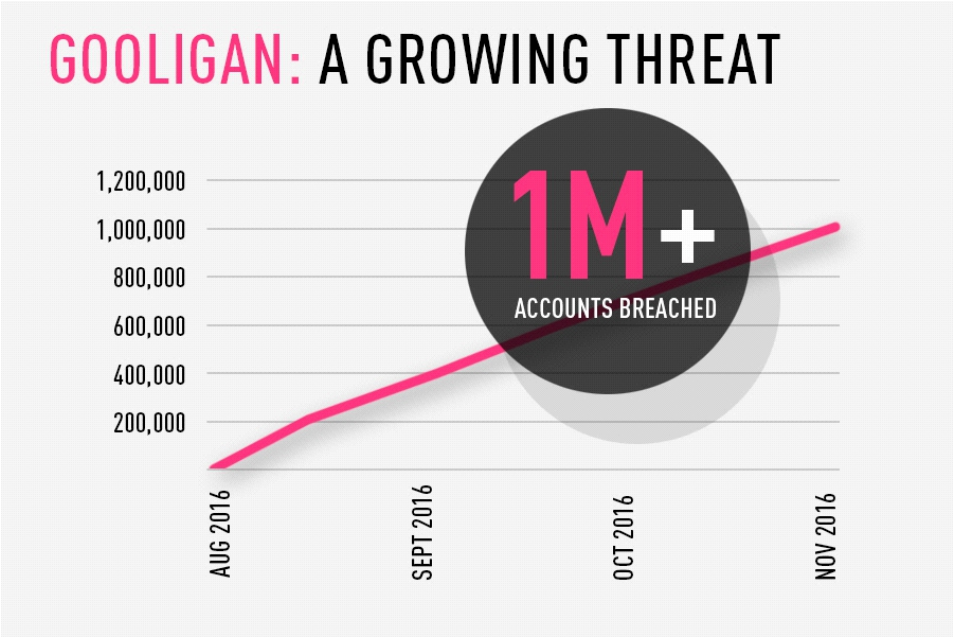
Part / 08

Android病毒展现更多面的恶意行为

Android病毒行为已经不光专注于短信拦截、隐私盗窃、恶意扣费等，黑产已经利用移动病毒为多种业务服务，Gooligan病毒也呈现类似特性。

今年6月份，趋势科技发表Godless木马，期间阿里聚安全监测发现国内市场存在同家族木马，应用名叫“魔百Wi-Fi”，该应用某些版本存在恶意代码，通过root设备、注入系统应用、偷取Google邮箱和authentication token进行恶意推广、恶意安装等恶意行为，并且还在各大新闻平台宣传声称自己拥有300万用户，覆盖终端上亿。我们对各个版本分析排查，发现2.3.5～2.3.10被官方插入了恶意代码，病毒在该设备锁屏时对设备root，root成功后向系统目录植入“刷榜僵尸”病毒，“刷榜僵尸”对指定应用在 GooglePlay商店上恶意刷量，同时还会诱骗用户安装“下载者”病毒，“下载者”病毒会在设备屏幕亮起状态会弹出广告页面，若用户触碰广告页面推广的应用将会自动安装运行。该病毒技术相当成熟，root 提权使用最高危的漏洞（CVE-2014-3153 Towelroot、CVE-2015-3636 PingPong和PutUser等），2015年10月之前的设备全部受影响。[3]

目前Gooligan感染用户超过100万，该家族恶意代码曾在2015年全球爆发，各大安全厂商报告并命明成不同病毒名包括GhostPush、Xinyinhe和MonkenTest，该病毒沉静到2016年夏季之后再次出现更复杂的变种。病毒利用多种知名root方案对设备提权，成功提权后，向Android系统进程注入恶意代码，偷取用户Google账号以及authentication token，利用受害设备对Google play的应用评分（刷榜），安装恶意推广的应用。



图摘自：“More Than 1 Million Google Accounts Breached” by Gooliganby Check Point Research Team

Part / 09

Android病毒攻击呈现出更隐秘的特性

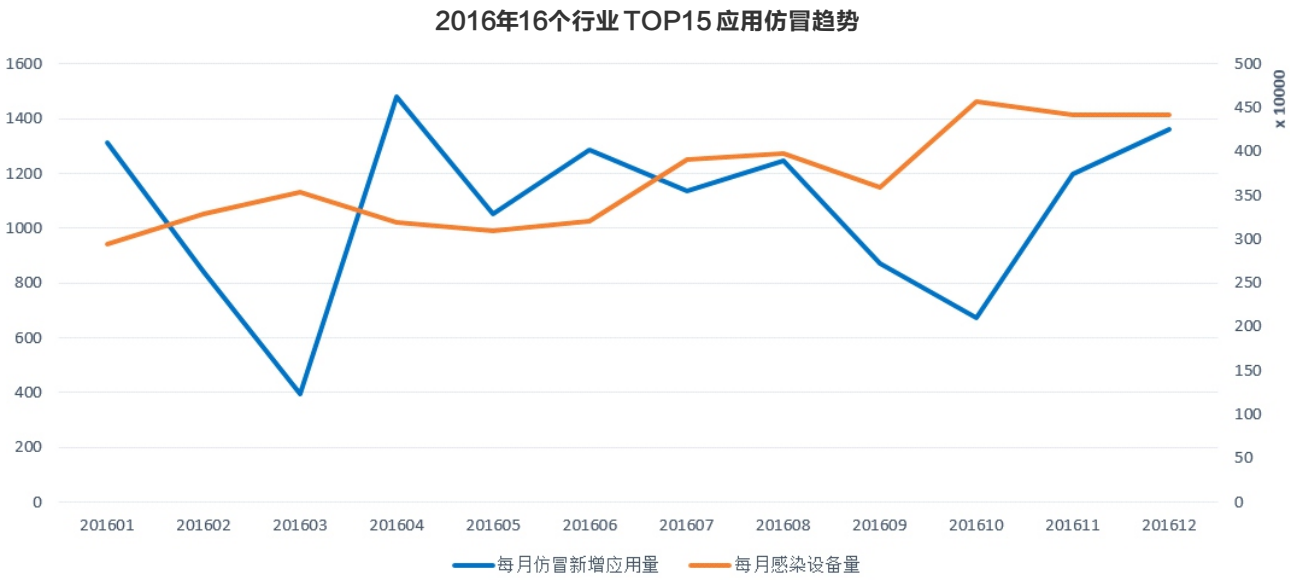
攻击者继续利用静默安装手法在2016年进行恶意推广，这些恶意应用利用系统AccessibilityService静默安装应用。一旦恶意的Accessibility服务被激活，恶意应用将弹出广告，即使用户关闭弹出的广告该应用程序也会在后台下载，随后自动安装推广的恶意应用。阿里聚安全监测到一款名为“WiFi密码查看器(增强版)”的应用滥用AccessibilityService。应用启动后诱导用户开启“WiFi信号增强服”，其实就是开启恶意应用自身的AccessibilityService以查看WIFI密码让恶意应用获得root权限。用户启用恶意应用的该服务之后，手机将疯狂下载该应用云端准备的应用包，并且在手机上自动安装运行。

今年滥用Accessiblity Service服务的病毒数持续上涨，此类病毒的恶意行为包括：自动安装、自动广告点击、应用劫持、浏览器劫持等等。阿里聚安全监测还发现在国内火热的抢红包应用也会利用AccessibilityService实现自动抢功能，黑客利用“自动抢红包”诱导用户开启AccessibilityService控制手机，建议用户在安全渠道下载抢红包软件，以免不必要的损失。

Part / 10

89%的热门应用存在仿冒

从16个行业分类分别选取了15个热门应用，共240个应用进行仿冒分析，发现89%的热门应用存在仿冒，总仿冒量高达12859个，平均每个应用的仿冒量达54个，总感染设备量达2374万台。3月份的仿冒应用量大幅下降，符合黑灰产在春节假期前后的活动较少的规律。

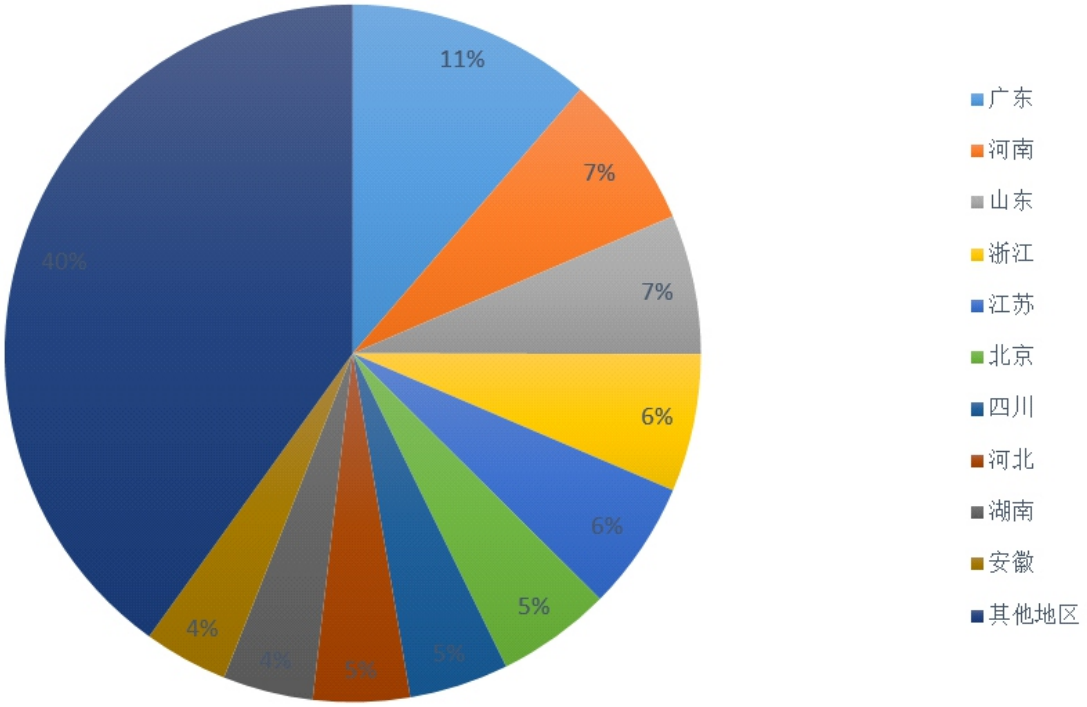


Part / 11

移动病毒和仿冒相辅相成，广东省两者都占首

2016年，广东省的仿冒应用感染设备量最大，占全国的11%。河南省和山东省仿冒应用感染量也非常大，占全国的7%，人口排名居全国前三。北京市作为直辖市，同时又是首都，仿冒应用感染量也很大，占全国的5%。从数据上看，仿冒应用的感染量与各地区的经济发达程度和人口密度有关，说明仿冒应用具有普遍性。

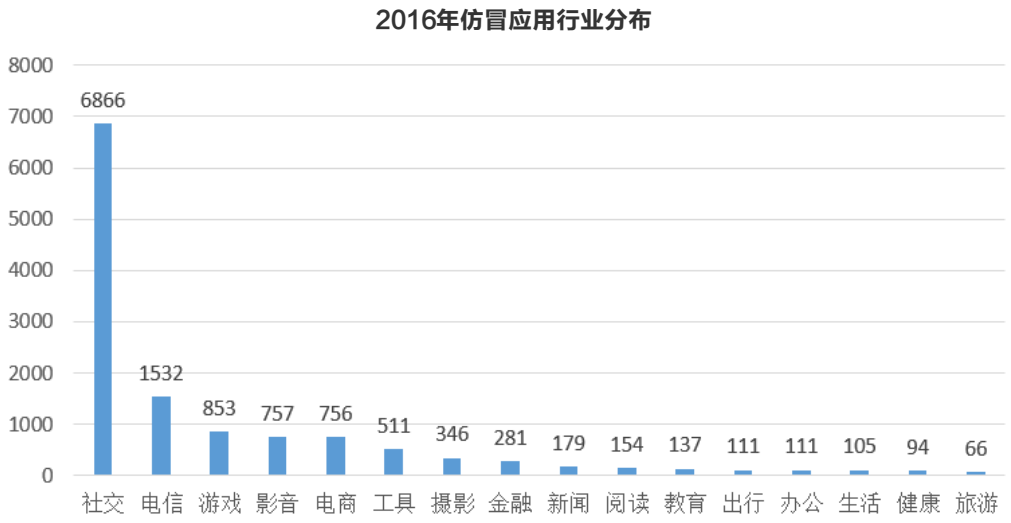
2016年仿冒应用感染量地区分布

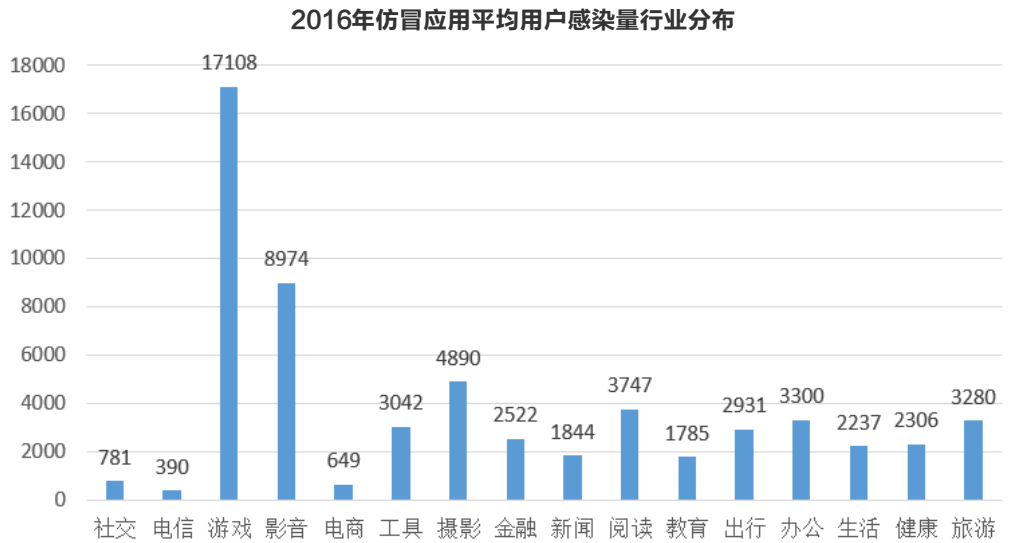


Part / 12

社交行业仿冒应用量最高，但游戏和影音的传播性更强

16个行业分类中，社交类应用的仿冒量达6866个，占总仿冒量的53%，排名第一，其中QQ和微信的仿冒量占社交类的96.7%。电信类应用的仿冒量排名第二，占总仿冒量的12%。电商、影音、游戏、工具、摄影和金融等6个行业分类，也是仿冒的重灾区。游戏和影音的仿冒应用平均感染量较大，说明这两个行业的仿冒应用传播性更强。





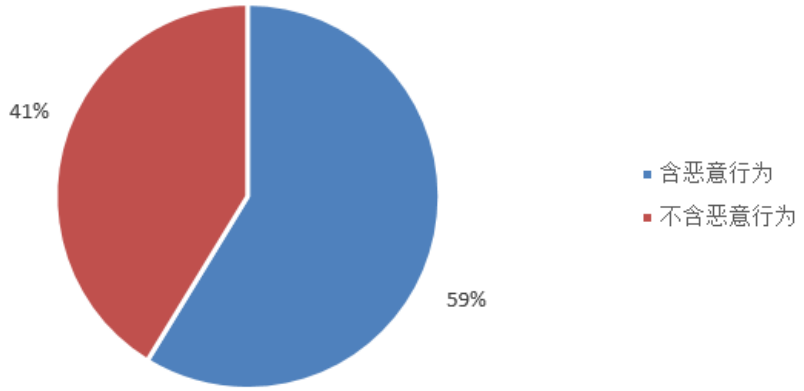
Part / 13

盗版软件、短信劫持、流氓行为、恶意扣费是仿冒应用主要恶意行为

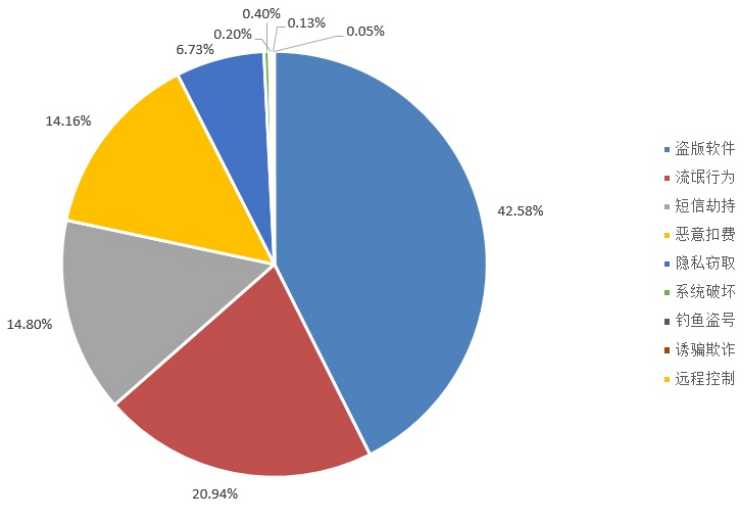
发现的12859个仿冒应用中，55%具有恶意行为。具有恶意行为的仿冒应用，对手机用户的账号、资金和隐私安全存在较大的威胁。45%虽然没有恶意行为，但是这类“山寨”应用产品都会影响到企业的正版权益和应用市场的有序运营。

病毒仿冒应用主要具有流氓行为、恶意扣费、短信劫持或隐私窃取等恶意行为，其中短信劫持的风险最高。

2016年病毒仿冒应用占比



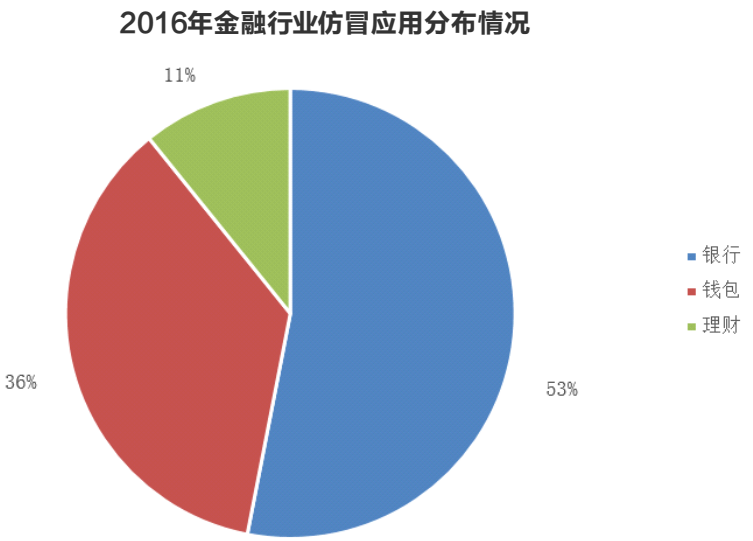
2016年病毒仿冒应用量风险分布



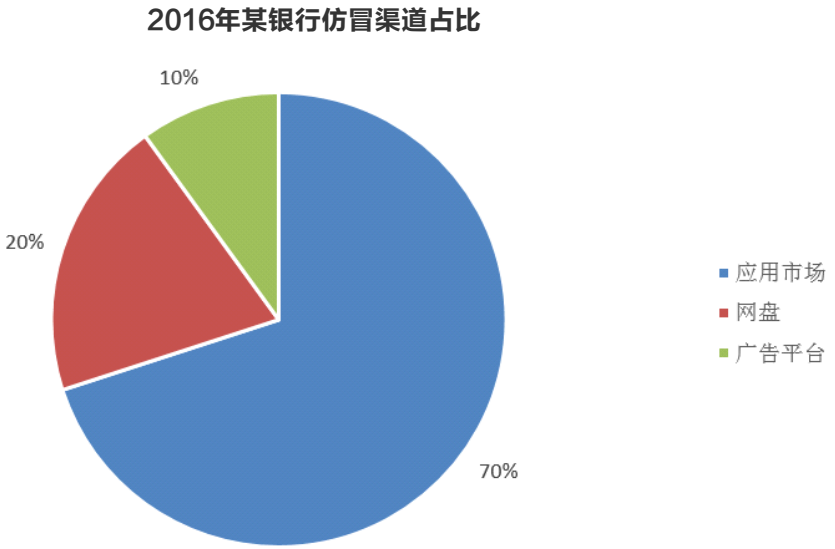
Part / 14

金融行业银行类仿冒居多，某银行仿冒应用全部具有短信劫持行为

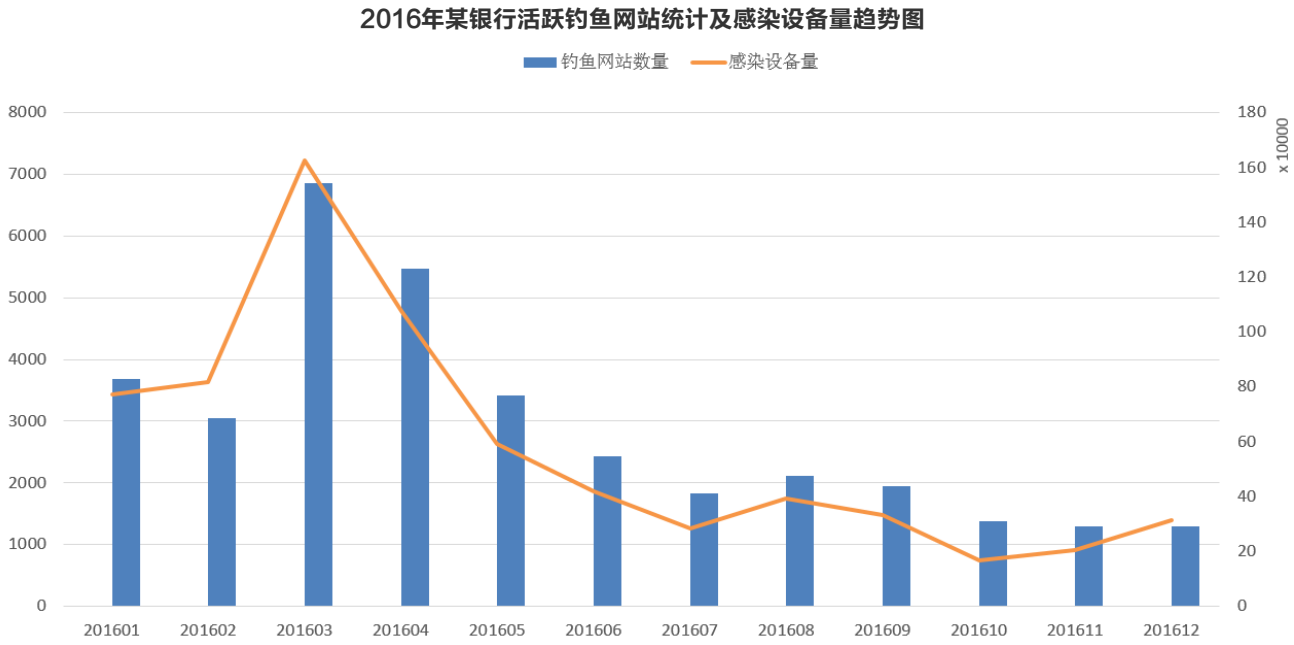
金融行业选取银行、钱包和理财3个子分类，分别选取10个热门应用进行分析，共发现仿冒应用407个。银行类仿冒应用占53%，钱包类仿冒应用占36%，理财类仿冒应用占11%。



在本次分析中，某银行共发现30个仿冒应用，全部具有短信劫持行为，感染设备量为33863台，感染用户主要分布在广东、北京和江苏等省份。该案例中的主要分发渠道是应用市场，网盘与广告平台。



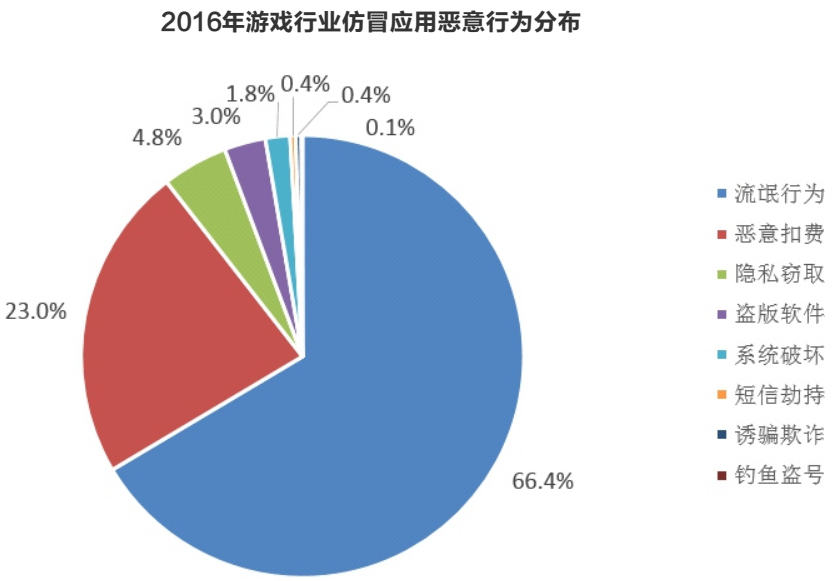
为防止网民误上钓鱼网站导致财产受损，2016年公安部加强了与相关银行组织的专项行动,并采取了一系列防控措施,有效遏制了此类案件的发生，4月开始呈下降趋势，有效降低了感染设备的数量。



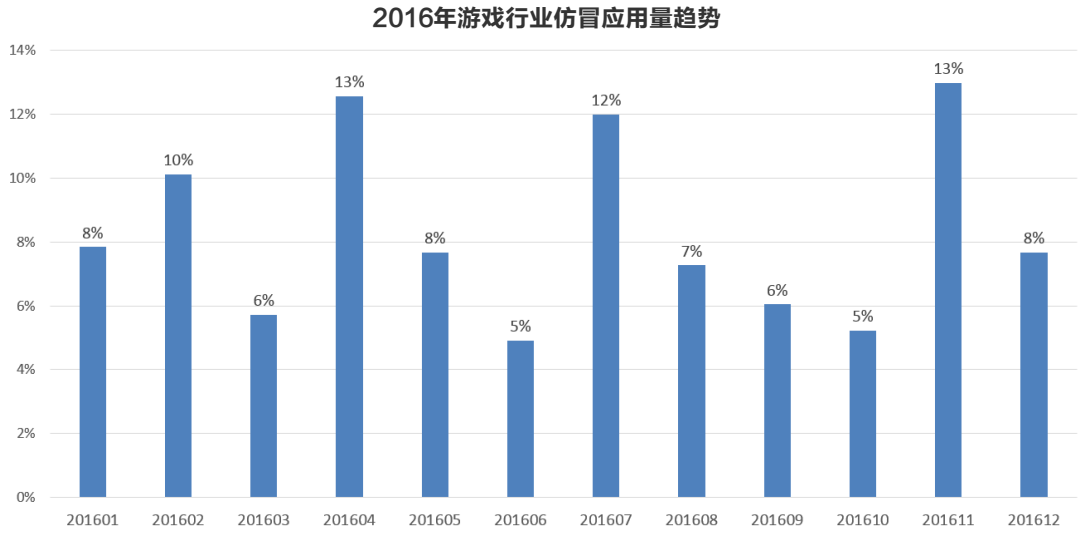
Part / 15

游戏行业仿冒应用分析

游戏行业选取了Top30个热门应用进行分析，共发现仿冒应用1225个。流氓行为的占比最高达到66.4%，其次为恶意扣费达到23%。



由于游戏行业应用的更新迭代较为频繁，热门应用活跃周期不长，所以在短时间内对仿冒应用的打击会有成效，但是仍然无法控制住对新的应用的仿冒趋势，整年呈波浪式高低起伏的态势。



Part / 16

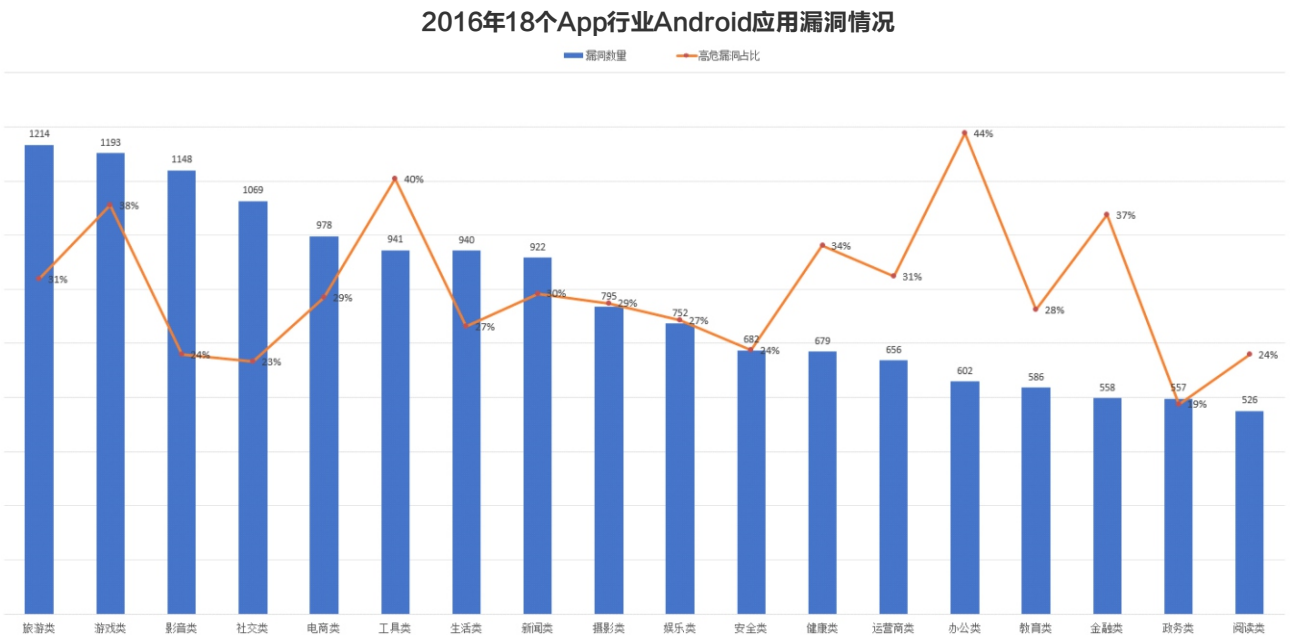
阿里聚安全移动安全扫描器创新迭代快速，帮助企业提高前置安全感知能力

阿里聚安全移动安全扫描器2016年全年成功提供的扫描服务305909次，平均每天提供的服务838次，检测漏洞数量达17698883个，全年所有扫描的App中有壳的App占比16.54%，产品迭代发布次数21次，新增规则16条。其中启发式规则扫描可检测外部可控数据对应用内部逻辑的影响，扫描器能够根据socket、网络、intent传入的数据，进行各种判断，进而判断是否存在可以被恶意用户使用的漏洞，涵盖了网络钓鱼、外部操作系统文件、命令执行、反射操作、启动私有组件（activity、service等）等各种类型的漏洞。此外，新增的拒绝服务扫描规则还可支持扫描动态注册的组件是否能够引起拒绝服务漏洞。

Part / 17

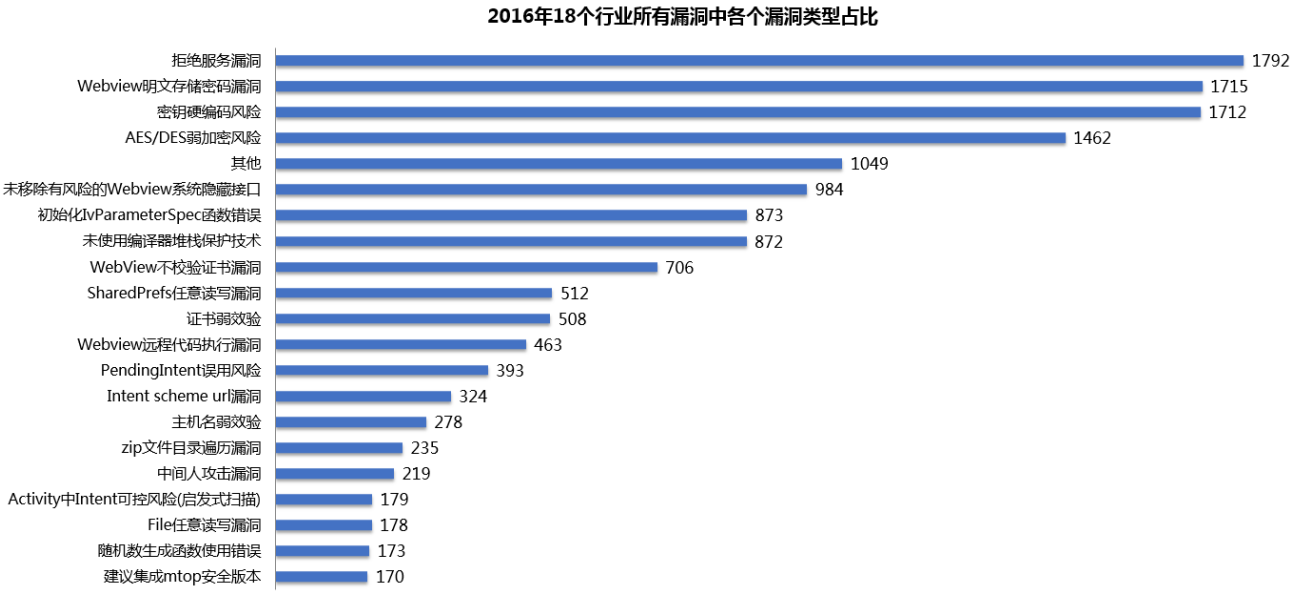
18个行业的Top10应用中98%的应用都存在漏洞，但Webview远程执行代码漏洞迅速下降

为分析移动应用各行业的漏洞情况，我们在第三方应用市场分别下载了18个行业的Top10应用共计180个，使用阿里聚安全漏洞扫描引擎对这批样本进行漏洞扫描。18个行业的Top10应用中，98%的应用都有漏洞，总漏洞量14798个，平均每个应用有82个漏洞。旅游、游戏、影音、社交类产品漏洞数量靠前。但是高危漏洞占比最高的依次是办公类、工具类、游戏类和金融类。企业在移动数据化进程过程中更需注意员工在使用这些行业App时的安全威胁。

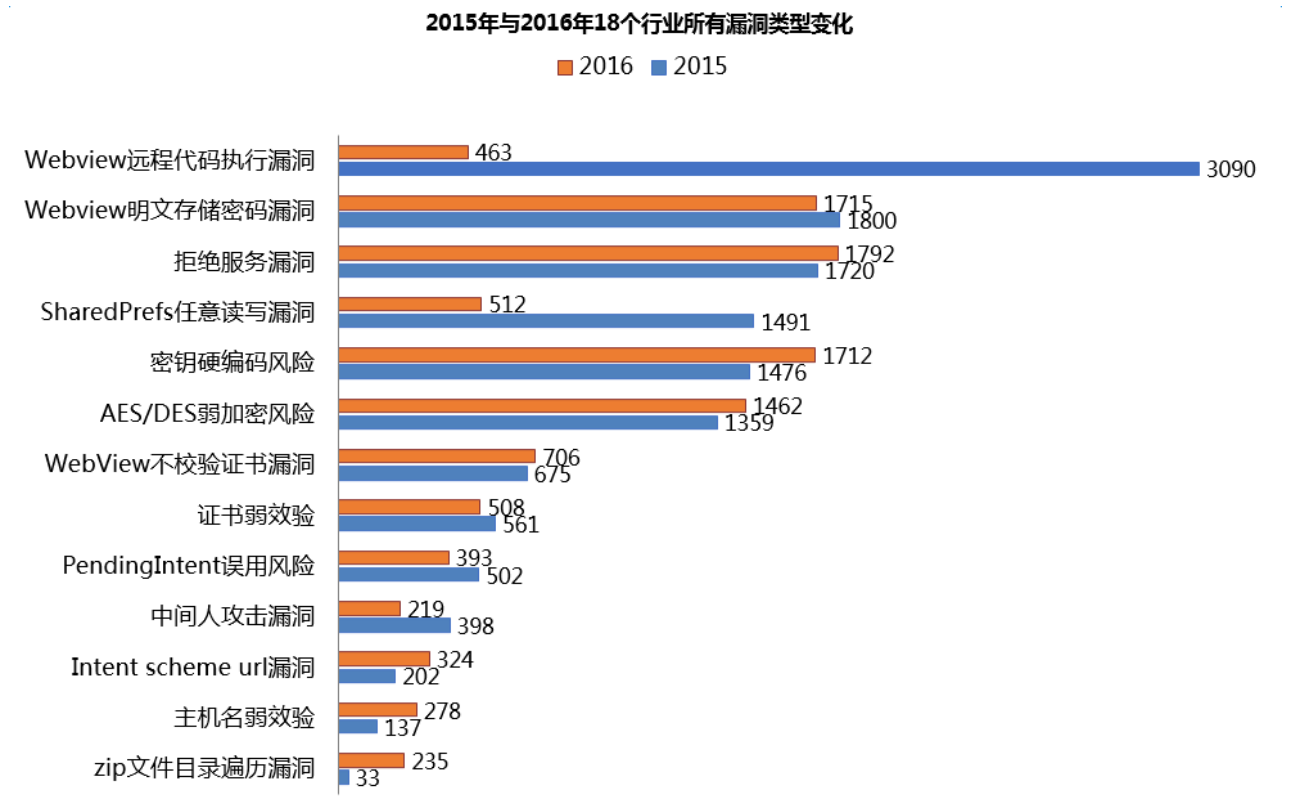


其中漏洞类型主要集成中“拒绝服务”、“Webview明文存储密码”、“密钥硬编码风险”及“AES/DES弱加密风险”中，“密钥硬编码风险”和“AES/DES弱加密风险” 漏洞会让基于密码学的信息安全基础瓦解，因为常用的密码学算法都是公开的，加密内容的保密依靠的是密钥的保密，密钥如果泄露，对于对称密码算法，根据用到的密钥算法和加密后的密文，很容易得到加密前的明文；对于非对称密码算法或者签名算法，根据密钥和要加密的明文，很容易获得计算出签名值，从而伪造签名。

这里建议企业用户在开发App过程中，通过阿里聚安全的漏洞扫描来检测应用是否具有密钥硬编码风险，使用阿里聚安全的安全组件中的安全加密功能保护开发者密钥与加密算法实现，保证密钥的安全性，实现安全的加解密操作及安全签名功能。



同时我们还注意到2016年相比2015年，Webview远程代码执行漏洞量占比迅速下降，从原来的3090个下降到463个，降低将近85%，主要原因是Android 4.2版本市场份额已经下降到7%；另外由于全网部署HTTPS的企业增加，导致中间人攻击漏洞也下降50%。

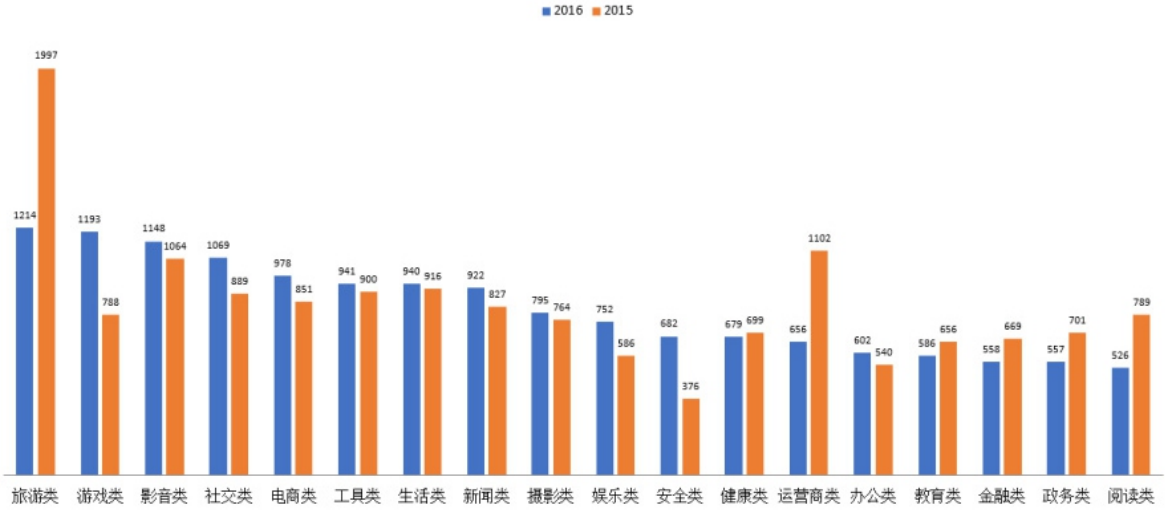


Part / 18

逐利是黑产本性，游戏行业漏洞上升较快

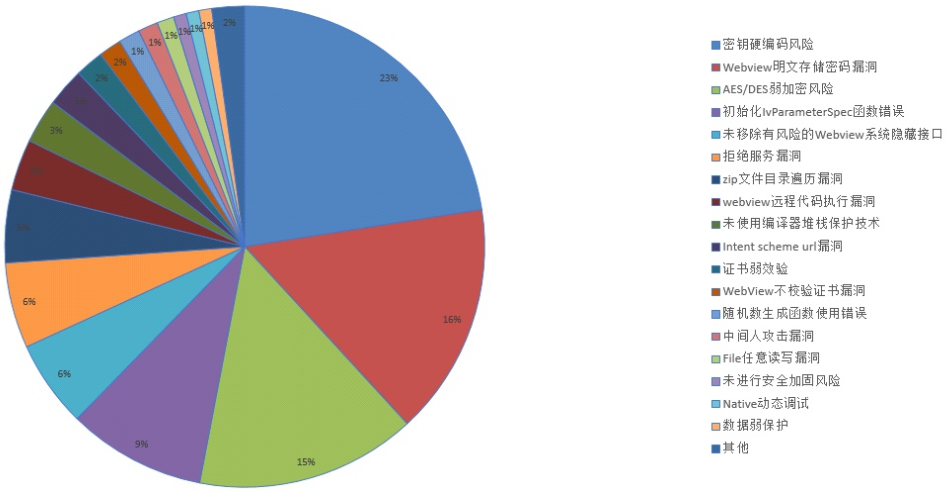
我们对比了2016年和2015年行业移动应用漏洞，2016年旅游类和运营商类的App应用漏洞呈明显减少趋势，而作为有大量利益可图的游戏类应用的漏洞2016年明显增加，从788个增加到1193个。

2015年和2016年18个行业Android应用漏洞对比情况



游戏行业漏洞类型占比最高的是“密钥硬编码风险”，其次是”Webview明文存储密码漏洞”及“AES/DES弱加密风险”。

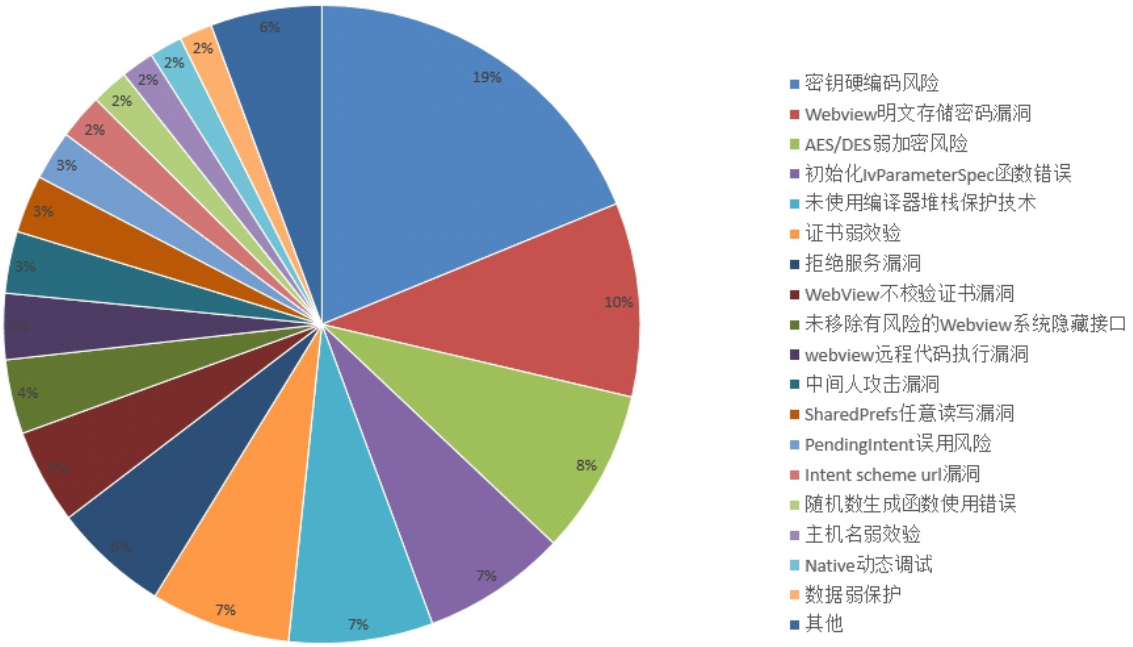
2016年游戏类应用漏洞类别分布



密钥硬编码在代码中，根据密钥的用途不同，可导致不同的安全风险，有的导致加密数据被破解，数据不再保密，有的导致和服务器通信的加签被破解，从而引发各种血案。阿里聚安全在审计某游戏App和服务器通信时接口采用HTTP通信，数据进行了加密，并且对传输参数进行签名，在服务器端校验签名以检查传输的数据是否被篡改，但是加签算法和密钥被逆向分析，可导致加签机制失效，攻击者可任意伪造请求包，若结合服务器端的权限控制有漏洞，则可引发越权风险等。

金融行业也存在与游戏行业类似的问题，“密钥硬编码风险”、“Webview明文存储密码”及“AES/DES弱加密风险”漏洞比率占据高位。

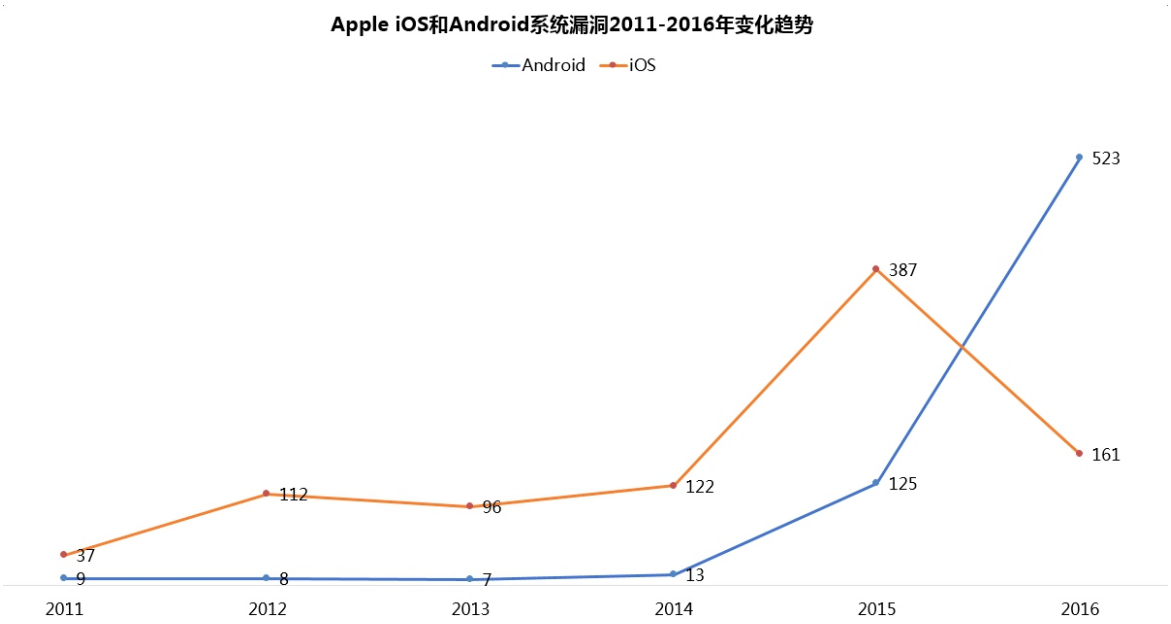
2016年金融类应用漏洞类别分布



Part / 19

安全闭环的Apple生态系统比Android系统表现出更安全的态势

2016年，Apple公司披露的安全漏洞呈现出明显下降的趋势，单从流行的iOS系统，就从2015年的387个漏洞下降到2016年的161个，下降一倍还多，而Android系统相反，从2015年的125个漏洞上升到523个。



闭环的Apple生态系统正在安全方面体现出其优越性，硬件、软件、安全框架的闭环使得iOS系统比Android系统更容易检测，修复，防御。而Android的大多数ROM都经过厂商的定制，使得大多数人无法及时更新到最新的操作系统，加上系统分布碎片化，极大地降低了Android的安全性。此外2015年漏洞数量使得iOS厂商更密切地关注其产品和代码，更谨慎的实施SDL实践，识别并修复漏洞，2016年的漏洞的下降趋势可能表明这些努力正显成效。

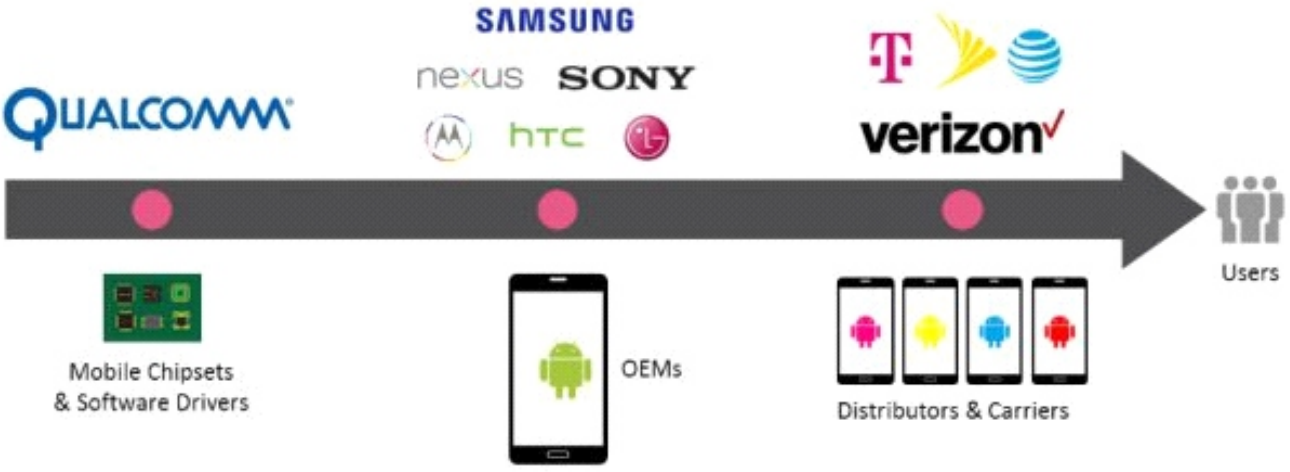
Part / 20

可能永远不会修复的漏洞影响9亿安卓用户

2016年中，CheckPoint安全公司研究员披露影响高通GPU芯片的Quadrooter漏洞，高通公司的芯片在安卓设备中的市场占有率高达65%，超过9亿台设备受此漏洞影响，攻击者可以利用这四个漏洞提升权限，获取root权限。影响的设备包括最流行的安卓设备如：

- BlackBerry Priv
- Blackphone 1 and Blackphone 2
- Google Nexus 5X, Nexus 6 and Nexus 6P
- HTC One, HTC M9 and HTC 10
- LG G4, LG G5, and LG V10
- New Moto X by Motorola
- OnePlus One, OnePlus 2 and OnePlus 3
- Samsung Galaxy S7 and Samsung S7 Edge
- Sony Xperia Z Ultra

修复漏洞所有设备需要相当长的时间，Qualcomm芯片组固件补丁需要由Android OEM供应商集成到它们的Android操作系统的自定义版本，然后到达移动运营商，最终决定适当的时间提供给最终用户，这会导致有些用户可能永远不会修复。[4][5]



Part / 21

折断的翅膀——WLAN芯片引入大量提权漏洞

Wi-Fi驱动在今年被披露大量安全漏洞，包括博通、高通、Mediatek等厂家提供的芯片，此类漏洞所使用到的系统调用权限低，漏洞涉及影响范围广，包括但不限于华为，谷歌，以及国内使用此类wlan芯片等大多数主流厂商的移动设备。

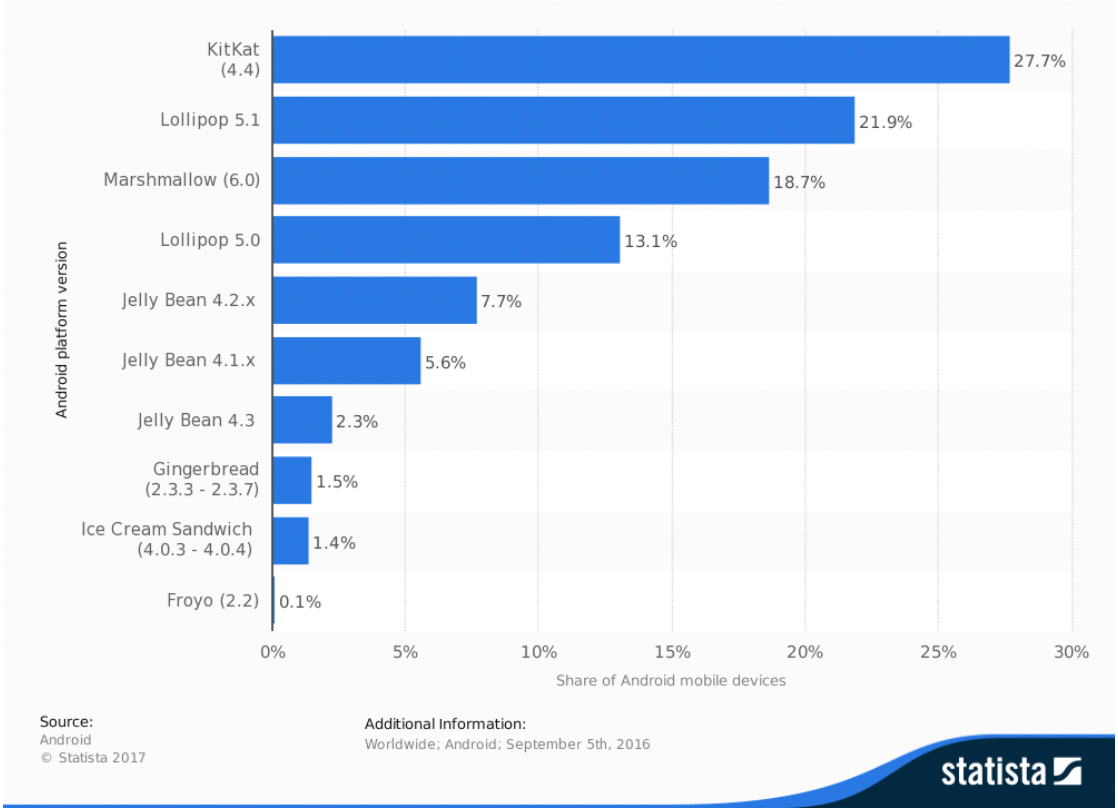
Wi-Fi驱动自身逻辑相对复杂，并且多依赖于各个wlan厂商的技术实现，不同的技术厂商技术实力不一致，对代码安全的重视程度也有高低之分，难免会存在良莠不齐的情况。同时，同一厂商的不同芯片往往也会采用相同的Wi-Fi驱动或是相似的驱动代码，这也使得Wi-Fi驱动漏洞的覆盖面和影响更为扩大，同一个漏洞往往会影响多款不同型号的手机。建议企业用户及时跟进相关安全补丁，或请专业安全团队协助处理。

Part / 22

对于移动安全漏洞，企业需要更多关注NDAY漏洞

CVE-2015-1805漏洞，存在于在linux内核3.16版本之前的fs/pipe.c当中,由于pipe_read和pipe_write没有考虑到拷贝过程中数据没有同步的一些临界情况,造成了拷贝越界的问题,可导致系统权限提升，该问题早在2014年就被发现，但直到2015年才被列为安全问题。而在2016年3月之前，该漏洞的严重程度一直被低估。Google在2016年3月18日为此问题单独发布了Android安全公告，并在2016年4月的Nexus公告中修复了该问题。在此之前，大量的Android设备，包括所有的Nexus设备都受到该漏洞的影响。据了解，该漏洞被多个root工具用以在Android设备上进行提权，影响广泛。移动设备修复过程缓慢，碎片化严重的问题，使移动安全上的NDAY漏洞体现出更强的生命力。Gartner预测，“到2019年，更多的企业将在企业发布的移动设备上部署移动威胁防御功能。企业在防御移动安全威胁时，需要更多的关注此类漏洞”。

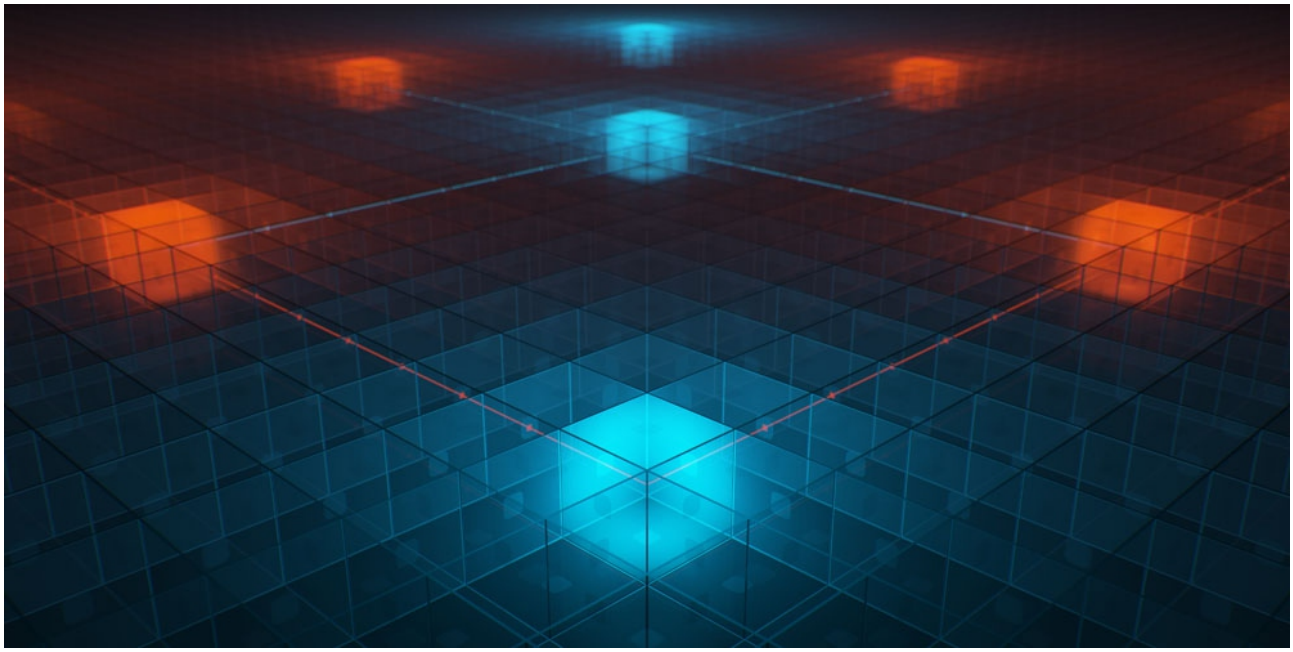
至2016年9月Android手机所有者使用的操作系统分布



Part / 23

只要接入网络就可能被攻击

来自加州大学河滨分校以及美国陆军研究实验室的研究人员，在2016年8月举办的USENIX安全大会上发表了题为《Off-Path TCP Exploits: Global Rate Limite Considered Dangerous》一篇论文。本文提到的漏洞是由于为防止 “blind in-window”攻击RFC5961引入Challenge ACK机制，但Linux 内核在实现该RFC文档时引入了安全问题。攻击者利用该漏洞在不需要利用中间人攻击的方式，可劫持未加密Web流量，注入恶意负载或者破坏如Tor连接一类的加密通讯。此漏洞影响Linux Kernel 3.6至最新版本，也就是说安卓4.4版本以上均存在该问题(80%安卓设备)，由于大量App中建立的是与服务器的长连接，导致可被利用的场景会有更多。



Part / 24

与操作系统和软件无关的硬件漏洞攻击出现—— Drammer

Drammer可以说是一种利用硬件芯片设计缺陷针对Android设备的攻击方式，与操作系统和软件无关。攻击者可以利用该漏洞获得root权限。内存厂商为了能让内存芯片存储更多的数据，于是将内存中的DRAM（The Dynamic Random Access Memory）cell越做越小并且离的越来越近，从而导致相邻的cell在通电的过程中会受到影响。因此，如果我们不断的访问某个位置上的内存，就可能会造成相邻的内存进行位翻转。随后Google project zero还通过PC上的linux提权，证明了这种现象的确存在并且可以用来进行攻击（https://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html）并将这种攻击方式称为RowHammer。该漏洞发现不光是linux和Android，Windows, OS X和iOS应该也是受影响的。

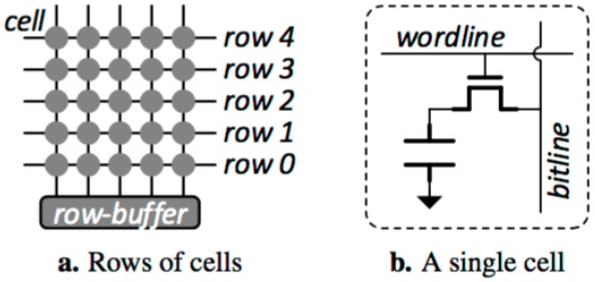


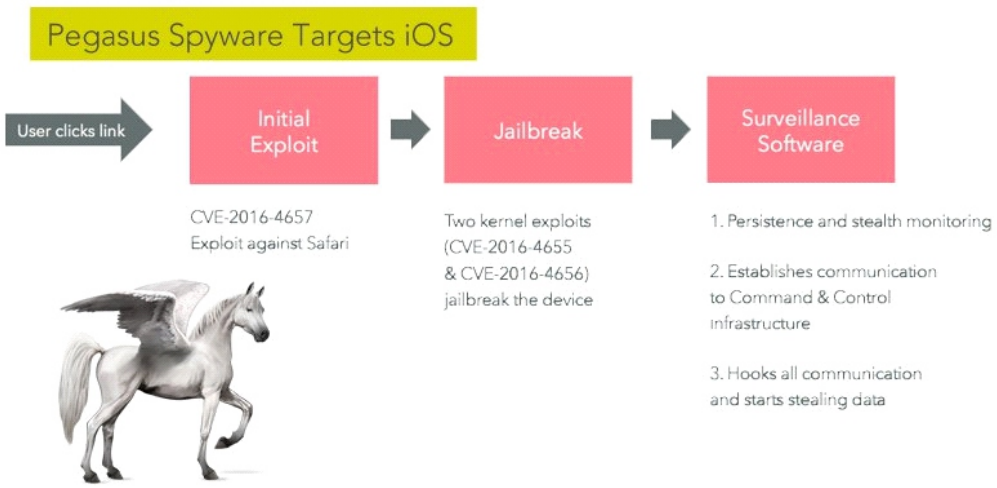
Figure 1. DRAM consists of cells

阿里聚安全认为对于企业用户，面对企业移动信息化到来，在面对更多移动设备漏洞威胁时对要接入公司内网的终端设备进行身份认证是必要的手段之一。

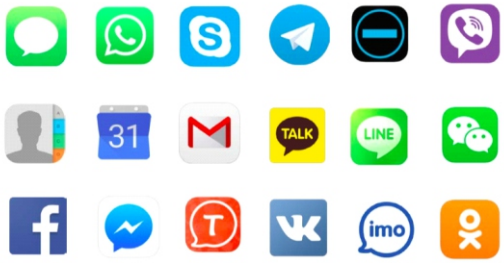
Part / 25

PEGASUS——三叉戟攻击链，最复杂精密的iOS APT攻击

该攻击链是在对阿联酋的一位人权活动家进行APT攻击的时候被发现。整个攻击链由三个漏洞组成：JS远程代码执行（CVE-2016-4657），内核信息泄露（CVE-2016-4655），内核UAF代码执行（CVE-2016-4656）。



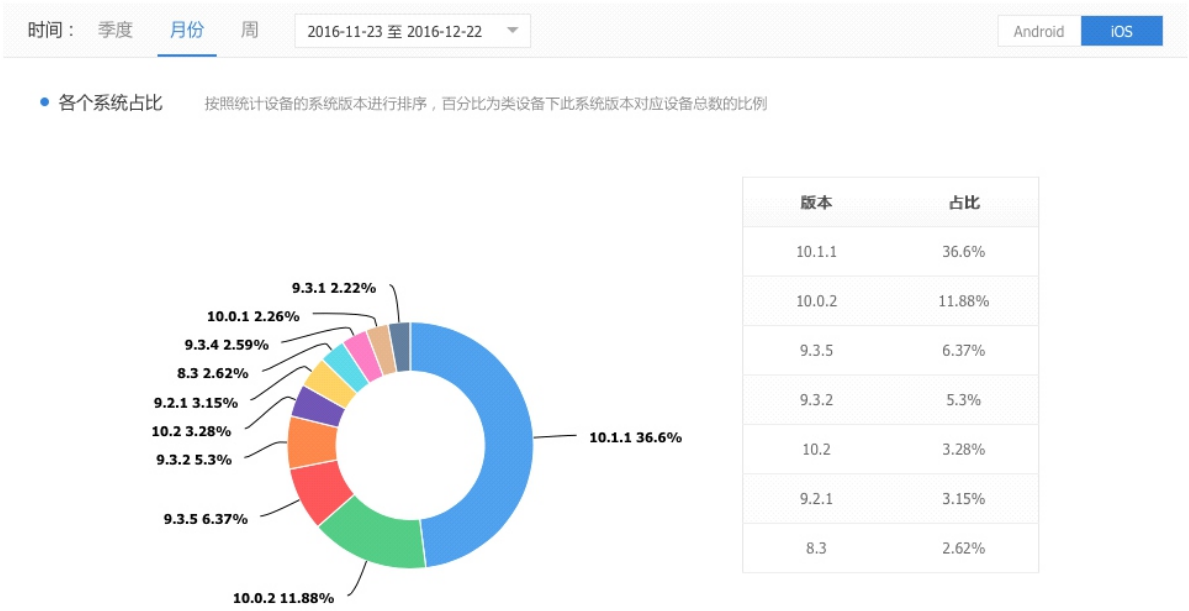
利用该攻击链可以做到iOS上的远程完美越狱，完全窃取Gmail, Facebook, Skype, WhatsApp, Viber, FaceTime, Calendar, Line, Mail.Ru, Wechat SS, Tango等应用的敏感信息。PEGASUS可以说是近几年来影响最大iOS漏洞之一，也是我们认为最复杂和稳定的针对移动设备APT攻击，可以认为是移动设备攻击里程碑。利用移动设备集长连接的Wi-Fi,3G/4G，语音通信，摄像头，Email，即时消息，GPS，密码，联系人与一身的特性，针对移动设备的APT攻击会越来越多。



Part / 26

iOS可公开利用的漏洞持续披露用户面临更大风险

阿里聚安全观察到2016年的公开可利用的漏洞数量是非常巨大的，相对2015年可以说是有了一个指数级的增长。虽然苹果更新系统的速度非常快并且无法降级，但随着老设备（iPhone 4s及以下已无法升级iOS 10）越来越多，并且用户对新系统期望越来越低，iOS设备的更新率已经变得非常缓慢。



版本	占比
10.1.1	36.6%
10.0.2	11.88%
9.3.5	6.37%
9.3.2	5.3%
10.2	3.28%
9.2.1	3.15%
8.3	2.62%

根据某专业移动分析平台2016年12月的数据可以看到，仅有3.28%的设备更新了最新版的iOS 10.2。这意味着96.72%的设备都有被mach_portal漏洞攻击的风险，（mach_portal漏洞可参看蒸米写的“黑云压城城欲摧——2016年iOS公开可利用漏洞总结”一文（https://jaq.alibaba.com/community/art/show?articleid=687)。我们相信，在新的一年，iOS的漏洞数量还会持续增加，并且随着漏洞利用技术的公开，黑灰产也极有可能利用漏洞对用户进行攻击，希望广大用户一定要注意自己iOS设备的安全。

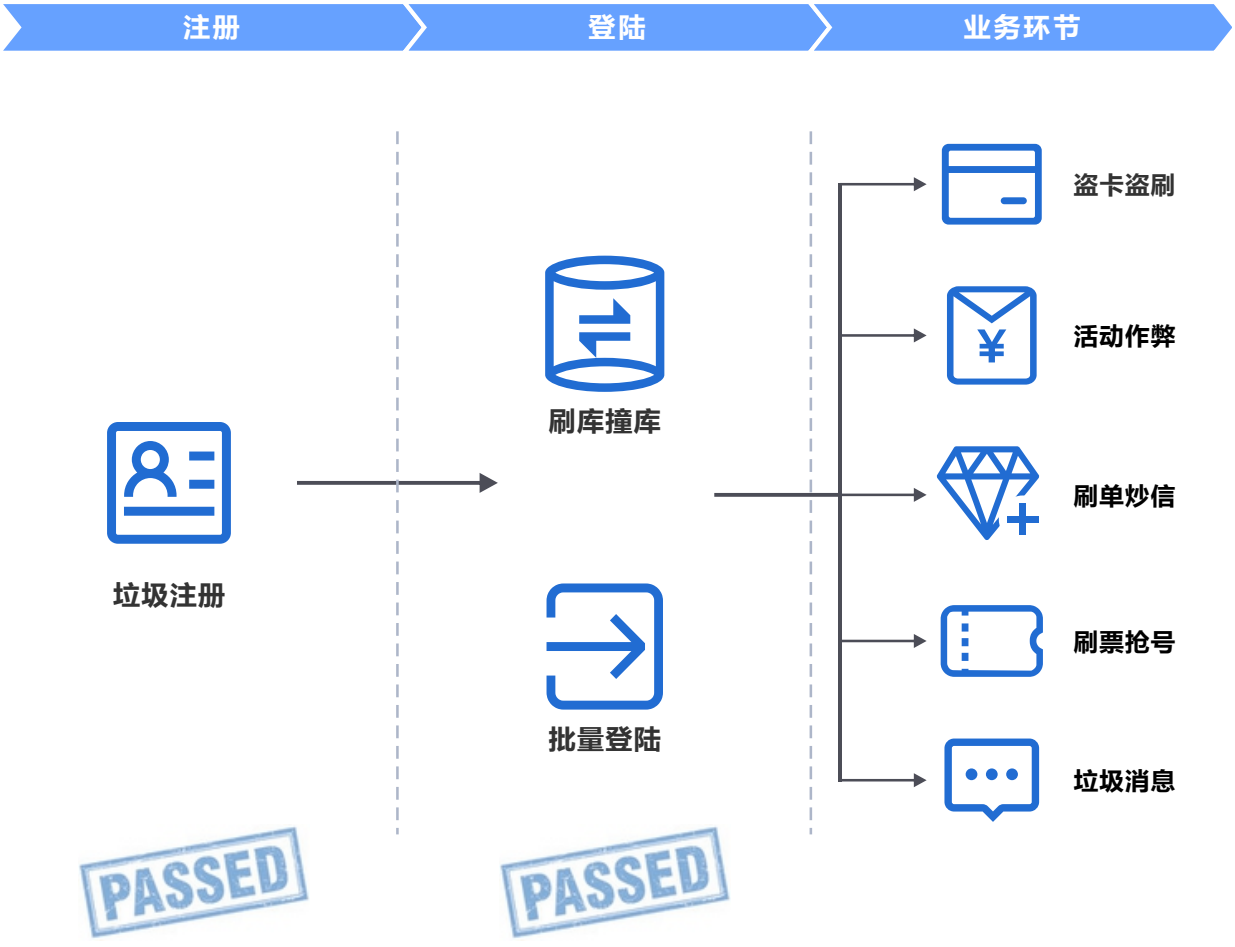
Part / 27

互联网业务风控或将成为下一个风口

Part / 28

羊毛党、黄牛党在2016年成为互联网业务发展过程中最大的毒瘤

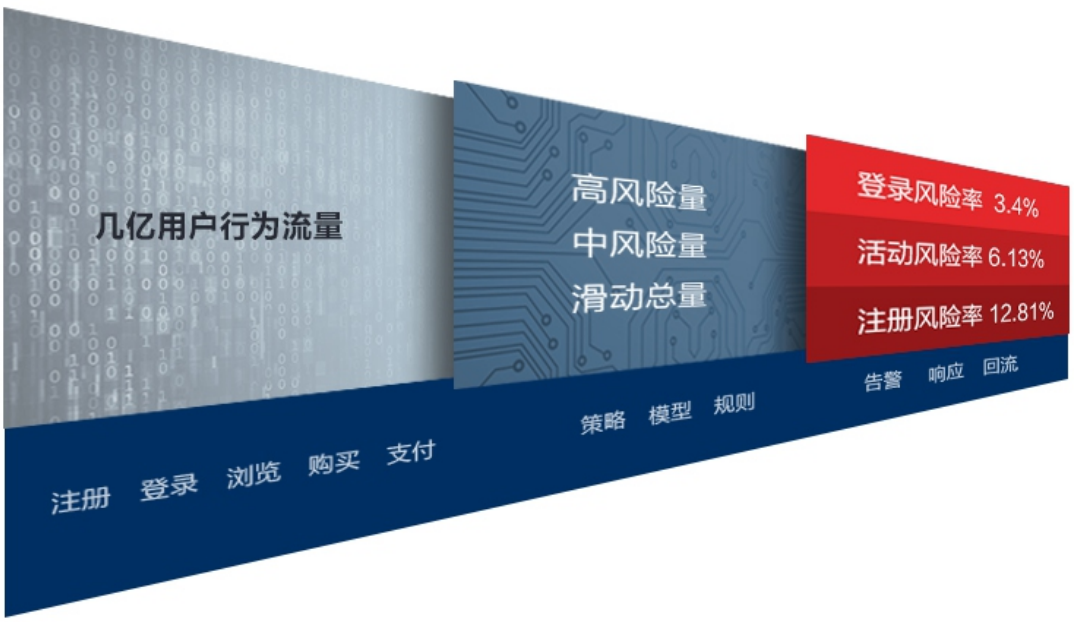
2016年在各种互联网业务活动中，羊毛党、黄牛党继续盛行，各种没有安全防控的红包/优惠券促销活动，会被羊毛党以机器/小号等各种手段抢到手，基本70%~80%的促销优惠会被羊毛党薅走，导致商家和平台的促销优惠最终进入了羊毛党的口袋。黄牛党能够利用机器下单、人肉抢单，将大优惠让利产品瞬间抢到手，然后高价格售出赚取差价。大规模的批量机器下单，还会对网站的流量带来压力，产生类似DDOS攻击，甚至能够造成网站瘫痪。此外使用简单维度的密码验证手法已经演变成使用复杂机器人猜测密码的技术，来逃避简单的策略防御。企业需要更多维度、指标，使用更复杂的规则、模型进行防御。



Part / 29

在干草堆里捞针，数据、算法、算力为王

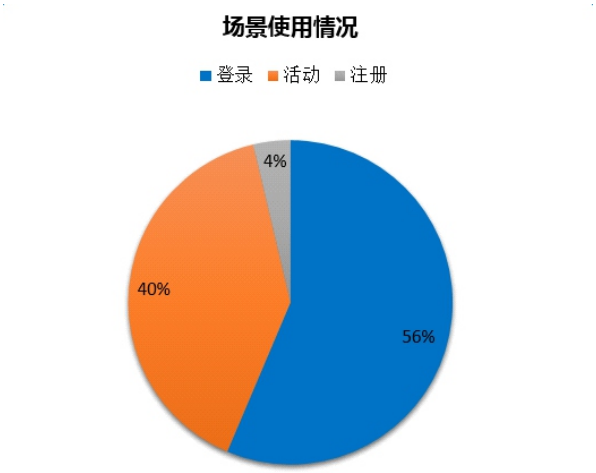
风控系统中往往遇到请求数据庞大、采集容易分析难，特征不够，建模准确度低，大量误报和漏报的威胁。安全团队经常必须面对筛选数十亿的用户活动来判断黑产用户的可疑活动。阿里聚安全基于阿里大数据计算能力,通过业内领先的风险决策引擎,解决企业账号、活动、交易等关键业务环节存在的欺诈威胁,降低企业经济损失。通过强大的数据风控，阿里聚安全能够从每天百亿级的交易、近百PB的数据中实时识别和处置恶意注册、盗号账户、欺诈、活动作弊等多种业务风险。

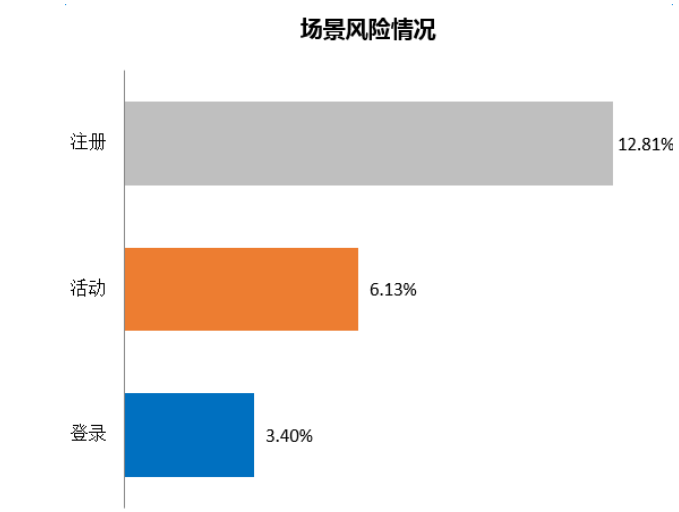


Part / 30

自动注册为王，细化防御才能精确打击

登录和活动一直占据互联网业务处理量的大部分，但由于注册是所有业务入门的门槛，因此面临的风险情况也是最严峻的，平均100个注册用户里，就有13个垃圾用户。





垃圾注册已经通过自动程序或者纯人力各种辅助工具大量注册，绕过注册防御手段一直是黑产持续研究的方向，风控系统在抵御黑产垃圾注册时，阿里聚安全认为更精细的防御才能更精确的打击模拟注册行为：如很多黑产在Web端操作的时候，会使用特殊的操作系统或浏览器，例如IE8，甚至IE6。这些低版本浏览器防控能力弱，并且服务提供者从中能够获取的内容少，这正中黑产下怀。另外一些黑产在进行垃圾注册的时候，要把浏览器嵌入到注册软件中 。这样的话，从浏览器的分辨率参数来看就是一个怪异的小尺寸。再比如，有一些H5网页，正常人几乎不会在电脑上操作。但是黑产为了速度和自动化，一定会在电脑上运行。这些参数，都可以辅助系统判定网络那头的操作者，究竟是人还是机器。

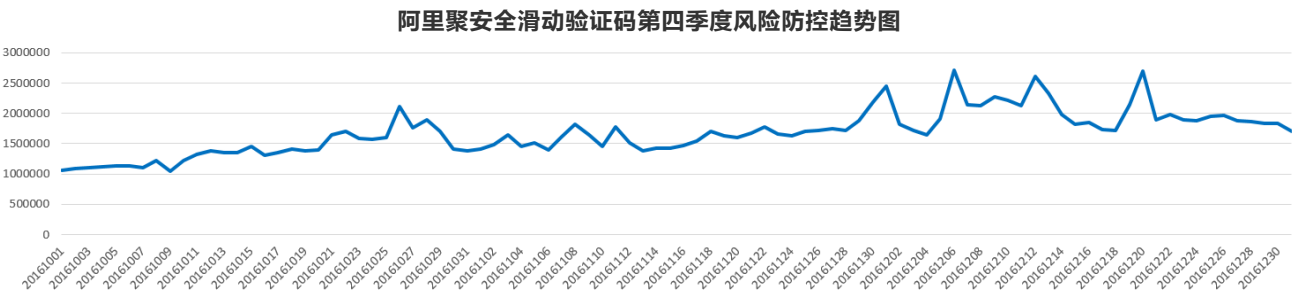
Part / 31

暗号谍战——滑动验证的混淆加密切换

滑动验证码作为对抗人机黑产的重要手段，对筛查出来的“灰黑用户”需要进一步精细判断。进化的滑动验证码已经不再基于知识进行人机判断，而是基于人类固有的生物特征以及操作的环境信息综合决策，来判断是人类还是机器。并且不会打断用户操作，进而提供更好的用户体验。验证码系统在对抗过程中，感知到风险，需要企业实时切换混淆和加密算法，极大提高黑产进行破解的成本。

阿里聚安全的人机识别系统，接口调用是亿级别，而误识别的数量只有个位数。除了误识别，我们的技术难点还在于如何找出漏报。一般情况下，会对整体用户流量的“大盘”进行监控，一旦监测到注册或登录流量异常，我们的安全攻防技术专家就会紧急响应。这种响应速度是小时级别的。

另外黑产通过刷库撞库也体现出业务时序的不同而不同。以2016年Q4为例，在双十一之前，黑产主要精力用于各平台的活动作弊，而过了双十一，刷库撞库风险就开始持续走高，稳定占据了所有风险的一半以上。

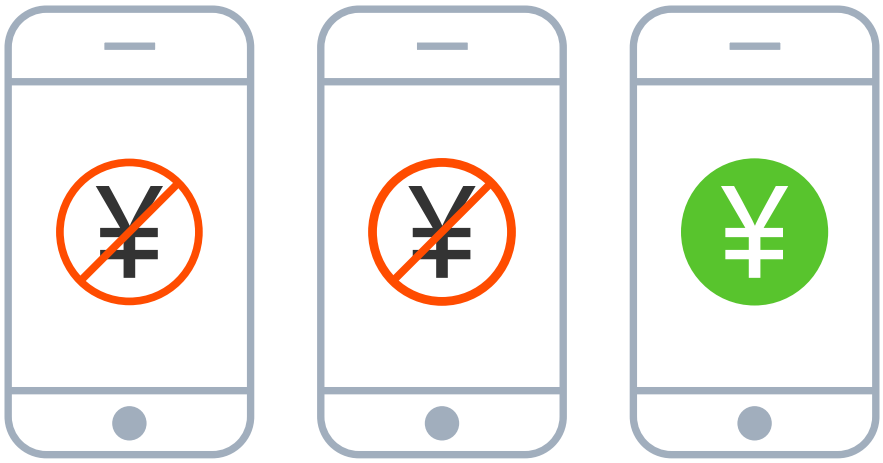


Part / 32

2016年移动欺诈损失超数亿美金

目前移动应用通过资源换量、搜索平台、广告网络及代理商、直接推广及自然安装等渠道来推广和互动。但推广者发现投入的费用反映的推广数据良好，但是沉淀到真是用户却表现非常不乐观。大量的渠道欺诈使得移动应用推广者损失巨大，根据某平台分析，2016年移动欺诈金额已经超数亿美金。

常用移动欺诈通过机刷、模拟器、改机工具等手段作弊，如通过一键生成改机软件修改手机硬件参数IMEI、MAC、蓝牙地址等，伪造新手机多次安装激活App；通过脚本批量操作各种安卓模拟器如天天模拟器、海马玩模拟器、夜神模拟器等，反复进行机刷-App安装-App激活等操作。阿里聚安全使用稳定的设备指纹技术 + 大数据分析，能准备识别各种作弊手段和作弊设备。为用户节约推广成本、时间成本、开发成本，保障推广者获取真实的用户数据为业务服务。



Part / 33

大规模图搜索和实时计算成为风控系统核心竞争力

对于承载3万亿GMV的淘系平台来说，面临着更加严峻的挑张。各类的促销，优惠商品，特别是像双11这类的大促，吸引来了各路黄牛，八仙过海各显神通。风控系统如何快速识别黑产团伙，是衡量风控系统是否强壮的核心能力。阿里聚安全使用的算法主要是以大规模图挖掘（Graph Mining）和在线学习（Online Learning）为核心，通过系统监控预警以及在线分析的方式将模型算法和人工运营有效结合起来，不仅能高效识别作弊行为并进行了有效地干预，同时还可以有效控制各种风险。

大规模图挖掘则是通过跳出行为“局部性”的方法考虑行为的“全局性”来深挖“精刷”类型的作弊手段。比如概率图模型对用户行为路径进行时间序列建模（假设正常用户的行为轨迹的时间序列是服从某种概率分布，异常的行为轨迹在某些点上服从其他概率分布），对那种机器刷单或者固定模式刷单能非常有效地识别。

期中标签图模型是大规模图挖掘的一种算法，是在大规模属性图结构上做社区和团伙挖掘，和以往的分类等机器学习算法不同的是，在属性图上有效地利用标签传播算法分析用户的行为可以挖掘出很多其他算法识别不到的同机团伙和协同炒作团伙。标签图传播模型就可以来做团伙刷单的识别，对炒信平台隐蔽性高组织性强的“精刷”模式的识别非常高效准确。为了进一步验证算法模型的精准性，反作弊体系也增加了实时干预模块来做交叉验证和分析，主要包括专家知识、人工举报、异常监控和人工评测，这些外部数据源加工处理后可以作为验证数据动态帮助模型进一步优化，对虚假交易的数据监控和算法识别上应用了覆盖全链路大数据的实时分析处理能力以及大规模图搜索技术来鉴别作弊行为。

Part / 34

快速接入与快速自动响应是营销反作弊系统重要指标

面对高QPS场景实时准确的识别羊毛党、黄牛党，营销反作弊系统在效率上、精准性、实时性面临着巨大的挑战，这些挑战包括：

效率上：业务活动都有各自的玩法，玩法多达几十上百种，在有限的人力下如何能迅速的适配接入各种形式的活动防控。
精准性：既要有效识别羊毛党、黄牛党，又不能误伤正常用户而影响GMV。
实时性：在秒杀、秒红包的场景下，让正常用户无感知，必须在几毫秒内完成反作弊扫描。

攻防行为不断升级，如何快速应对变化的新型攻击。如何在业务系统之前拦截异常用户，譬如不能因为在交易系统之后拦截而影响下单成功率。阿里聚安全认为健壮有效的营销系统必须能在短时间内接入黄牛和活动防控，支撑几百个营销活动和商品的黄牛防控。能在几十亿次攻击、几十万QPS、几毫秒内响应的苛刻条件下，通过基于用户身份特质、行为特质、设备环境信息、历史信用等信息，建立用户风险画像来实时识别。通过实时预警分析、模型定时自动更新等技术手段，不断升级防御手段，以应对不断变异的攻击方法。

Part / 35

创造纵深的有适应力的数字化业务系统

互联网+或者企业在面对互联网业务发展过程中的安全威胁时，实施数字化业务系统适应力所需的实践，对传统公司具有极大的挑战，在面对各种业务部门参与、协作的过程中，需要区分业务风险优先级，关注纵深防御节点，做出平衡业务的取舍，才能使业务安全部门更敏捷，更具有弹性。阿里聚安全帮助企业评估业务安全资产与风险优先级，使用纵深防御保护关键价值链上重要节点的安全，在实践中为业务提供针对性的保护。

阿里聚安全作为提供互联网业务解决方案的领先者，能力涉及移动安全、内容安全、数据风控、实人认证等多个纬度。其中内容安全包括智能鉴黄、文本过滤、图文识别等，移动安全包括漏洞扫描、应用加固、安全组件、仿冒监测等，数据风控包括安全验证、风险识别等，实人认证包括身份造假和冒用的识别。

目前阿里聚安全已经有超过8亿多终端，使互联网企业享受到淘宝、天猫、支付宝的“同款”安全防护技术，保护互联网企业的业务安全。

参考文献

[1]Alon Menczer and Alexander Lysunets,Check Point Research Team ,DressCode Android Malware Discovered on Google Play [DB/OL].http://blog.checkpoint.com/2016/08/31/dresscode-android-malware-discovered-on-google-play/,2016/08/31

[2]Echo Duan (Mobile Threat Response Engineer),DressCode and its Potential Impact for Enterprises[DB/OL]. http://blog.trendmicro.com/trendlabs-security-intelligence/dresscode-potential-impact-enterprises/,2016/09/29

[3]Veo Zhang (Mobile Threats Analyst),“GODLESS” Mobile Malware Uses Multiple Exploits to Root Devices[DB/OL].http://blog.trendmicro.com/trendlabs-security-intelligence/godless-mobile-malware-uses-multiple-exploits-root-devices/,2016/06/21

[4] Adam Donenfeld, Check Point Mobile Research Team，Check Point Research Team ,QuadRooter: New Android Vulnerabilities in Over 900 Million Devices [DB/OL]. http://blog.checkpoint.com/2016/08/07/quadrooter/. 2016/08/07

[5]Catalin Cimpanu,QuadRooter Android Security Bugs Affect over 900 Million Devices[DB/OL]. http://news.softpedia.com/news/quadrooter-android-security-bugs-affect-over-900-million-devices-507052.shtml.2016/08/7

Credit

Special Thanks To:

木懿、蒸米、笙华、释涯、逆巴、舟海、呆狐、阿刻、浣羽、意尘等对年报的大力支持

Graphic Designer:

连羽

Editor:

迅迪、凝琼

阿里聚安全
ALIBABA JAQ SECURITY

About

阿里聚安全是阿里巴巴集团整合自身安全能力对外输出的安全开放平台，依托国际领先的风险扫描引擎、立体式安全防护技术、庞大的数据库体系和计算能力，为企业级应用和移动应用开发者提供多维度的全周期安全解决方案，集成方式简单快捷，帮助企业与开发者快速定位并解决互联网应用中存在的风险，与行业共享阿里巴巴集团十几年来在互联网安全领域实战的积累。

Website jaq.alibaba.com

E-mail mobilesecurity@service.alibaba.com

Weibo 阿里聚安全