广东省移动智能终端应用软件(APP)
2020安全白皮书

广东省通信管理局

二〇二一年三月

版权声明

编 委 会

主　编

苏少林

副主编

张红霞

编写人员（排名不分先后）

梁建翔　　罗志强　　洪经章　　杨邦意

古　元　　阮伟军　　曾卓文　　杨　伦

詹斯伟　　王艳玲　　陈　煦

前　言

随着智能手机的普及，人们在沟通、社交、娱乐等活动中越来越依赖于移动智能终端应用软件（以下简称APP），手机上五花八门的APP涵盖了消费者衣食住行的各个方面。截至2020年12月底，广东省通信管理局APP监管平台（以下简称APP监管平台）收录全国APP应用共计597万个版本，242.12万款，其中有78.12万余款APP可以根据明确的开发运营主体进行归属地划分。从区域来看，归属广东省开发运营的APP数量为19.61万款，占据全国第一位，占全国已知归属地APP总量的25.1%，广东省移动互联网用户达到1.4亿户，广东省已成为名副其实的APP开发运营大省和APP用户大省。

APP产业快速发展的同时也伴生着侵犯隐私、恶意行为、安全隐患和不良内容等安全风险。为切实加强APP用户个人信息保护，在工业和信息化部的领导下，2020年广东省通信管理局持续深入开展APP专项治理工作，坚持以“技管结合，以网管网”的思路治理APP生态环境，自主建设了APP监管平台。APP监管平台具备摸清底数、快速研判、证据留存、精准执法等功能，极大地提升了政府APP监管治理能力，对督促行业相关企业落实主体责任发挥了重要作用，广东在国

内率先构建了技管结合、政企联动、多方共治的 APP 安全监管体系。

2020 年，APP 监管平台共发现 18619 个疑似存在恶意行为的 APP，监测到 75025 个疑似存在安全漏洞的 APP 和 11835 个疑似存在隐私违规问题的 APP。在 APP 监管平台的支撑下，经过人工复核，广东省通信管理局累计对 412 款 APP 发出违法违规 APP 处置通知，根据相关部门认定意见关停违法有害 APP 328 款，下架问题 APP 35 款，对问题突出的 APP 运营者做出 27 起行政处罚，并将违规企业纳入电信业务经营不良名单，有力保护了 APP 用户的合法权益。

本白皮书基于广东省通信管理局 APP 监管平台 2020 年监测数据编写，展示了广东省内 APP 的发展状况和安全态势，为社会各界研究 APP 个人信息保护提供了宏观、权威的数据参考；所披露的 APP 侵害用户权益十大案例问题典型，对 APP 运营者具有积极的警示教育意义。APP 安全治理是护航行业健康发展，维护用户合法权益的基础保障工作。广东省通信管理局将在工业和信息化部的领导下，坚持“以人民为中心”的发展思想和“技管结合，以网管网”的治理思路，加强行业自律，推动社会共治，指导组建 APP 安全生态联盟，构建 APP 监管治理新格局，持续深入推进违法违规 APP 乱象治理专项工作。

目 录

1.综述.....1
1.1.全国 APP 概况.....1
1.2.归属广东省开发运营的 APP 数量位居全国第一.....2
1.3.APP 产业快速发展伴生着各类安全风险.....3
2.APP 监管平台运行及安全监测情况.....5
2.1.APP 监管平台运行概述.....5
2.2.隐私合规监测情况.....7
2.2.1.存在隐私违规问题的 APP 月度数量小幅性波动.....7
2.2.2.“休闲娱乐”类 APP 的隐私违规问题较为突出.....7
2.2.3.存在隐私违规问题的 APP 主要分布在深圳和广州.....8
2.2.4.私自收集个人信息和注销账号难两类排名在隐私违规问题前两位.....9
2.3.恶意 APP 监测情况.....9
2.3.1.恶意 APP 月度感染事件数量整体呈现周期性波动趋势..9
2.3.2.恶意 APP 行为特征以流氓行为类最为突出.....10
2.3.3.恶意 APP 传播源数量呈现快速下降趋势.....11
2.4.安全漏洞监测情况.....12
2.4.1.存在安全漏洞的 APP 月度数量在六千上下波动.....12
2.4.2.“休闲娱乐”类 APP 存在安全漏洞的问题较为突出....13
2.4.3.疑似存在安全漏洞的 APP 主要分布在深圳和广州.....14

2.4.4.APP 安全漏洞以加固壳识别类型为主.....14
2.5.被责令整改问题 APP 的主要情况.....15
2.5.1.问题 APP 的类型分布.....15
2.5.2.被责令整改 APP 的主要问题.....15
3.广东 APP 监管总体情况与典型案例.....17
3.1.APP 监管执法总体情况.....17
3.2.APP 侵害用户权益的十大典型案例.....19
3.2.1.某生活购物类 APP 侵害用户知情权和违反必要原则过度索取高敏感权限被行政处罚.....19
3.2.2.某电商导购类 APP 侵害用户知情权和选择决定权默认开启多项权限被行政处罚并纳入不良名单.....21
3.2.3.某停车服务类 APP 因设置不合理账号注销障碍、提前索权等问题被行政处罚.....23
3.2.4.某购物服务类 APP 无故强迫用户授予非必要权限被责令整改.....25
3.2.5.某驾考服务类 APP 未经用户同意收集使用个人信息（Android ID、MAC 地址等）被警告及罚款.....27
3.2.6.某地图导航类 APP 未公示列明所集成第三方 SDK 及其收集使用个人信息规则被警告及罚款.....28
3.2.7.某证券交易类 APP 存在“界面劫持”高危安全漏洞被责令整改.....30
3.2.8.某购物类 APP 存在“webview 远程代码执行”高危安全

漏洞被责令整改.....31
3.2.9.某游戏类 APP 存在“Janus 签名机制漏洞”高危安全漏洞被责令整改.....32
3.2.10.某金融类 APP 存在流氓行为、信息窃取等恶意行为被下架封堵.....33
4.构建 APP 监管治理新格局.....35
4.1.加强行政执法，加大监督惩处力度.....35
4.2.加强技管结合，持续提升 APP 技术监测能力.....36
4.3.指导组建安全生态联盟，构建 APP 绿色生态圈.....36
4.4.倡议签署个人信息保护自律公约，促进行业自律.....37
4.5.压实 APP 相关企业主体责任，维护用户合法权益.....38
4.5.1.压实 APP 分发平台主体责任.....38
4.5.1.1.落实 APP 上架实名登记.....38
4.5.1.2.落实上架 APP 软件包和相关信息日志留存.....38
4.5.1.3.加强 APP 安全上架审核及跟踪管理.....39
4.5.1.4.规范 APP 上架基本信息公示.....39
4.5.1.5.加强对 APP 提供者的监管政策宣贯.....39
4.5.1.6.公开投诉举报方式并受理公众举报.....40
4.5.1.7.履行 ICP 备案或取得相应电信业务许可.....40
4.5.2.压实 APP 运营者主体责任.....40
4.5.2.1.健全 APP 安全合规管理制度和工作机制.....40
4.5.2.2.重视保障用户的知情权、选择决定权.....40

4.5.2.3.严格遵循合法、正当、必要的原则.....41
4.5.2.4.加强对所使用第三方插件、程序代码的安全审核，并做好第三方收集使用个人信息规则的公示.....41
4.5.2.5.保障所收集使用的数据和个人信息的安全.....41
4.5.2.6.不得恶意干扰用户终端环境和干扰用户使用 APP.....42
4.5.2.7.及时响应处理个人信息删除、更正诉求.....42
4.5.2.8.配合 APP 分发平台提供真实身份信息、联系方式、上架审查材料和公示信息.....43
4.5.2.9.履行互联网信息服务备案（ICP 备案）手续，涉及电信业务的应取得相应电信业务许可.....43
4.5.3. 压实第三方 SDK 提供者主体责任.....43
4.6.提升用户风险防范意识，养成安全使用习惯.....44
4.6.1.从 APP 运营者官网或正规应用商店下载 APP，不点击来源不明的链接下载安装软件.....44
4.6.2.遵循最小授权原则管理 APP 权限.....45
4.6.3.谨慎使用公共 WIFI，避免通过不安全充电设备进行充电.....45
4.6.4.注意日常生活中的隐私保护.....45
4.6.5.不要随意破解手机、开启 root 权限，以及刷装不明来源的第三方操作系统和桌面应用.....46
4.6.6.遇到 APP 违法违规行为可向有关机构举报，涉及网络违法犯罪的应及时报案.....46

5. 结束语.....48

附录一：广东省通信管理局 APP 专项治理工作公开发布的报道....49

报道一：广东省通信管理局严查违规 APP 应用商店 为电信用户合法权益保驾护航 发布时间：2019 年 3 月 14 日.....49

报道二：多款 APP 收集个人敏感信息 广东省通信管理局依法查处涉事企业 发布时间：2019 年 4 月 24 日.....51

报道三：广东省通信管理局关于转发工信部开展 APP 侵害用户权益专项整治工作的通知 发布时间：2019 年 11 月 8 日.....54

报道四：广东省通信管理局聚焦用户个人信息保护 纵深推进 APP 依法监管 发布时间：2020 年 1 月 21 日.....56

报道五：广东省通信管理局查处一批违反用户个人信息保护规定 APP 发布时间：2020 年 3 月 15 日.....59

报道六：广东省通信管理局不断加大执法力度 狠抓 APP 数据安全和隐私合规 发布时间：2020 年 9 月 15 日.....63

报道七：广东省通信管理局 APP 监管情况通报（2020 年 10 月）发布时间：2020 年 11 月 23 日.....67

报道八：209 款 APP 被广东省通信管理局责令整改或关停（2020 年 11-12 月） 发布时间：2021 年 1 月 11 日.....70

报道九：215 款 APP 被广东省通信管理局责令限期整改（2021 年 1 月）发布时间：2021 年 2 月 23 日.....73

附录二：APP 监管部分重要依据.....77

依据一：《中华人民共和国网络安全法》（摘录）.....77

依据二：《中华人民共和国民法典》（摘录）.....81
依据三：《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）.....85
依据四：《公共互联网网络安全威胁监测与处置办法》（工信部网安〔2017〕202 号）.....94
依据五：《APP 违法违规收集使用个人信息行为认定方法》（国信办秘字〔2019〕191 号）.....99
依据六：工业和信息化部关于开展 APP 侵害用户权益专项整治工作的通知（工信部信管函〔2019〕337 号）.....104
依据七：工业和信息化部关于开展纵深推进 APP 侵害用 户权益专项整治行动的通知（工信部信管函〔2020〕164 号）..... 109
依据八：《 YD/T 2439-2012 移动互联网恶意程序描述格式》
.....115

1. 综述

1.1. 全国 APP 概况

根据 APP 监管平台收录数据，截至 2020 年底，全国第三方应用商店 APP 数量为 597 万个版本，242.12 万款。其中，2020 年 12 月新增上架 APP 数量 7.76 万款，比 11 月减少 2.26 万款，新增上架量环比下降 22.66%。

在所有 APP 类型分类中，休闲娱乐类 APP 数量继续保持领先，达 66.38 万款，占全部 APP 比重为 29.65%。生活服务类和新闻资讯类 APP 数量分别达 45.51 万和 21.85 万款，分列第二、三位，旅行交通类 APP 数量超过教育文化类，达到 20.68 万款，上升为第四位。上述占据前 4 位种类的 APP 数量占比达 68.98%，其他教育文化、社交交友、购物导购、体育健身、移动金融、医疗健康、政务和工业互联网等 8 类 APP 占比为 31.02%。

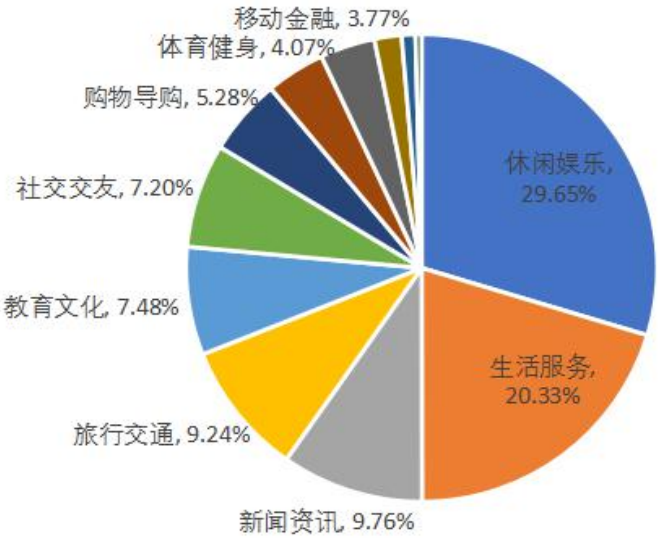


图 1-1 休闲娱乐类和生活服务类 APP 数量占比达到 50%

在应用分发量方面，休闲娱乐类 APP 应用分发量居首位。根据 APP 监管平台数据，截至 2020 年底，我国第三方应用商店在架 APP 分发总量达到 587767 亿次。其中，休闲娱乐 APP 下载量达 155759 亿次，排第一位，环比增长 6%；社交交友类 APP 下载量达 95627 亿次，排第二位；生活服务类、新闻资讯类、购物导购类、旅行交通类、移动金融类 APP 分别以 82528 亿次、74677 亿次、44292 亿次、43148 亿次、34313 亿次分列第三至七位，在其余各类 APP 应用中，下载总量超过万亿次的 APP 应用还有教育金融类和体育健身类 APP，下载量分别为 28390 亿次和 17447 亿次。

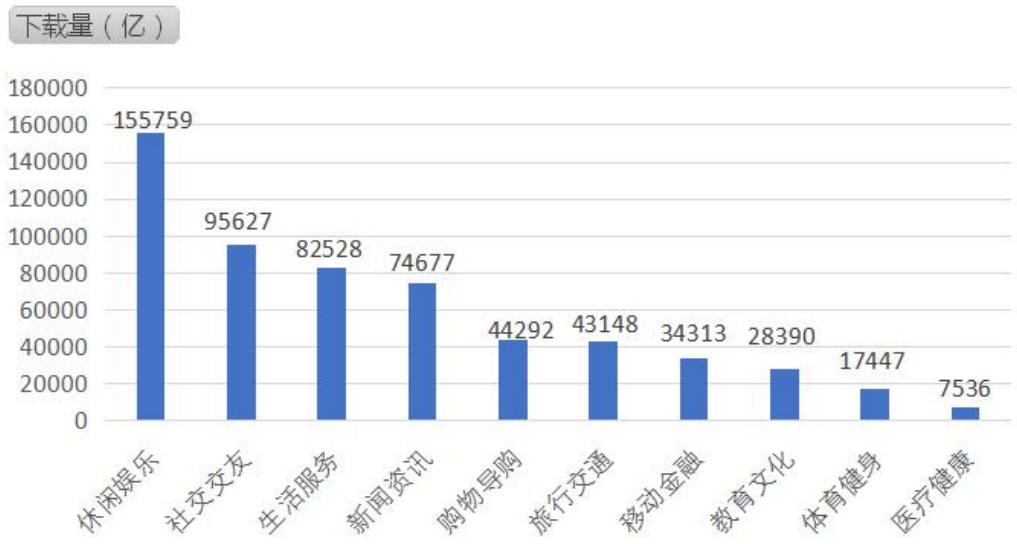


图 1-2 休闲娱乐类 APP 稳居应用分发量首位

1.2. 归属广东省开发运营的 APP 数量位居全国第一

APP 监管平台收录全国 APP 应用共计 597 万个版本，242.12 万款，其中有 78.12 万余款 APP 可以根据明确的开发运营主体进行归属地划分，剩余 APP 属于个人开发运营主体，

不能划分明确的归属地。

从区域来看，归属广东省开发运营的 APP 数量为 19.61 万款，占据全国第一位，占全国已知归属地 APP 总量的 25.1%，其次是归属北京市开发运营的 APP 数量为 17.58 万款，占全国已知归属地 APP 总量的 22.5%；归属上海市开发运营的 APP 数量为 8.36 万款，位列第三，占全国已知归属地 APP 总量的 10.7%。浙江、福建、江苏、四川、山东、湖北、安徽分别以 8.92%、6.12%、5.72%、3.91%、3.1%、2.1%、1.7% 的份额排名第四至第十位。

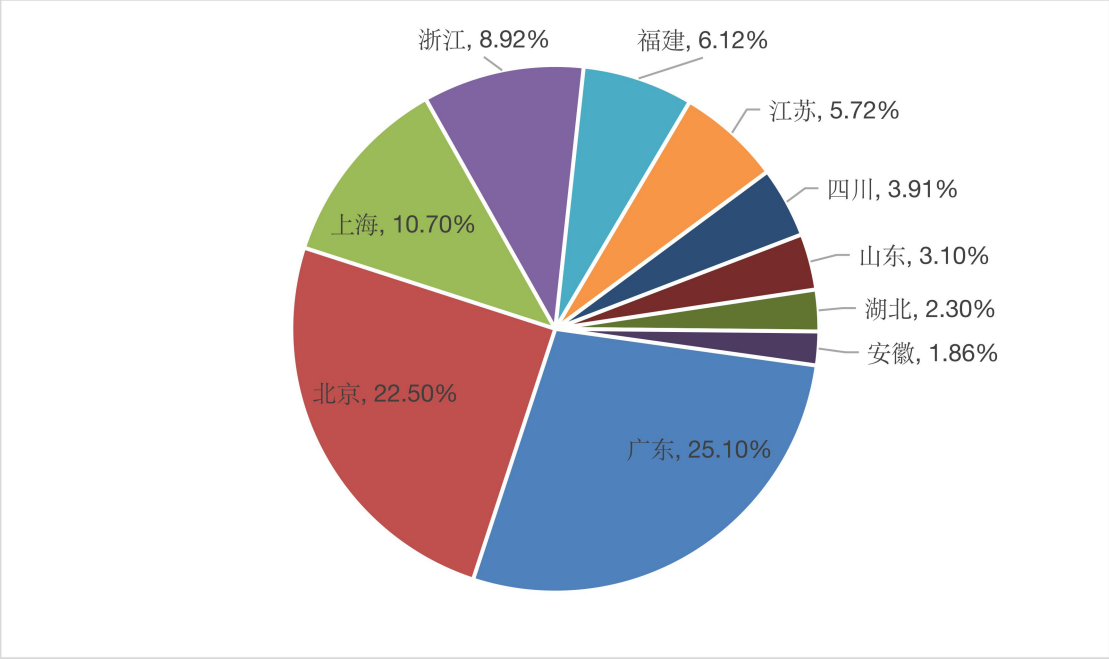


图 1-3 归属广东省开发运营的 APP 数量位居全国第一

1.3. APP 产业快速发展伴生着各类安全风险

APP 产业快速发展的同时也伴生着侵犯隐私、恶意行为、安全隐患和不良内容等安全风险。具体来说表现为以下四类

安全风险：

（1）侵犯隐私：APP 使用过程中，常常出现肆意收集使用用户个人信息的行为，如未经用户同意，APP 及嵌入的第三方 SDK 收集个人 MAC 地址、IMEI 码、电话号码等信息，以及 APP 强制、频繁、过度索取权限等。

（2）恶意行为：恶意开发者可在 APP 中植入插件，窃取用户手机号码、地理位置、短信、密码等信息，导致用户财产损失；也可在 APP 运行过程中调用相关权限，模拟用户发起支付，并拦截平台的支付通知短信，导致用户被不知情扣费，进而直接获利。

（3）安全隐患：安全隐患包括加固壳识别、Java 代码反编译风险、Webview File 同源策略绕过漏洞、界面劫持风险等，这些安全隐患可能导致存储在原手机上的数据被读取，用户的账号、密码、银行卡等敏感信息泄露；以及对用户输入做各种监听、拦截、欺诈，引导用户输入密码，转账，导致用户财产损失。

（4）不良内容：APP 在运营过程中可能存在色情、诈骗、赌博、侵权和暴恐等违法违规内容。

2. APP 监管平台运行及安全监测情况

2.1. APP 监管平台运行概述

APP 已成为互联网服务的主角与用户最依赖的入口，在为网民提供丰富的网络服务的同时，恶意扣费、隐私窃取、数据泄漏等各种乱象和安全问题丛生，不仅使用户的个人信息安全受到威胁，同时也给国家信息安全带来了重大安全隐患。数量庞大、种类繁杂的 APP，参差不齐、分散在各地的应用商店，加上 APP 的程序代码与网络结构比较复杂，存在“全网监测难、溯源定位难、闭环处置难”三大监管痛点。为解决这些痛点，自 2019 年下半年以来，广东省通信管理局本着“技管结合，以网管网”的思路，着手建设 APP 监管平台。平台实现了四大核心能力：

（1）摸清底数，建立行业基础数据库

APP 监管平台通过多源汇聚数据建设 APP 库、开发者库、应用市场库三库合一的 APP 行业基础数据库，可以对每款 APP 的应用类型、历史版本、运营主体、所属地域、分布应用商店、下载总量等一目了然。汇聚了 60 多万 APP 运营者、597 万个 APP 版本和 278 家 APP 应用商店数据。

（2）主动监测，发现问题依法定性

APP 监管平台可圈定重点监管目标，支持“恶意程序”“安全漏洞”“侵犯用户隐私权益”三个角度进行轮巡检测和取证。平台可主动对入库 APP 进行多引擎分析检测，支持静态源码

分析和动态行为监测，包括 41 种静态特征 129 种动态特征，并对发现的问题依法定性。截至 2020 年底，平台累计发现全国范围内疑似恶意 APP 4 万多个,疑似侵权 APP 8 万多个，疑似漏洞 APP 33 万多个。

（3）精准溯源，关键证据及时留存

APP 监管平台通过动态引擎模拟人工 APP 运行,捕获后台传输数据、请求数据、返回数据，支撑引擎分析是否存在侵犯隐私行为、恶意行为，如未经授权唤醒第三方应用、索取与当前服务场景无关的权限、私自收集个人信息等，留存违规版本的安装程序并对违法违规行为进行截图留存。结合 APP 行业基础数据库，可以对 APP 传播、接入和运营服务情况进行精准定位溯源，同时支持历史版本的回溯。

（4）快速处置，多管齐下依法整治

通过政企联动,多管齐下对违法违规 APP 进行快速处置。APP 监管平台可以联动基础电信企业，实现一键关停；可联动应用商店，实现快速下架。

广东省通信管理局基于 APP 监管平台实现了“数据采集-主动检测-发现问题-溯源取证-快速处置-整改反馈-复测-恢复运营”闭环监管流程管理，可通过下架处置、断开接入、行政处罚以及纳入电信业务经营不良名单或失信名单并公开曝光等措施及时处置违法违规 APP,大大提升了对 APP 的监管能力与处置效率，在国内率先构建了政府、企业、用户多

方治理的 APP 安全监管体系。

2.2. 隐私合规监测情况

2.2.1. 存在隐私违规问题的 APP 月度数量小幅性波动

APP 监管平台共发现 11835 个疑似存在隐私违规问题的 APP。违规 APP 月度数量在 938 和 1021 之间小幅波动，其中 9 月份为全年最高，共有 1021 个 APP 疑似存在隐私违规行为，2 月疑似存在隐私违规行为的 APP 938 个，为全年最低。

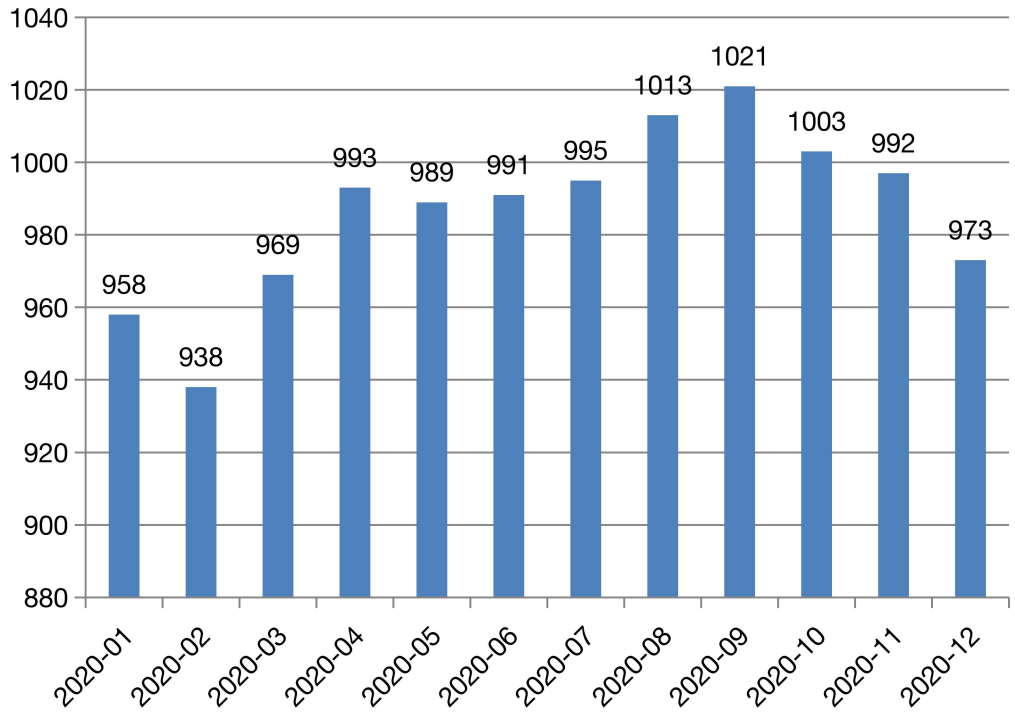


图 2-1 疑似存在隐私违规问题的 APP 月度数量

2.2.2. “休闲娱乐”类 APP 的隐私违规问题较为突出

疑似存在隐私违规问题的 APP 主要有休闲娱乐、生活服务、社交交友、购物导购、旅行交通、教育文化等应用类型。排名前三的为休闲娱乐、生活服务、社交交友类，数量分别

为 3730、2568 和 2538 个。

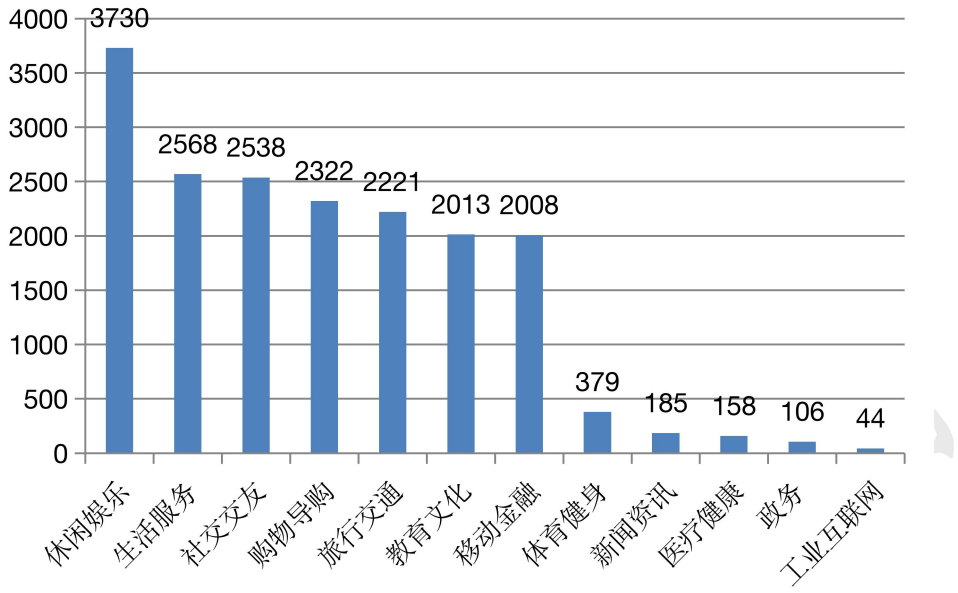


图 2-2 “休闲娱乐”类 APP 的隐私违规问题数量

2.2.3. 存在隐私违规问题的 APP 主要分布在深圳和广州

从归属地看，疑似存在隐私违规问题的 APP 主要分布在深圳、广州和珠海市，分别为 4176、3299、1188 个。

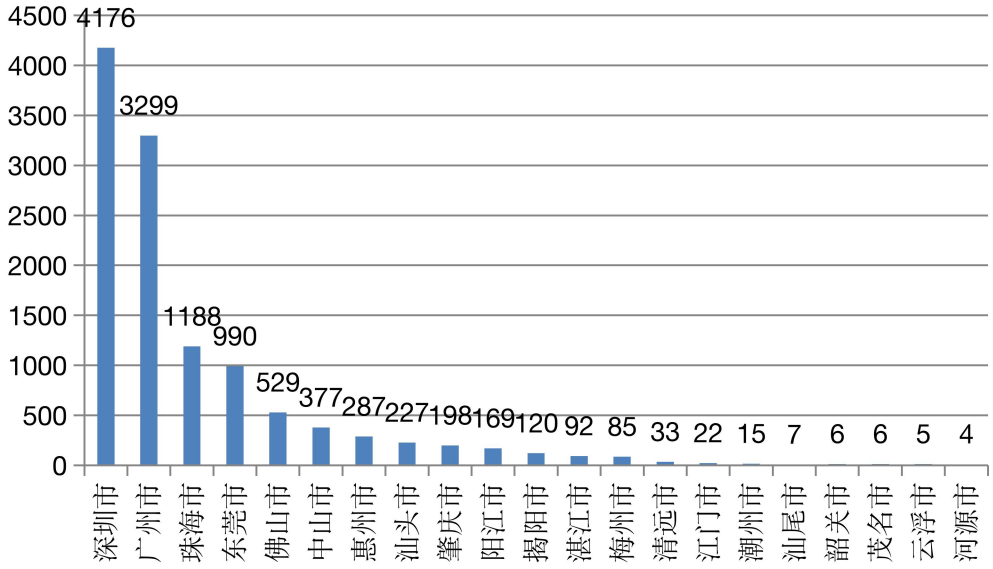


图 2-3疑似存在隐私违规问题的 APP 地区归属分布

2.2.4.私自收集个人信息和注销账号难两类排名在隐私违规问题前两位

隐私违规问题主要体现在私自收集个人信息、注销账号难、私自共享第三方、强制用户使用定向推送功能、超范围搜集个人信息等方面。其中私自收集个人信息、注销账号难、私自共享第三方等三类问题占比较高，分别为 4581、4318 和 4145 个。

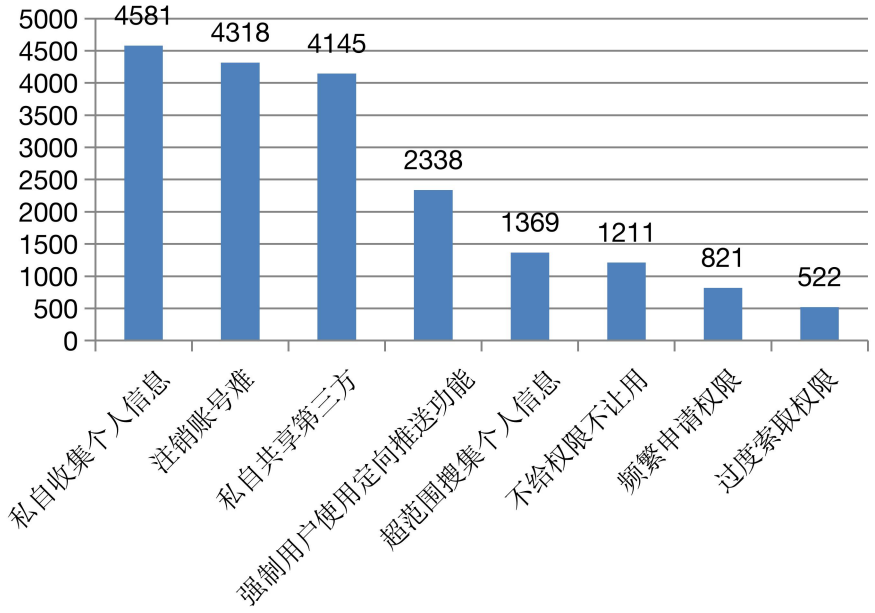


图 2-4　隐私违规主要体现在私自收集个人信息等问题

2.3. 恶意 APP 监测情况

2.3.1.恶意 APP 月度感染事件数量整体呈现周期性波动趋势

根据广东三家基础电信运营企业的移动互联网恶意程序监测和处置系统数据统计，2020 年广东地区恶意 APP 感染事件总量为 1273.64 万次，与去年相比有小幅上升。恶意 APP 感染事件数量最多的月份分别是 4-5 月、7-8 月、11-12

月，呈周期性波动趋势。其中 2 月为最低值（317772 个），5 月最高值（1614755 个）。

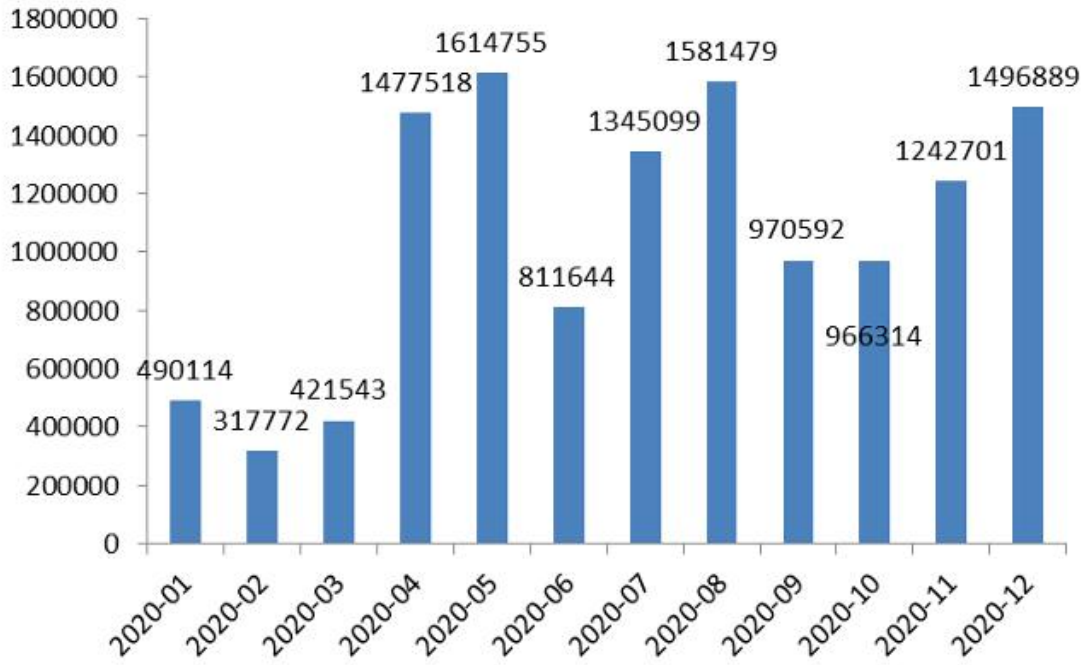


图 2-5 恶意 APP 月度感染事件数量

2.3.2.恶意 APP 行为特征以流氓行为类最为突出

依据《移动互联网恶意程序描述格式》的八类分类标准，对 18619 个 APP 相关恶意行为统计数据显示，排名前三的分别为流氓行为类、诱导欺诈类和资费消耗类。

APP 各类恶意行为的分类统计数据为：流氓行为 13272 个（占总数的 71.28%）、诱导欺诈 2466 个（占总数的 13.24%）、资费消耗 1744 个（占总数的 9.37%）、信息窃取 430 个（占总数的 2.31%）、系统破坏 420 个（占总数的 2.26%）、恶意传播 177 个（占总数的 0.95%）、恶意扣费 99 个（占总数

的 0.53%）、远程控制 11 个（占总数的 0.06%）。

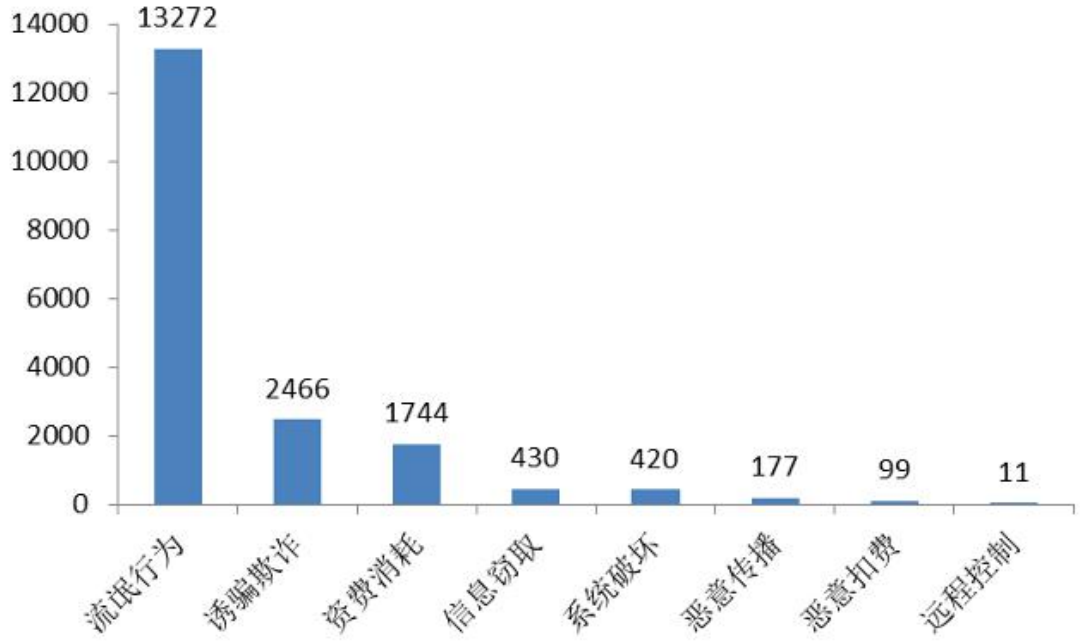


图 2-6 恶意 APP 行为特征分类统计

2.3.3.恶意 APP 传播源数量呈现快速下降趋势

广东三家基础电信运营企业对这些存在恶意行为的 APP 采取了处置控制端、处置恶意传播源和处置感染用户等处置措施，2020 年共处置控制端（IP 和 URL）92702 个，处置恶意传播源（IP 和 URL）640706 个，处置感染用户 504883 个。

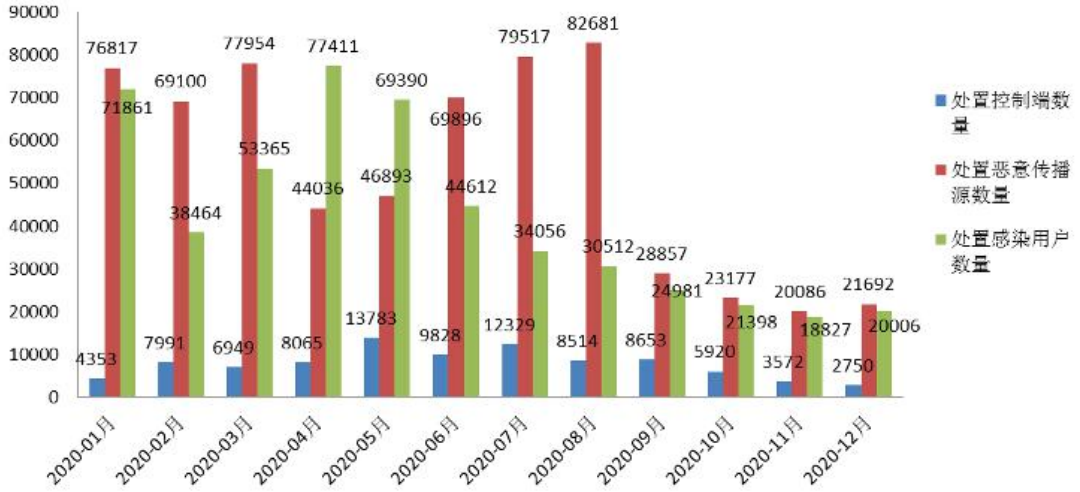


图 2-7 2020 年移动互联网恶意 APP 事件处置情况

2.4. 安全漏洞监测情况

2.4.1. 存在安全漏洞的 APP 月度数量在六千上下波动

APP 监管平台共发现疑似存在安全漏洞风险 APP 为 75025 个。疑似存在安全漏洞风险的 APP 每月数量在 6000 上下波动。其中 6 月份发现的疑似存在安全漏洞风险的 APP 数量为全年最高，达到 7113 个，2 月疑似存在安全漏洞的 APP 为 4432 个，为全年最低。

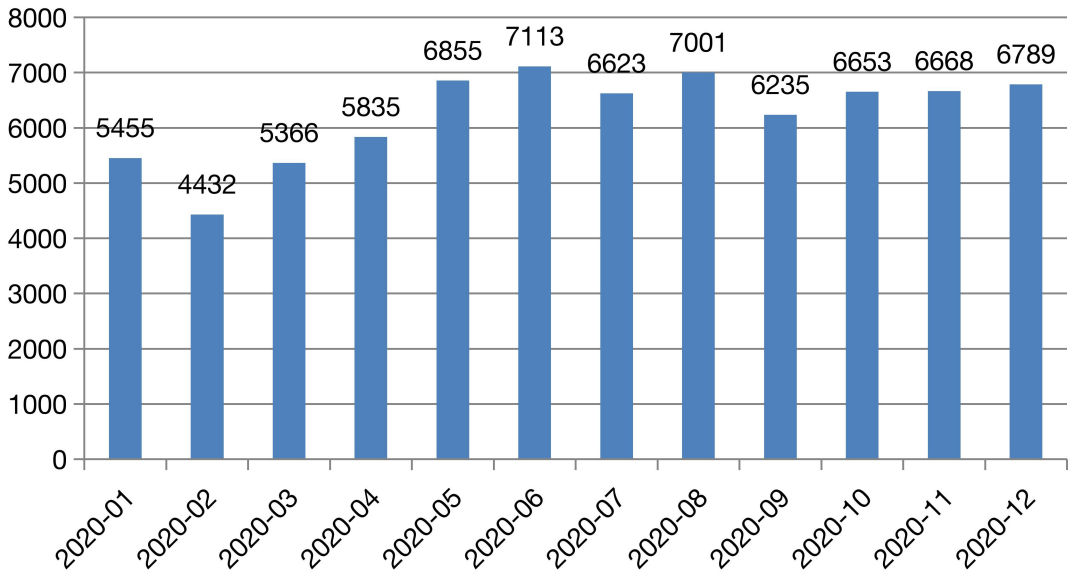


图 2-8 疑似存在安全漏洞的 APP 月度数量

2.4.2. “休闲娱乐”类 APP 存在安全漏洞的问题较为突出

疑似存在安全漏洞的 APP 主要有休闲娱乐、生活服务、社交交友、购物导购、旅行交通等应用类型，其中休闲娱乐、生活服务和社交交友类的安全漏洞数量排名前三，分别为 21150、15868、12633 个。

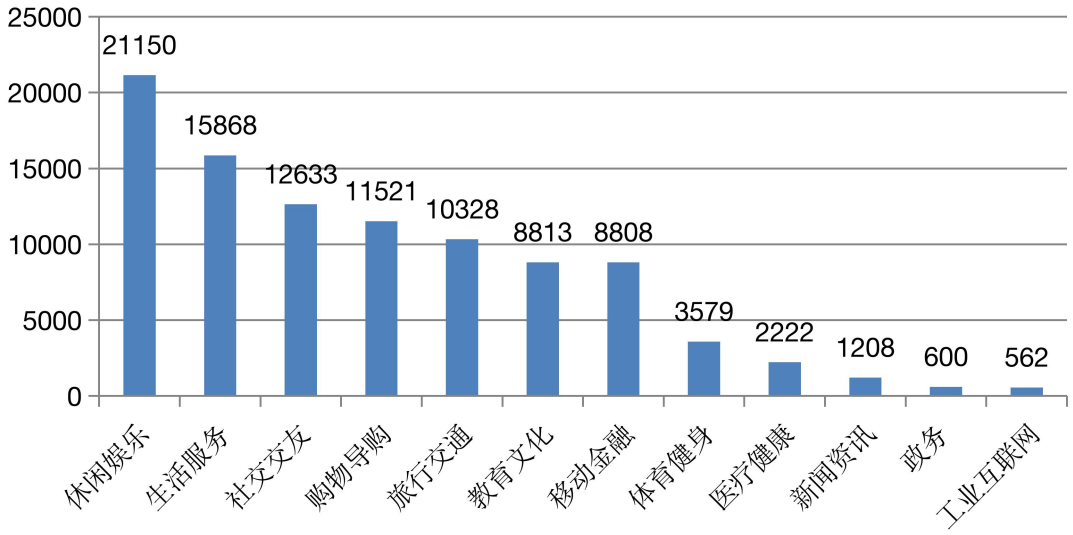


图 2-9 疑似存在安全漏洞的 APP 分类统计

2.4.3. 疑似存在安全漏洞的 APP 主要分布在深圳和广州

从归属地看，疑似存在安全漏洞的 APP 主要分布在深圳、广州、珠海，数量分别为 26239 个和 23285、9991 个。

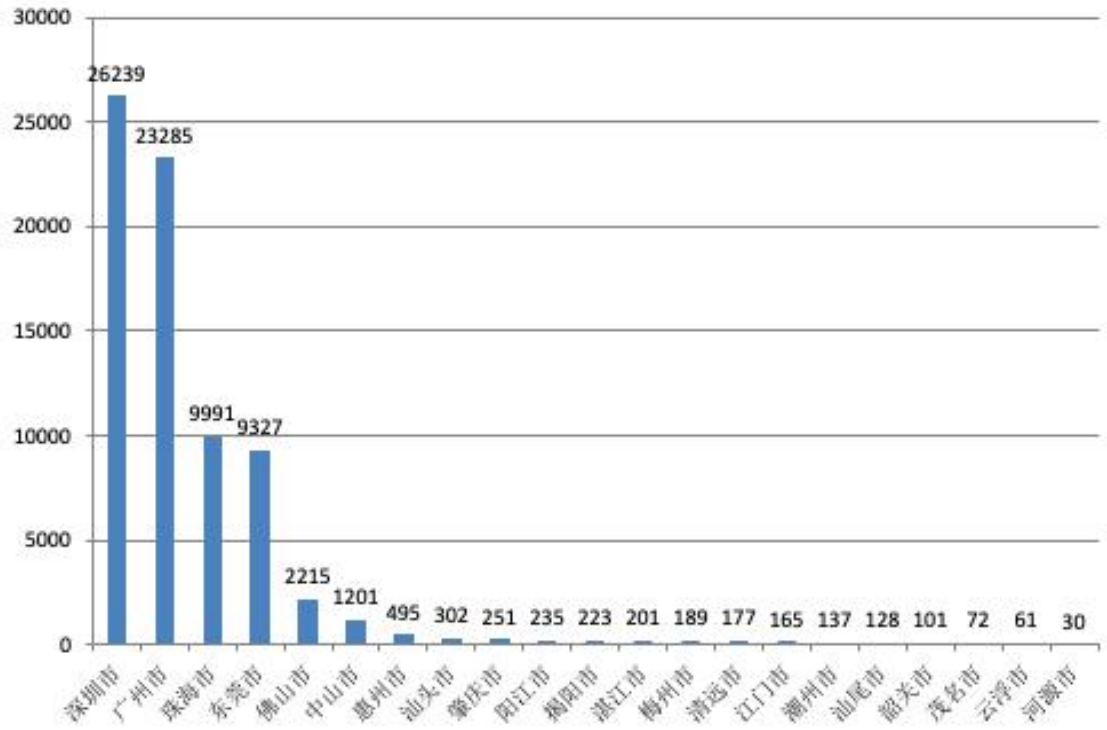


图 2-10 疑似存在安全漏洞的 APP 地域分布

2.4.4. APP 安全漏洞以加固壳识别类型为主

对相关安全漏洞问题统计数据显示，排名前三的的安全漏洞为加固壳识别、java 代码反编译风险和 Webview File 同源策略绕过漏洞，数量分别为 35266、23299 和 11823 个，这些漏洞可被非法利用，导致远程代码执行、窃取密钥和敏感信息等危害。

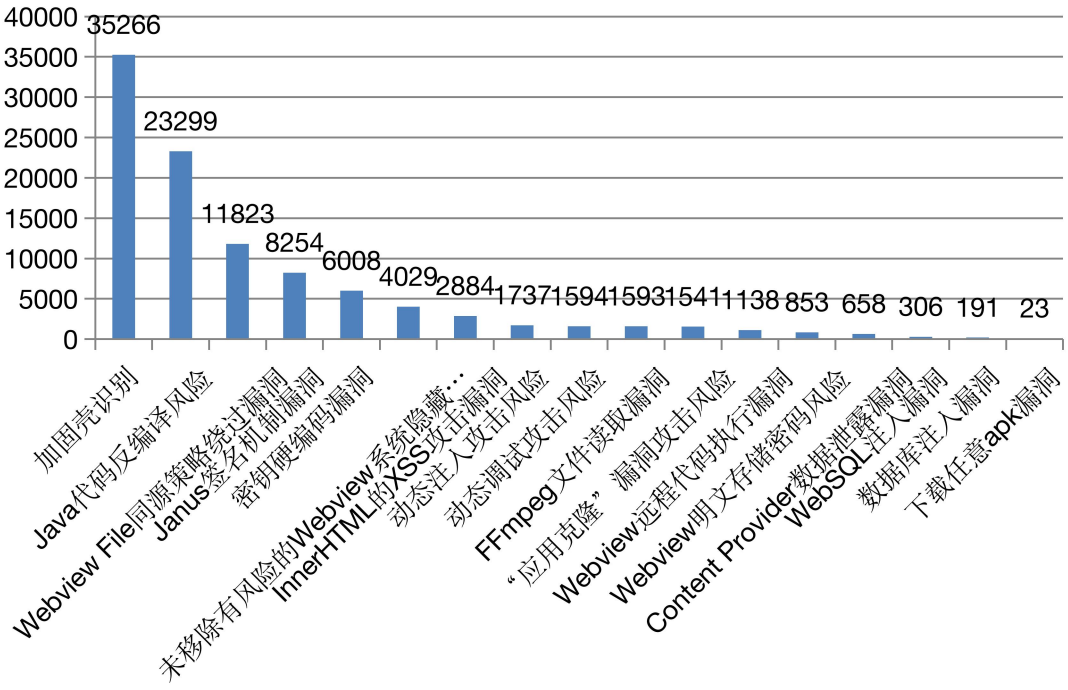


图 2-11 APP 安全漏洞分类统计

2.5. 被责令整改问题 APP 的主要情况

2.5.1. 问题 APP 的类型分布

被责令整改的 412 款侵害用户权益和安全漏洞隐患问题 APP 中，包括了金融类 56 款、工具类 49 款、游戏类 48 款、生活服务类 42 款、购物类 41 款、聊天社交类 38 款、音乐视频类 30 款、教育类 29 款、新闻阅读类 20 款、医疗健康类 18 款、旅行交通类 17 款、拍照摄影类 13 款、办公类 11 款。

2.5.2. 被责令整改 APP 的主要问题

被责令整改 APP 的问题有两类，一是违反用户个人信息保护规定（隐私违规）问题，二是网络数据安全隐患问题。

其中违反 APP 隐私规定的典型表现有：一是未在隐私政

策等公示文本中逐一列明 APP 所集成第三方 SDK 收集使用个人信息的目的、方式和范围，二是 APP 未通过弹窗告知隐私政策等方式公开收集使用个人信息的规则并征得用户同意前就开始收集个人信息或索取终端相关权限，三是 APP 在用户未使用相关功能或服务时，提前申请开启通讯录、定位、短信、录音、相机等权限，四是未按法律规定提供账号注销、删除、更正个人信息功能或未公布相关投诉举报方式。

网络数据安全隐患问题则主要有 Janus 签名机制漏洞、未移除有风险的 Webview 系统隐藏接口漏洞、界面劫持安全、密钥硬编码漏洞、Java 代码反编译风险等。

3. 广东 APP 监管总体情况与典型案例

3.1. APP 监管执法总体情况

2019 年以来，广东省通信管理局在工业和信息化部的领导下，深入贯彻落实习近平总书记关于国家网络安全“四个坚持”的重要指示精神，践行以人民为中心的发展思想，以实现网络空间治理体系和治理能力现代化为目标，切实开展 APP 监管工作。2020 年，按照工业和信息化部《关于做好 2020 年电信和互联网行业网络数据安全管理工作的通知》（工信厅网安函〔2020〕103 号）和《关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》（工信部信管函〔2020〕164 号）的部署和要求，不断加大监管力度，狠抓 APP 数据安全和隐私合规，主要做了“抓手段建设、抓行政执法、抓关键环节”三方面的工作。

抓手段建设方面，广东省通信管理局本着“技管结合，以网管网”的思路，着手建设 APP 监管平台，通过平台汇聚的海量 APP 数据和多维度引擎检测，解决了“全网监测难、溯源定位难、闭环处置难”三大监管痛点，有效支撑开展 APP“侵犯用户权益专项整治”“网络数据安全”“恶意程序威胁监测处置”等专项工作。

抓行政执法方面，2020 年，广东省通信管理局依据《中华人民共和国网络安全法》《电信和互联网用户个人信息保护规定》（工业和信息化部令第 24 号）、《移动智能终端

应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）、《公共互联网网络安全威胁监测与处置办法》（工信部网安〔2017〕202 号）等法律法规规定共发出《违法违规 APP 处置通知》责令整改 APP 412 款，下架拒不整改的 APP 35 款，根据相关部门认定意见关停违法有害 APP 328 款，对问题突出 APP 运营者做出行政处罚 27 起，并将处罚对象纳入电信业务经营不良名单，并加大曝光力度，累计发出公开报道 6 篇，媒体转载 20 万余次，营造了行业主管部门坚决严抓 APP 的浓厚氛围，对 APP 从业者形成较大威慑力，从而激发了更多 APP 运营者合法合规的内在驱动力，加强自律落实主体责任。

抓关键环节方面，广东省通信管理局抓好“应用商店”“第三方 SDK”等关键环节，要求相关企业做好上架审核、存量排查、督促整改、配合下架、停止服务等相关工作，履行平台责任与义务。2020 年，广东省通信管理局组织相关应用商店排查问题 APP 150 万余次，发现并下架违规 APP 12 万款，驳回违规 APP 上架申请 16 万次；组织了第三方 SDK 服务商开展违法 APP 排查，共发现违法 APP 并停止消息推送服务 627 款，督促运营者完成合规整改 APP 84 款。

3.2. APP 侵害用户权益的十大典型案例

3.2.1.某生活购物类 APP 侵害用户知情权和违反必要原则过度索取高敏感权限被行政处罚

2020 年 3 月，广东省通信管理局协助市场监督管理部门调查某生活购物类 APP 提供野猪肉和野猪捕获工具相关商品信息的案件。广东省通信管理局使用 APP 监管平台进行检查时发现该 APP 还存在违反用户个人信息保护规定的情形，具体表现为：APP 安装后首次运行，在没有使用任何功能和未告知收集个人信息规则的情况下，就向用户索取包括“通讯录”“拍摄照片和录制视频”“录制音频”“发送和查看短彩信息”等敏感权限在内的 7 项手机权限，APP 正式运行后主要界面也未见隐私政策或其他收集使用个人信息的规则，属于典型的“未公开收集使用规则”“未明示收集使用个人信息的目的、方式和范围”和“违反必要原则，收集与其提供的服务无关的个人信息”违法违规情形。根据调查情况，广东省通信管理局依据《网络安全法》和《电信和互联网用户个人信息保护规定》的相关规定，责令该 APP 运营者整改并对其做出给予警告和罚款的行政处罚。

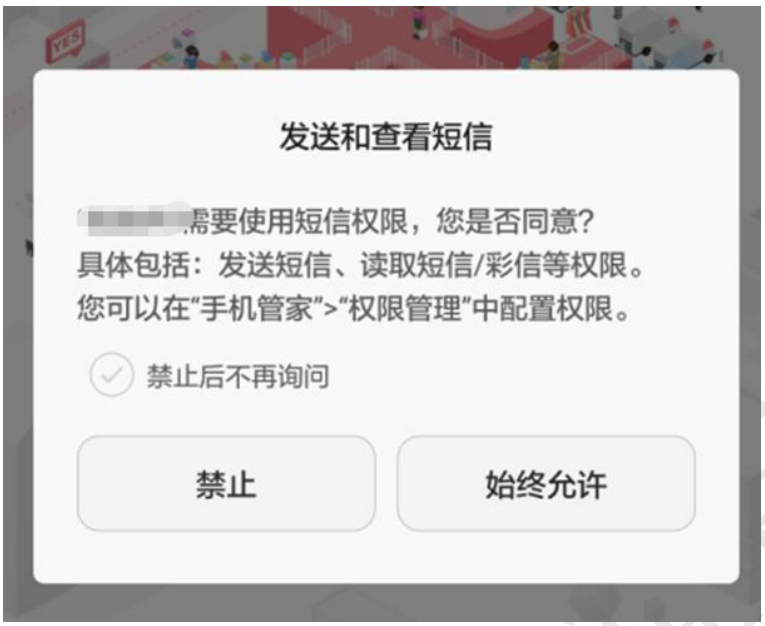


图 3-1 未明示收集规则前弹窗获取短信权限（违反必要原则收集信息）

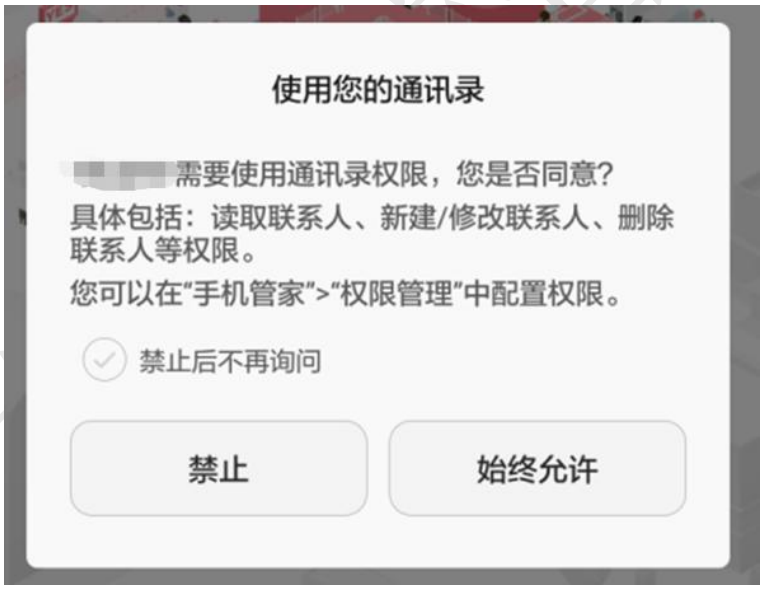


图 3-2 未明示收集规则前弹窗获取通讯录权限（违反必要原则收集信息）

3.2.2.某电商导购类 APP 侵害用户知情权和选择决定权默认开启多项权限被行政处罚并纳入不良名单

2020 年 3 月，广东省通信管理局执法人员从 APP 监管平台监测结果中发现某电商导购类 APP 疑似存在相关隐私违规问题，通过手机测试，发现问题属实，具体问题表现为：（一）APP 安装后尚未运行之前就已默认打开用户手机的“存储”、“电话”、“位置”、“相机”、“短信/彩信”权限；（二）APP 首次运行以及正式运行后的主要界面均未发现隐私政策，注册账号时虽有《网络服务条款及使用协议》，但却直接默认勾选，且该协议也未提及任何手机权限获取和收集、使用个人信息的情况。根据调查情况，广东省通信管理局依据《网络安全法》和《电信和互联网用户个人信息保护规定》的相关规定，责令该 APP 运营者整改并对其做出给予警告和罚款的行政处罚，并依据《电信业务经营许可管理办法》的相关规定，将该 APP 运营者纳入电信业务经营不良名单。

图 3-3 某电商导购类 APP 安装默认开启了“信息”“相机”等多项权限

3.2.3.某停车服务类 APP 因设置不合理账号注销障碍、提前索权等问题被行政处罚

2020 年 9 月，广东省通信管理局收到用户举报反映某停车服务类 APP 存在“账号注销难”的问题。执法人员使用 APP 监管平台和手机进行检测固证后，约谈该 APP 运营者负责人，确认该 APP 存在突出的“账号注销难”问题，具体表现为：APP 在用户注册账号时仅凭手机号码及验证码即完成注册，但注销账号时却要求用户提供手机号码的真实姓名、身份证正反面照片，甚至要求用户提供电信运营商出具的手机号码权属证明方可受理。此外，检测发现该 APP 还存在未使用相关功能就索取用户相机权限，且相机权限及 APP 集成的地图、支付、推送、统计、分享等多个 SDK 均未在隐私政策中逐一列明。根据调查情况，广东省通信管理局依据《网络安全法》和《电信和互联网用户个人信息保护规定》的相关规定，责令该 APP 运营者整改并对其做出给予警告和罚款的行政处罚。

图 3-4 某停车服务类 APP 设置不合理账号注销障碍

图 3-5 某停车服务类 APP 未使用相关功能提前索取用户相机权限

3.2.4.某购物服务类 APP 无故强迫用户授予非必要权限被责令整改

2020 年 10 月，广东省通信管理局执法人员从 APP 监管平台监测结果中发现某购物服务类 APP 疑似存在“无隐私政策”、“拒绝授予非必要权限无法使用”等问题。通过手机测试，发现问题属实，具体问题表现为： APP 首次运行，未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则，就依次索取“设备信息”“访问外部存储”“发送和查看短信”“拍摄照片和录制视频”“位置信息”五项权限，拒绝授权任意一项或多项权限，都提示“由于 APP 运行必须的权限被禁用，APP 无法正常运行，请进入 APP 时允许权限或前往权限管理修改权限！”。由于上述权限并非 APP 运行所必需，也无收集规则说明和相应场景支持，为此，广东省通信管理局依据《网络安全法》《电信和互联网用户个人信息保护规定》相关规定，责令该 APP 运营者期限整改，该 APP 运营者收到《责令通知书后》反馈已决定暂停运营该 APP 服务并全线下架。

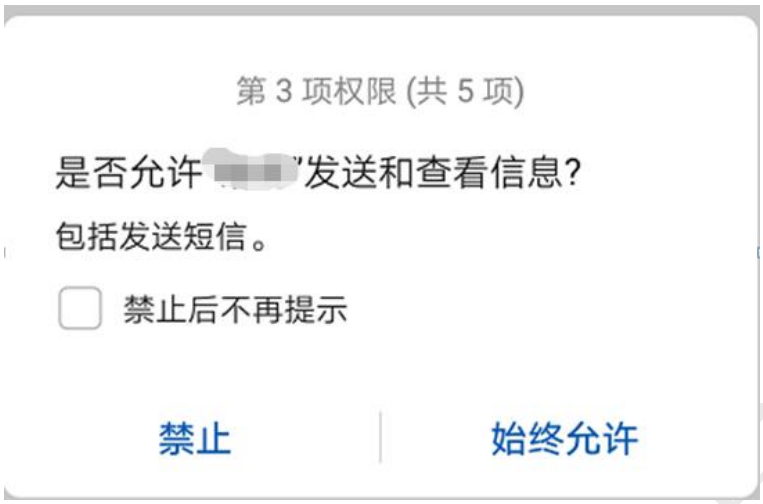


图 3-6 某购物服务类 APP 无故索取短信权限

图 3-7 某购物服务类 APP 无故索取摄像权限

图 3-8 拒绝授予任意一项或多项权限均无法使用该 APP

3.2.5.某驾考服务类 APP 未经用户同意收集使用个人信息（Android ID、MAC 地址等）被警告及罚款

2020 年 9 月，广东省通信管理局执法人员从 APP 监管平台监测结果中发现某驾考服务类 APP 疑似存在“未经用户同意收集使用个人信息”等问题。通过手机测试，发现问题属实，具体问题表现为：APP 征得用户同意前就开始收集个人信息（Android ID、MAC 地址等），以默认方式同意隐私政策。为此，广东省通信管理局依据《网络安全法》相关规定，责令该 APP 运营者逐一改正，给予警告并处相应罚款。

图 3-9 某驾考服务类 APP 征得用户同意前就开始收集个人信息

3.2.6.某地图导航类 APP 未公示列明所集成第三方 SDK 及其收集使用个人信息规则被警告及罚款

2020 年 9 月，广东省通信管理局执法人员从 APP 监管平台监测结果中发现某地图导航类 APP 疑似存在“未明示收集使用个人信息的目的、方式和范围”等问题。通过手机测试，发现问题属实，具体问题表现为：APP 申请使用相机、麦克风和通信录三项权限，超出隐私政策用户授权范围；应用内集成多个可收集用户个人信息的第三方 SDK，亦未在隐私政策中声明。为此，广东省通信管理局依据《网络安全法》相关规定，责令该 APP 运营者逐一改正，给予警告并处相应罚款。

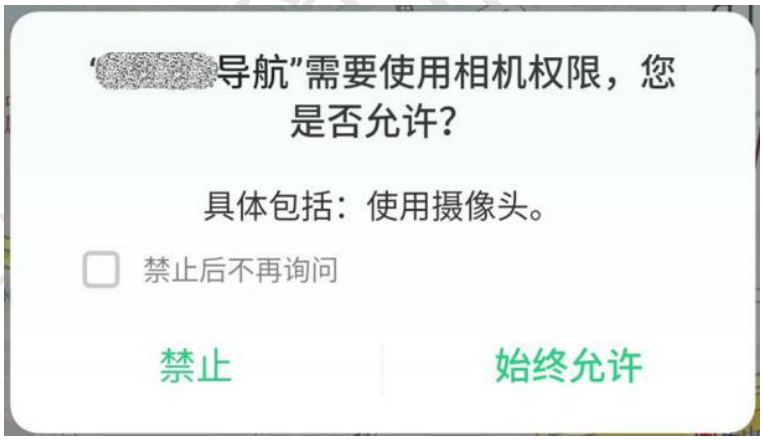


图 3-10 某地图导航类 APP 未公示列明收集使用相机权限

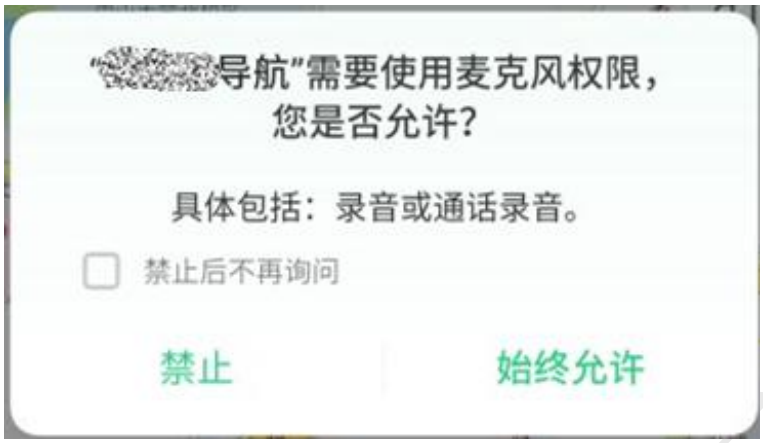


图 3-11 某地图导航类 APP 未公示列明收集使用麦克风权限

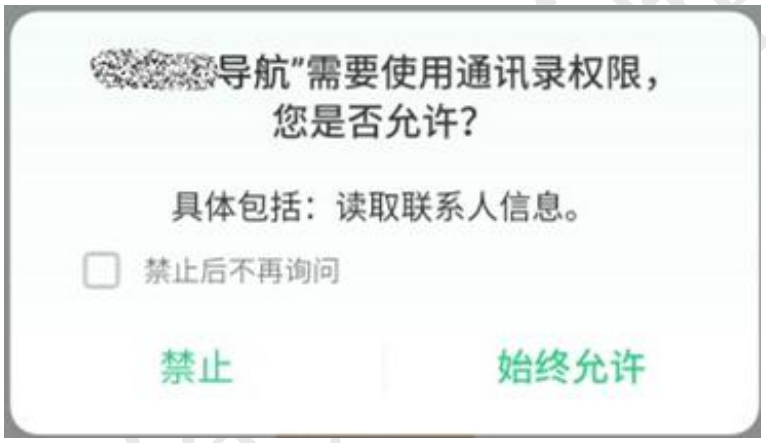


图 3-12 某地图导航类 APP 未公示列明收集使用通讯录权限

3.2.7.某证券交易类 APP 存在“界面劫持”高危安全漏洞被责令整改

2020 年 12 月广东省通信管理局 APP 监管平台发现某证券交易 APP 存在“界面劫持”高危安全漏洞。在用户移动终端被入侵的情况下，入侵者通过 Activity 界面劫持漏洞可对客户端内的登录界面、注册页面、支付界面进行 Activity 方式的界面覆盖，诱导用户输入账号和密码，从而窃取用户的敏感信息，甚至劫持支付，导致用户财产损失。针对此安全隐患，广东省通信管理局及时通过 APP 监管平台通报 APP 运营者限期整改，并同步通知应用商店督促整改。APP 运营者反馈整改后，广东省通信管理局进行了复测验证，确认该 APP 已完成修复。

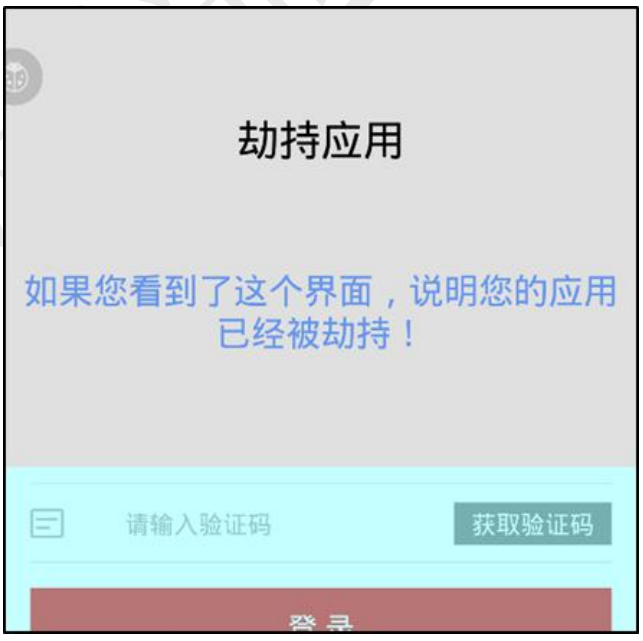


图 3-13 某证券交易类 APP 存在“界面劫持”高危安全漏洞

3.2.8.某购物类 APP 存在“webview 远程代码执行”高危安全漏洞被责令整改

2020 年 12 月广东省通信管理局 APP 监管平台发现某购物 APP 存在“WebView 远程代码执行”高危安全漏洞。该 APP 采用 webView 技术加载商品浏览网页，由于 APP 开发者未正确使用 WebView.addJavascriptInterface 方法，用户在使用该 APP 浏览商品详情过程中，远程攻击者借助 JavaReflection API 可以通过该漏洞对使用该 APP 的用户实现远程任意代码执行攻击，进而访问用户设备的 SD 卡、甚至是联系人信息、短信等敏感信息，导致用户财产损失，用户手机也可能被植入木马病毒，进而导致手机被 root，甚至被远程操控。针对此隐患，广东省通信管理局及时通过 APP 监管平台通报 APP 运营者限期整改，并同步通知应用商店督促整改。APP 运营者反馈整改后，广东省通信管理局检测人员进行了复测验证，确认该 APP 已完成修复。

3.2.9.某游戏类 APP 存在“Janus 签名机制漏洞”高危安全漏洞被责令整改

2020 年 12 月广东省通信管理局 APP 监管平台发现某游戏 APP 存在“Janus 签名机制漏洞”高危安全漏洞。该漏洞可以让攻击者绕过安卓系统的 signature scheme V1 签名机制，进而直接对 APP 进行篡改。而且由于安卓系统的其他安全机制也是建立在签名和校验基础之上，该漏洞相当于绕过了安卓系统的整个安全机制。一旦攻击者利用该 APP 的漏洞篡改成带有恶意代码的仿冒 APP 再通过社交软件、二维码等渠道传播，用户下载安装使用被篡改仿冒的游戏 APP 后，个人游戏账号、密码就可能被窃取，导致游戏虚拟资产损失，手机也可能被植入木马病毒，进而导致手机被 root，甚至被远程操控。针对此隐患，广东省通信管理局及时通过 APP 监管平台通报 APP 运营者限期整改，并同步通知应用商店督促整改。APP 运营者反馈整改后，广东省通信管理局检测人员进行了复测验证，确认该 APP 已完成修复。

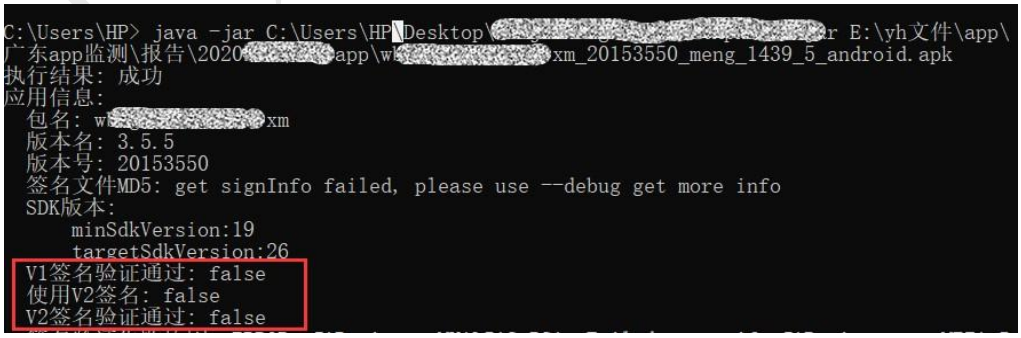


图 3-14 某游戏类 APP 存在“Janus 签名机制漏洞”高危安全漏洞

3.2.10.某金融类 APP 存在流氓行为、信息窃取等恶意行为被下架封堵

2020 年 7 月广东省通信管理局监测发现，某金融借贷类 APP 存在信息窃取、流氓行为等恶意行为。经分析，该款 APP 嵌入了第三方 SDK“com.creditx.xbehavior.sdk”（氪信 SDK），嵌入该 SDK 的该款 APP 启动后会私自获取用户地理位置、手机号码、短信、通讯录以及手机 IMEI、IMSI、设备 ID、基带版本、用户网络 wifi 状态等用户手机基本信息，具有窃取隐私属性。此外，该款 APP 使用第三方插件开机自动启动服务，且源码中加载广告 ID，企图加载某互联网企业广告，具有流氓行为。2020 年 7 月 16 日中央电视台延迟播出的“315”晚会中，也已曝光氪信 SDK 插件侵犯用户隐私的问题，但该金融借贷 APP 尚未完成自查整改。针对此 APP 仍存在的恶意行为，广东省通信管理局及时对该 APP 下载链接采取封堵措施，并同步通知应用商店下架处置。

```
C2283a(Context context) {
    this.f7673b = C2352f.m10090m(context);
    this.f7674c = C2352f.m10093p(context);
    this.f7675d = C2352f.m10092o(context);
    this.f7677f = C2352f.m10091n(context);
    this.f7676e = C2352f.m10094q(context);
    this.f7681j = C2352f.m10069a(context);
    this.f7682k = C2352f.m10095r(context);
    this.f7683l = C2352f.m10096s(context);
    this.f7684m = C2322a.f7869a;
    this.f7685n = C2352f.m10073b();
    this.f7686o = C2362n.m10139a(context);
    this.f7687p = C2352f.m10087j(context);
    this.f7688q = C2352f.m10074b(context);
    this.f7689r = C2352f.m10068a();
    this.f7690s = C2352f.m10084g(context);
    this.f7692u = C2352f.m10088k(context);
    this.f7691t = C2352f.m10089l(context);
    long[] d = C2352f.m10078d();
    this.f7694w = d[0];
    this.f7693v = d[1];
    long[] e = C2352f.m10080e();
    this.f7696y = e[0];
    this.f7695x = e[1];
    this.f7697z = "android";
    this.f7661A = Build.VERSION.RELEASE;
    this.f7662B = Build.VERSION.SDK_INT;
    this.f7666F = C2352f.m10081f();
    this.f7667G = C2352f.m10083g();
    this.f7665E = TimeZone.getDefault().getID();
    if (C2335k.m9996a().mo11356c()) {
```

图 3-15 APP 运行后加载获取 IMEI、IMSI、设备 ID 等用户

手机基本信息，具有隐私窃取属性

```
</service>
<receiver android:name="p025cn.jpush.android.service.PushReceiver" android:enabled="true" android:exported="false">
    <intent-filter android:priority="1000">
        <action android:name="cn.jpush.android.intent.NOTIFICATION_RECEIVED_PROXY"/>
        <category android:name="com.qb.quickloan"/>
    </intent-filter>
    <intent-filter>
        <action android:name="android.intent.action.USER_PRESENT"/>
        <action android:name="android.net.conn.CONNECTIVITY_CHANGE"/>
    </intent-filter>
    <intent-filter>
        <action android:name="android.intent.action.PACKAGE_ADDED"/>
        <action android:name="android.intent.action.PACKAGE_REMOVED"/>
        <data android:scheme="package"/>
    </intent-filter>
```

图 3-16 使用第三方插件开机自动启动服务，具有流氓行为

```
    /* renamed from: s */
    public static String m10096s(Context context) {
        C2369t.m10150a(context);
        if (f7972k == null && m10070a(9, true)) {
            try {
                Class<?> cls = Class.forName("com.google.android.gms.ads.identifier.AdvertisingIdClient");
                Object invoke = cls.getMethod("getAdvertisingIdInfo", new Class[]{Context.class}).invoke(cls.newInstance(), ne
                f7972k = String.valueOf(invoke.getClass().getMethod("getId", new Class[0]).invoke(invoke, new Object[0]));
            } catch (Exception e) {
            }
        }
        return f7972k;
    }
```

图 3-17 源码中加载某企业广告 id，具有流氓行为

4. 构建 APP 监管治理新格局

构建 APP 个人信息保护监管治理新格局，不仅需要政府“外施监管压力”，不断强化 APP 监督执法，更需要 APP 从业者“内生安全动力”，主动落实用户个人信息保护主体责任，同时也需要行业社会组织、上下游产业链、第三方专业机构等行业各方力量积极参与，多管齐下，相互支撑、相互制衡，协同共治。本章节从政府监管、行业自律、生态构建等多维度提出了构建 APP 监管治理新格局的思路，对 APP 分发平台（以下均包括 APP 应用商店、下载网站和其他分发渠道）、APP 运营者、第三方 SDK 提供者等提出落实主体责任的具体要求，并为 APP 用户提供安全使用建议，提升用户风险防范意识。

4.1. 加强行政执法，加大监督惩处力度

广东省通信管理局加强常态化监督检查，依法加大对各类违法违规行为的处置和曝光力度。对整改不彻底和没有举一反三对标自查自纠仍然存在问题的，广东省通信管理局将采取公开通报、组织下架、断开接入、行政处罚并将受到行政处罚的违规主体纳入电信业务经营不良名单或失信名单等措施，不断压实 APP 运营者、分发平台和第三方 SDK 的主体责任，促使企业进一步提高政治站位，坚决把用户合法权益放在首位，深刻领会并用实际行动践行习近平总书记提出的以人民为中心的发展思想，切实把实现好、维护好用户

的合法权益和赢得用户的信任作为企业的立业之本。

4.2. 加强技管结合，持续提升 APP 技术监测能力

广东省通信管理局坚持“技管结合，以网管网”的监管理念，大力推进 APP 监管平台建设，并凝聚产业力量，鼓励有条件的企业积极参与，持续提升行业主管部门 APP 技术检测能力和水平。APP 监管平台聚焦用户个人信息保护和网络数据安全，以发现问题为出发点，以解决监管痛点并建立长效机制为目标，重点关注用户活跃度较高的应用领域，对在广东省内提供服务的相关 APP 进行监督抽查。目前 APP 监管平台具备了“三库四能力”的闭环监管技术支撑能力，基于基础资源数据库（APP 信息库、APP 商店库、APP 运营者库）实现了主动监测能力、溯源分析能力、政企通报能力、应急处置能力等四种 APP 监管技术支撑能力。下一步，广东省通信管理局将不断扩大平台数据采集范围和提升监测能力，覆盖更多的 APP 分发平台，扩展安全分析类型和检测方法，进一步提高平台监测广度和检测深度，强化自动研判，提高 APP 监管效率。

4.3. 指导组建安全生态联盟，构建 APP 绿色生态圈

广东省通信管理局指导广东省互联网协会发起成立广东省 APP 安全生态联盟。联盟的宗旨是全面贯彻落实《网络安全法》等法律法规和习近平总书记关于网络强国的重要思想，致力于吸纳 APP 产业生态各领域的企业、机构和人才，

搭建 APP 行业交流平台，发挥联盟各成员单位优势，建立联盟协作机制，共同分析 APP 行业发展状况和趋势，总结行业合规管理经验，探索制定 APP 从业规范标准，并加强行业自律，定期组织开展培训交流，共享安全成果，同时向政府主管部门提出建议，构建一个自我监督、资源共享、互利共赢的 APP 绿色生态圈，提升 APP 开发运营企业安全合规水平，促进移动互联网健康有序发展。

联盟成员包括了 APP 开发企业、APP 分发平台、APP 运营企业、网络安全企业、基础电信企业、相关政府部门、事业单位、媒体单位、科研院校等 APP 产业生态各领域的企业、机构和人才。

4.4. 倡议签署个人信息保护自律公约，促进行业自律

广东省通信管理局指导广东省互联网协会、广东省通信行业协会联合制定《广东省 APP 用户个人信息保护自律公约》并组织相关 APP 应用商店和运营企业签署，同时倡议广大 APP 从业者积极遵守。自律公约对企业用户个人信息保护方面进行规范，为开展个人信息保护行业自律工作提供参考和依据，引导广东省互联网协会和广东省通信行业协会会员单位以及其他 APP 从业者（包括移动智能终端生产者、移动智能终端操作系统服务提供者、APP 分发服务提供者、APP 运营者、APP 开发者、第三方 SDK 服务提供者等）进一步落实个人信息保护主体责任，自觉维护用户合法权益。

自律公约的签署通过两种方式进行。一是现场签署，广东省互联网协会、广东省通信行业协会组织了省内二十家知名 APP 运营企业相关负责人到广东省通信管理局 APP 个人信息保护监管成果发布会上现场签署《广东省 APP 用户个人信息保护自律公约》，签署企业承诺将严格落实电信主管部门监管要求，自觉遵守和履行公约内容，保障用户合法权益。二是线上签署，广东省互联网协会、广东省通信行业协会持续分批组织省内重点 APP 运营者通过线上方式签署《广东省 APP 用户个人信息保护自律公约》并相互监督履行公约，营造 APP 行业依法合规经营的良好氛围，促进行业健康有序发展。

4.5. 压实 APP 相关企业主体责任，维护用户合法权益

4.5.1. 压实 APP 分发平台主体责任

4.5.1.1.落实 APP 上架实名登记

APP 分发平台应严格落实网络实名制，在为 APP 提供上架、发布、下载、推荐等分发服务，以及 APP 上架主体（包括 APP 提供者、运营者、开发者）发生变更后再次申请相关服务时，做好 APP 上架主体真实身份信息和联系方式登记。未提供真实身份信息的，不得为其提供 APP 分发服务。

4.5.1.2.落实上架 APP 软件包和相关信息日志留存

分发平台应留存上架 APP 相关信息以备追溯检测，留存内容包括但不限于历次上架 APP 软件包、包名、版本号、上

架时间、功能简介、类别、用途、MD5（消息-摘要算法 5）校验值、服务器接入等信息，相关信息的留存时间不短于半年。

4.5.1.3.加强 APP 安全上架审核及跟踪管理

分发平台应建立 APP 上架审核及跟踪管理机制。上架前，对 APP 进行审核检测，将 APP 数据安全与个人信息保护措施作为审核检测重点，对发现存在恶意行为和内容明显违法违规的 APP 不予上架；上架后，对在架 APP 进行动态跟踪监测，及时处理自查发现和电信主管部门要求下架的违法违规 APP。

4.5.1.4.规范 APP 上架基本信息公示

分发平台在发布 APP 信息时，应规范发布 APP 的名称、应用类型、图文简介、应用提供者、年龄分级、应用大小、下载数量、安全检测、权限检测、广告检测、隐私政策等 APP 上架基本公示信息，不得发布虚假违法广告，不得使用欺诈、诱骗的方式诱导、误导用户下载 APP。

4.5.1.5.加强对 APP 提供者的监管政策宣贯

分发平台应强化平台社会责任，完善移动应用软件分发服务协议，进一步明确与 APP 提供者的权利与义务，并加强对 APP 提供者的监督管理和政策宣贯，督促 APP 提供者遵守国家法律法规和 APP 分发服务协议。

4.5.1.6.公开投诉举报方式并受理公众举报

分发平台应建立 APP 网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关 APP 网络信息安全的投诉和举报。

4.5.1.7.履行 ICP 备案或取得相应电信业务许可

分发平台应向属地电信主管部门履行 ICP 互联网信息服务备案手续，涉及经营电信业务的应当取得电信主管部门颁发的相应电信业务许可证。

4.5.2. 压实 APP 运营者主体责任

4.5.2.1.健全 APP 安全合规管理制度和工作机制

APP 运营者作为责任主体，应建立企业内部的网络与信息安全保障机制，明确网络与信息安全领导架构、负责人并设置相应工作团队，制定完善 APP 安全合规管理制度，保障经费、技术和人力投入，严格履行法律法规规定的责任义务，依照国家、行业相关规定和 APP 安全标准、政策要求、行业指南，对自有 APP 开展安全合规自评估，并及时完成整改。

4.5.2.2.重视保障用户的知情权、选择决定权

APP 运营者应严格遵守国家相关法律法规和工信部相关规范标准，充分保障 APP 用户对个人信息收集、使用的知情权和选择决定权，切实落实“公开收集、使用用户个人信息（包括索取手机权限）的规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意”等要求，不得使用默认同意、

默认勾选同意等方式。

4.5.2.3.严格遵循合法、正当、必要的原则

APP 运营者收集、使用信息，应当遵循合法、正当、必要的原则，不得收集与其提供服务无关的个人信息，不得在用户未使用相关功能或服务时，提前索取手机权限或超频次调取程序收集个人信息，不得以欺骗、误导、强迫等方式或者违反法律法规和双方约定收集、使用个人信息。不得因用户未提供非必要权限，拒绝提供业务功能、退出应用程序。

4.5.2.4.加强对所使用第三方插件、程序代码的安全审核，并做好第三方收集使用个人信息规则的公示

APP 运营者作为责任主体，应采用必要的技术检测手段加强对所使用第三方 SDK 插件、程序代码的安全审核，不得使用包括恶意行为的插件和程序代码。应加强对第三方 SDK 提供者的服务协议及产品说明的审核，不使用个人信息保护不到位的第三方插件、程序代码。涉及第三方插件或程序代码收集、使用个人信息的，应同时落实“公开收集、使用用户个人信息（包括索取手机权限）的规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意”的要求。

4.5.2.5.保障所收集使用的数据和个人信息的安全

APP 运营者应采取技术措施和其他必要措施确保所收集使用的数据和个人信息全生命周期安全，防止信息泄露、毁损、丢失。措施包括但不限于：采集环节遵循合法正当必

要原则并征得用户同意，传输环节应采取加密传输技术措施，存储环节应采取加密、备份保护措施，使用、共享个人信息时，应按最小化原则进行脱敏和匿名化处理，定期开展 APP 及服务端安全风险评估，及时修复漏洞、消除隐患，采取必要 APP 加固措施，使用完毕、终止服务时应及时彻底删除处理有关信息并确保不可还原等。APP 运营者在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

4.5.2.6.不得恶意干扰用户终端环境和干扰用户使用 APP

APP 运营者不得违反《规范互联网信息服务市场秩序若干规定》（工业和信息化部令第 20 号）实施侵犯用户合法权益的行为，包括但不限于：恶意干扰用户终端上其他 APP 提供的服务；恶意干扰 APP 的下载、安装、运行和升级；恶意对其他 APP 实施不兼容；恶意修改或者欺骗、误导、强迫用户修改手机和其他 APP 设置参数；捏造、散布虚假事实诋毁其他 APP，误导用户卸载 APP；欺骗、误导或者强迫用户下载安装使用 APP（例如未经用户同意捆绑安装其他 APP）；未提供弹窗关闭方式；用户未提供非必要权限，拒绝提供业务功能或退出应用程序等。

4.5.2.7.及时响应处理个人信息删除、更正诉求

APP 运营者应建立个人信息删除、更正的投诉、举报制度，公布投诉、举报方式，并在承诺时限内（最长不超过 15

个工作日）及时响应受理有关删除、更正个人信息的诉求。有提供账号注册功能的 APP 应同时提供账号注销功能或相应指引方式，不得为更正、删除个人信息或注销用户账号设置不必要或不合理条件。

4.5.2.8.配合 APP 分发平台提供真实身份信息、联系方式、上架审查材料和公示信息

APP 运营者要配合 APP 分发平台提供上架主体真实身份信息、联系方式、计算机软件著作权登记证书、其他相关资质证明、应用软件功能简介、隐私政策、权限列表、收集使用个人信息规则等上架审核材料和上架公示信息等。

4.5.2.9.履行互联网信息服务备案（ICP 备案）手续，涉及电信业务的应取得相应电信业务许可

涉及互联网信息服务的 APP 运营者应向属地电信主管部门履行互联网信息服务备案（ICP）手续，涉及电信业务的，APP 运营者应取得电信主管部门颁发的相应电信业务许可证。

4.5.3. 压实第三方 SDK 提供者主体责任

第三方 SDK 提供者应切实落实主体责任，按照 APP 运营者同等的义务与责任落实用户个人信息保护规定和相关要求，吸取 2020 年央视 315 晚会曝光的第三方 SDK 违法违规收集用户个人信息行为的教训，不得在 SDK 中设置恶意程序。第三方 SDK 提供者要根据电信主管部门监管要求加

强合规管理，并协助配合停止为违法违规 APP 提供相关服务。

第三方 SDK 提供者应按照用户个人信息保护规定和要求提供完善的 SDK 使用协议和产品说明，自觉明确 SDK 产品收集、使用个人信息规则和安全保护措施。SDK 涉及收集、使用个人信息的，要在使用协议和产品说明中要求并指引 APP 开发运营者落实“公开收集、使用用户个人信息（包括索取手机权限）的规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意”的要求。涉及需要 SDK 更正、删除用户个人信息的，SDK 提供者应配合 APP 开发运营者履行相应责任义务。

4.6. 提升用户风险防范意识，养成安全使用习惯

用户需要加强个人信息保护，提升安全风险防范意识，掌握相关网络知识和使用技能，养成良好的 APP 安全使用习惯。本白皮书提供以下参考建议：

4.6.1.从 APP 运营者官网或正规应用商店下载 APP，不点击来源不明的链接下载安装软件

APP 用户应对 APP 安装下载来源的可靠性进行仔细考量。建议从 APP 运营者官网或正规应用商店下载 APP 安装包，谨慎从社交软件、短彩信传播的链接和二维码下载，来历不明的 APP 坚决不下载安装，避免进入钓鱼网站下载仿冒 APP。下载之前，应查看应用商店公布该 APP 的上架主体、安全检测、权限检测、年龄分级等信息加以甄别。

4.6.2.遵循最小授权原则管理 APP 权限

APP 安装和使用 APP 时，应谨慎授权予“通讯录”“短信”“存储（媒体相册）”“摄像（照相）”“麦克风”“位置”等敏感权限，在缺乏相应合理的使用场景并告知明确索取权限目的情况下，坚决不予授权。对于临时需要授权使用的权限，应选择设置为“每次询问”或者手动临时开启权限，使用完毕及时关闭。对于明确不影响 APP 使用的权限，拒绝申请并点击“不再询问”。发现 APP 可疑行为时，应及时关闭不必要权限，退出并卸载，减少个人信息泄露的风险。

4.6.3.谨慎使用公共 WIFI，避免通过不安全充电设备进行充电

尽量不要连接公共 WIFI（尤其是免密 WIFI）进行上网和下载使用 APP。尽量不安装和使用共享 WIFI 密码的 APP，避免家庭 WIFI 标识和密码泄漏。建议进入公共场合时关闭 WIFI 开关，以免在不自觉的情况下自动连接不安全热点。避免通过公共电脑和带有软件系统功能的充电设备为手机充电，尤其需要防范机场、火车站、客运站、休闲区、公共区域提供的此类充电设备。

4.6.4.注意日常生活中的隐私保护

APP 用户在日常生活中不要随意扫描陌生的二维码，或者随意点击来路不明的链接。在网络上不要轻信中奖、问卷、星座测试，尤其要防范收集个人敏感信息的活动，以免造成

个人信息泄露。不同 APP 注册账号所使用的密码不要相同，密码不要设置成生日、简单数字排列等弱口令。

通过社交类 APP 发布个人信息时需要密切注意以下信息的隐私保护：火车票、飞机票、登机牌含多项重要个人信息，护照、门禁卡、车牌可能暴露当前位置或家庭住址，定位信息直接暴露生活或工作详细信息。孩子照片和姓名分享时建议设置分享范围，以有限分组分享孩子的照片。注意家中老人信息保护，家中老人更容易受蒙蔽和欺骗，共享家中老人信息会增加不法分子联系老人、欺诈老人的可能性。

4.6.5.不要随意破解手机、开启 root 权限，以及刷装不明来源的第三方操作系统和桌面应用

破解手机、开启 root 权限，会使手机处于极不安全的环境。刷装第三方操作系统和 UI 桌面应用虽会带来不同于原厂操作系统的界面和操作体验，但同时也可能由于第三方操作系统和桌面应用存在恶意程序或安全漏洞，从而导致个人信息被窃取，因此建议保持原厂操作系统并及时通过官方提供的系统更新。

4.6.6.遇到 APP 违法违规行为可向有关机构举报，涉及网络违法犯罪的应及时报案

用户如发现 APP 违反相关法律法规和规定要求，可向 APP 运营者、应用商店投诉举报，并监督其是否妥善处理；对处理结果不满意的，用户可向有关投诉举报受理机构举报。

如发现窃取公民个人信息并涉嫌违法犯罪，应及时保留证据并向公安机关报案。

5. 结束语

APP 安全治理是一场持久战、攻坚战，必须坚持标本兼治、综合治理。个人信息保护和网络数据安全监管工作任重而道远，广东省通信管理局将坚持以人民为中心的发展思想，继续履行职责做好网络安全和 APP 监管工作。持续加强与其他政府部门之间的协同配合，压实 APP 分发平台、APP 运营者和第三方 SDK 提供者的主体责任，切断违法违规 APP 传播链条，构建全环节管理的综合治理模式，持续深入推进 APP 专项治理工作。

下一步，广东省通信管理局将持续加强技术手段建设，加大监督检查力度，及时发现并通报侵犯用户权益的 APP，同时加强对已通报 APP 及其运营者关联 APP 进行跟踪复查，对问题严重或拒不整改的，坚决采取下架、停接入、停域名、行政处罚以及纳入电信业务经营不良名单或失信名单并公开曝光等措施，依法严厉处置，切实维护 APP 用户合法权益和网络安全秩序，让“以人民为中心”的 APP 监管理念在广东落地生根，让人民群众放心享受信息通信业发展带来的各项美好成果，确保“十四五”开好局，起好步，以优异成绩庆祝建党 100 周年。

附录一：广东省通信管理局 APP 专项治理工作公开发布的报道

报道一：广东省通信管理局严查违规 APP 应用商店为电信用户合法权益保驾护航

发布时间：2019 年 3 月 14 日

广东省通信管理局严查违规 APP 应用商店为电信用户合法权益保驾护航

近年来，移动互联网应用程序（APP）得到广泛应用，在促进经济社会发展、服务民生等方面发挥了不可替代的作用。同时，APP 强制授权、过度索权、超范围收集个人信息的现象大量存在，违法违规使用个人信息的问题十分突出，广大网民对此反应强烈。广东省通信管理局加大执法力度，近期查处了一批违反《网络安全法》、《规范互联网信息服务市场秩序若干规定》（工信部第 20 号令）、《公共互联网网络安全威胁监测与处置办法》（工信部网安〔2017〕202 号）的 APP 应用商店，有力保障了电信用户的合法权益。

被查处的 APP 有的私自添加桌面广告图标，弹窗插屏广告；有的安装运行会加载释放广告子包，匿名弹窗插屏广告，广告界面难关掉而且可能在无意操作中就下载； 有的在安装运行后无法使用并要求下载其他应用软件。截止发稿之日，广东省通信管理局已对珠海市某通讯设备有限公司、深圳某计算机通信科技有限公司、深圳市某网络科技有限公司、彭某杨等应用商店（平台）的六款应用核实存在“未经用户同意强行捆绑推广其他应用软件”的问题，造成用户流量损失，间接导致资费消耗，已对上述企业和个人给予警告的行政处罚。

此外，广东省通信管理局还对广州、深圳市等十五家企业及个人的应用商店（平台）合计 138 款 APP 下发了责令整改通知书。

广东省通信管理局将继续履职，加强对违法违规收集使用个人信息行为的监管和处罚，为净化互联网网络环境保驾护航！

报道二：多款 APP 收集个人敏感信息

广东省通信管理局依法查处涉事企业

发布时间：2019 年 4 月 24 日

多款 APP 收集个人敏感信息

广东省通信管理局依法查处涉事企业

互联网时代，各类 APP 给我们带来便利的同时，也留下了个人信息泄露的隐患，部分 APP 获取了实际功能不需要的敏感权限。今年央视“3·15”晚会曝光了某些企业利用 APP 违规收集个人信息进行非法牟利的违法行为。

广东省通信管理局于“3·15”前夕抽查了辖区内各大应用商店，重点排查收集用户信息的违规行为，发现违规 APP20 个。广东省通信管理局约谈涉事应用商店所属企业，包括广州优视网络科技有限公司（PP 助手）、广东太平洋互联网信息服务有限公司（太平洋电脑）等公司，责令其下架违规 APP。截至发稿之日，违规 APP 已全部下架。同时，广东省

通信管理局已对北京钰诚科技有限公司、陕西艺唐新文化传播有限公司、北京享宇金融服务外包有限公司、鼎盛鑫金融服务（深圳）有限公司等 APP 运营企业给予了警告的行政处罚。

本次发现的违规 APP 多为贷款类，存在的主要问题有：（一）注册时没有公示用户服务协议和隐私协议；（二）隐私协议未明确收集哪些用户个人信息；（三）隐私协议包含获取“用户的手机通讯运营商的服务密码、验证码”，甚至“学历信息、学信网账户名及密码等”；（四）未提供注销功能；（五）存在静默下载的问题，使用过程中在用户不知情时下载别的应用软件，消耗流量；（六）存在积分墙的限制，即在安装运行后无法使用并要求下载其他应用软件。

中央网信办、工信部、公安部、市场监管总局等四部门联合发布《关于开展 APP 违法违规收集使用个人信息专项治理的公告》指出，APP 运营者收集使用个人信息时要严格履行《网络安全法》规定的责任义务，对获取的个人信息安全负责，采取有效措施加强个人信息保护。遵循合法、正当、必要的原则，不收集与所提供服务无关的个人信息；收集个人信息时要以通俗易懂、简单明了的方式展示个人信息收集使用规则，并经个人信息主体自主选择同意；不以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反法律法规和与用户的约定收集使用个人信息。

广东省通信管理局将严格落实《网络安全法》、《电信和互联网用户个人信息保护规定》（工业和信息化部令第 24 号）中关于用户信息保护的规定，按照《关于开展 APP 违法违规收集使用个人信息专项治理的公告》持续加强电信和互联网用户个人信息保护，依法依规严厉查处涉事企业，并将违规企业纳入电信业务经营不良名单。

附：受处罚 APP 企业信息

报道三：广东省通信管理局关于转发工信部开展 APP 侵害用户权益专项整治工作的通知

发布时间：2019 年 11 月 8 日

广东省通信管理局关于转发工信部开展 APP 侵害用户权益专项整治工作的通知

各 APP 分发服务提供者、各 APP 服务提供者:

APP 违规收集个人信息、过度索权、频繁骚扰、侵害用户权益等问题引起社会关注度高。工业与信息化部决定组织开展 APP 侵害用户权益专项整治行动工作，印发了《关于开展 APP 侵害用户权益专项整治工作的通知》（工信部信管函〔2019〕337 号，以下简称《通知》，网页地址：http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c7506353/content.html），现将该通知转发给你们，各相关企业应高度重视，认真执行落实。

一、本次专项整治工作的对象

一是 APP 服务提供者，主要检查是否存在《通知》中涉及的四个方面 8 类问题，8 类问题的典型场景参见《关于开展 APP 侵害用户权益专项整治工作的解读》（网页地址：http://www.miit.gov.cn/n1146295/n7281315/c7507241/content.html）；二是 APP 分发服务提供者，含应用商店和基础电信企业营业厅等承担 APP 分发功能的各类企业，主要检查是否已

落实《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）等有关要求。

二、专项整治工作分三个阶段实施

（一）企业自查自纠阶段：请各收文单位按照《通知》要求于 11 月 10 日前全面开展自查自纠。

（二）监督抽查阶段：我局将抽查省内应用商店的部分 APP，重点抽测与群众生活密切相关、下载使用量较大的 APP 产品和分发平台。

（三）结果处置阶段：我局将根据监督抽查结果对存在问题的企业依法依规予以处理，采取的措施包括但不限于通报、约谈、责令整改、行政处罚、媒体曝光等。

请各单位切实提高思想认识，畅通用户投诉渠道，巩固建立长效机制。

扫一扫在手机打开当前页

报道四：广东省通信管理局聚焦用户个人信息保护 纵深推进 APP 依法监管

发布时间：2020 年 1 月 21 日

广东省通信管理局聚焦用户个人信息保护 纵深推进 APP 依法监管

随着移动互联网与智能终端全面渗透，APP 已经超越传统网站成为承载网络服务和信息数据的主要载体，极大地丰富了人们的生活。然而，APP 违规收集个人信息、过度索权、频繁骚扰用户等侵害用户权益问题日益突出。为有效打击侵犯用户隐私信息的违法违规行为，广东省通信管理局 2019 年下架存在恶意程序和侵害用户权益的 APP 175 款，发出责令整改通知书 44 份（共 185 款 APP），关停涉黄涉赌等传播违法有害信息的 APP 100 多个，处罚 APP 应用商店和 APP 运营者 14 起。

2020 年 1 月 16 日，为进一步巩固深化 APP 侵害用户权益专项整治行动成果，广东省通信管理局召开 APP 监管政策宣贯会，传达 APP 相关整治工作要求及监管法规依据。省内基础电信企业、主要 APP 分发平台（应用商店）、相关 APP 运营企业、管局技术支撑单位专家共 50 余人参加本次会议。

会上，广东省通信管理局全方位进行 APP 监管政策和法律要求宣贯，结合近期处罚案例，对常见的侵犯用户合法权益的四个方面 8 类问题对应的法律条款、罚则及常见的违法违规场景进行了深度解读。本次宣贯会议进一步加深了企业对 APP 监管政策和法律的理解与认识，明晰了电信行业主管部门对 APP 监管在用户信息保护、实名制、网站备案和域名注册管理等方面的各项要求，有利于提高相关企业的遵法守法意识和建立 APP 长效治理机制。

会议对 APP 应用商店及 APP 运营者提出了三点要求：一是要高度重视，落实企业主体责任，践行习近平总书记“网信事业要发展，必须贯彻以人民为中心的发展思想”讲话精神，坚持以人民为中心，把用户感知作为企业发展内驱动力，切实做好用户权益保护和网络信息安全相关工作；二是要技管结合，健全相关管理制度和工作机制，明确人员职责分工，建立健全配套管理和技术手段，认真开展 APP 安全评估与合规检查；三是要加强学习，组织相关责任人员加强法律法规学习和培训，增强法律意识和技能，切实履行主体责任。

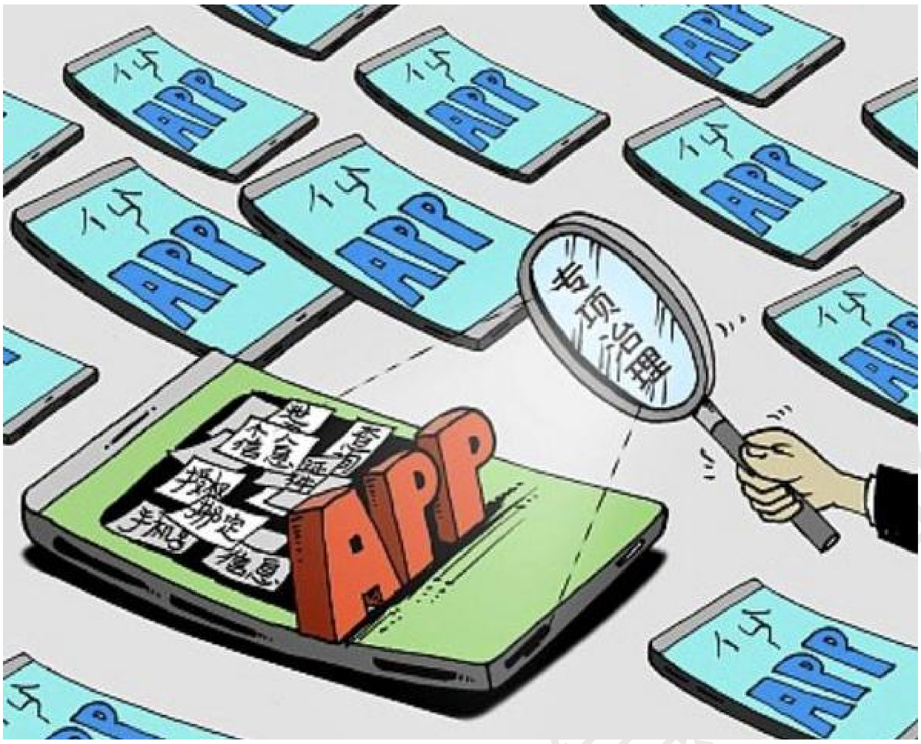
报道五：广东省通信管理局查处一批

违反用户个人信息保护规定 APP

发布时间：2020 年 3 月 15 日

广东省通信管理局查处一批违反用户个人信息保护规定 APP

广东省通信管理局高度关注 APP 的个人信息保护和数据安全问题并持续开展相关监管工作，2020 年 1 月 16 日召开 APP 监管政策宣贯会，对省内基础电信企业、主要应用商店、重点 APP 运营企业传达 APP 相关整治工作要求及监管法规依据。“3·15”之际，广东省通信管理局再次聚焦用户权益保护开展 APP 隐私合规及网络数据安全专项检查工作，督促各应用商店排查疑似违规 APP 七万余款，发现并下架违规 APP5998 款，驳回违规 APP 上架申请 2807 次。**近日，广东省通信管理局加大执法力度，对抽检存在问题的 21 款 APP 运营者发出责令整改通知书并同步通知应用商店下架处置，对问题突出的“我连网”“聚超值”等 5 款 APP 运营者做出警告并罚款的行政处罚。**



此次查处的 APP 问题有两类，**一是违反用户个人信息保护规定**，主要体现在“无隐私政策或隐私政策中没有收集使用个人信息规则”“违反必要原则，索取或自动开启可收集用户敏感信息且与当前服务无关的权限”“未提供账号注销功能或指引”“默认同意或默认选中隐私政策、服务协议”“不给非运行必要权限自动退出”“私自共享给第三方”“未明示收集规则提前索取权限”“超出隐私政策列举范围索取权限”等；**二是存在可能导致信息泄漏的 APP 安全隐患**，主要体现在“源文件风险”“安全策略风险”“组件风险”“Activity 劫持风险”“SO 注入风险”“通讯传输风险”“内部数据交互风险”“程序反编译风险”“键盘劫持风险”“WebView 远程代码执行漏洞”等。两起典型案例通报如下：

一、深圳某科技有限公司运营的“我连网”APP 索取与服务无关的高敏感权限。广东省通信管理局在协助市场监督管理部门调查“我连网”APP 提供野猪肉和野猪捕获工具相关商品信息的案件时发现，该 APP 还存在违反用户个人信息保护规定的情形，具体表现在：APP 安装后首次运行，在没有使用任何功能和未告知收集个人信息规则的情况下，就向用户索取包括**“通讯录”“拍摄照片和录制视频”“录制音频”“发送和查看短彩信息”**等敏感权限在内的 7 项手机权限，APP 正式运行后主要界面也未见隐私政策或其他收集使用个人信息的规则，属于典型的“未公开收集使用规则”“未明示收集使用个人信息的目的、方式和范围”和“违反必要原则，收集与其提供的服务无关的个人信息”违法违规情形。

二、广东某互联网信息服务有限公司运营的“聚超值”APP 安装后默认开启“短信”等多项权限。该款 APP 安装后**尚未运行之前**就已默认打开用户手机的“存储”、“电话”、“位置”、“相机”、“短信/彩信”权限，APP 首次运行及正式运行后的主要界面均未发现隐私政策，注册账号时虽有《服务条款及使用协议》，但却直接默认勾选同意，且该协议也未提及任何手机权限获取和收集使用个人信息的情况。

上述两起案件，广东省通信管理局均已依据《网络安全法》《电信和互联网用户个人信息保护规定》相关规定责令该两家公司整改并对其做出给予警告和罚款的行政处罚。

另外，广东省通信管理局还在疫情防控期间对省内疫情防控有关互联网应用开展网络安全威胁监测，并为疫情防控重点保障 APP 运营单位在数据安全防护和隐私合规等方面提供相关技术服务和政策指导，切实保障我省疫情防控工作的顺利开展和相关 APP 的网络数据安全。。

个人信息保护和网络数据安全监管工作任重而道远，广东省通信管理局将“不忘初心、牢记使命”，坚持以人民为中心的发展思想，继续履行职责做好网络安全和 APP 监管工作。

报道六：广东省通信管理局不断加大执法力度

狠抓 APP 数据安全和隐私合规

发布时间：2020 年 9 月 15 日

广东省通信管理局不断加大执法力度

狠抓 APP 数据安全和隐私合规

继今年“3·15”查处一批违法违规 APP 后，广东省通信管理局不断加大执法力度，按照工业和信息化部《关于做好 2020 年电信和互联网行业网络数据安全管理工作的通知》（工信厅网安函〔2020〕103）和《关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》（工信部信管函〔2020〕164 号）的部署和要求，持续深入开展 APP 专项整治行动，狠抓 APP 数据安全和隐私合规。

一是督促辖区各应用商店加强分发审核，累计排查疑似违规 APP 近 140 万余次，发现并下架违规 APP 11.6 万款，驳回违规 APP 上架申请 15.9 万次。**二是加强对属地主流 APP 的重点巡查检测，**在工信部筛选的全国 TOP 550 中广东属地的 106 款主流 APP 基础上，扩大巡检范围至 5 千余款，同时委托第三方专业机构开展技术摸排和整改复测，累计检测 APP 五万余款。**三是建设 APP 监管系统**，坚持以“技管结合，以网管网”的思维治理 APP；**四是强化通报整改、下架处置、行政处罚和复测上架等闭环监管，**今年以来累计发出责令整改通知 110 份，直接下架 19 款，逾期未改正下架 4 款，对问题突出的“不思议迷宫”“鱼丸大人”“捕鱼荣耀”“省点花”“GO 桌面”“妈妈 100”等 18 款 APP 运营者做出警告并罚款的行政处罚决定。

被查处的 APP 存在两方面的问题，**一是违反用户个人信息保护规定**，主要有“APP 中未发现隐私政策或隐私政策未列明收集使用个人信息的目的、方式和范围”“未经用户阅读隐私政策或用户协议就索取手机敏感权限”“使用默认勾选或注册登录即代表同意等非明确方式表示用户同意隐私政策”“APP 集成多个第三方 SDK，但未在隐私政策中声明”“APP 内找不到账号注销的功能菜单或相关指引，没有在线客服或客服不受理账号注销事宜”“超声明、超必要、超前、超频次收集用户个人信息或索取相关手机权限”“不给非运行必要权限自动退出应用”等违法违规场景；**二是存在可能导致用户数据泄漏的安全隐患**，主要有“ JAVA 代码反编译风险”“组件风险”“数据明文传输风险”“键盘、界面劫持风险”“内存未加密敏感信息泄漏风险”“敏感代码未混淆风险”等。

下一步，广东省通信管理局将不断加强技术手段建设和加大检查执法力度，检查将覆盖第三方 SDK、小程序、快应用、应用分发平台、移动终端设备等，发现问题将依法责令改正，整改不彻底并情节严重的直接下架处置、给予行政处罚并将处罚主体纳入电信业务经营不良名单或失信名单、公开通报等措施，切实维护 APP 用户合法权益，提升 APP 网络数据安全水平。

附件：存在问题的 APP 名单（2020 年截至 9 月 15 日）

扫一扫在手机打开当前页

报道七：广东省通信管理局 APP 监管情况通报

（2020 年 10 月）

发布时间：2020 年 11 月 23 日

广东省通信管理局 APP 监管情况通报 （2020 年 10 月）

广东省通信管理局践行“以人民为中心”的发展思想，按照工业和信息化部关于 APP 数据安全和侵害用户权益专项整治的工作部署和要求，加强对属地 APP 的监督检查，建设 APP 监管平台，并委托第三方专业机构进行检测，累计检测 5 千余款 APP，共发现疑似存在问题 APP 237 款，经核验确定问题 APP 88 款，对其中“红娘婚恋”等 85 款 APP 运营者发出《违法违规 APP 处置通知》责令限期改正并通知各应用商店督促整改，对问题突出的“捷停车”“驾考家园”“凯立德导航”3 款 APP 运营企业做出警告并罚款的行政处罚决定。

被查处的 APP 存在两方面问题，一是 APP 及其后台服务器存在“明文存储密码”“反编译”“SQL 注入”等数据安全隐患问题；二是违反用户个人信息保护规定，包括“未公开明示收集规则”“默认勾选同意隐私协议”“未列明所集成 SDK 及其采集信息”“为注销账号、删除个人信息设置障碍”“未经用户同意共享给第三方”等侵犯用户对其个人信息处理享有的知情权、决定权，以及违反最小必要原则超前、超需、超频索取权限或采集信息，甚至不给必需权限不让用等强迫行为。

被予以行政处罚的“捷停车”APP 存在侵害用户权益的问题较为典型，其中最为突出的问题是：为用户注销账号设置过多不合理的障碍。APP 在用户注册账号时仅凭手机号码及验证码即完成注册，但注销账号时却要求用户提供手机号码的真实姓名、身份证正反面照片，甚至要求用户提供电信运营商出具的手机号码权属证明方可受理。此外，该 APP 还存在未使用相关功能就索取用户相机权限，且相机权限及 APP 集成的地图、支付、推送、统计、分享等多个 SDK 均未在隐私政策中逐一列明。对此，广东省通信管理局约谈了捷停车 APP 运营公司的负责人，对该公司做出给予警告并罚款两万元的行政处罚，同时报请工业和信息化部纳入电信业务经营不良名单。

下一步，广东省通信管理局坚持“技管结合”，不断加大对 APP 的监督检查力度，并强化对已责令整改或行政处罚的

APP 进行跟踪复测，对问题突出、整改不彻底的 APP 及运营企业，坚决采取下架、停接入、停域名、行政处罚以及纳入电信业务经营不良名单或失信名单并公开曝光等措施进行严厉处置，切实维护 APP 网络数据和个人信息安全。

附件：存在问题的 APP 名单（88 款）

扫一扫在手机打开当前页

报道八：209 款 APP 被广东省通信管理局责令整改或关停（2020 年 11-12 月）

发布时间：2021 年 1 月 11 日

209 款 APP 被广东省通信管理局责令整改或关停（2020 年 11-12 月）

广东省通信管理局持续开展 APP 专项整治工作，一是抓 APP 隐私合规，二是抓 APP 网络数据安全，三是打击违法有害 APP。2020 年累计发出《违法违规 APP 处置通知》责令整改 APP 400 多款，下架 APP 30 多款，关停违法有害 APP 300 多款，对问题突出 APP 运营者做出行政处罚 27 起。其中 11 至 12 月，隐私合规和网络数据安全监管方面，广东省通信管理局共监测发现 201 款 APP 存在侵害用户权益和安全隐患问题（详见附件 1），并依据《网络安全法》《电信和互联网用户个人信息保护规定》等法律法规对 APP 运营者发出《违法违规 APP 处置通知》，责令限期改正并通知各应用商店督促整改；打击违法有害 APP 方面，广东省通信管理局根据有关部门书面认定意见查处关停“汇聊”“富游网”“依依直播”等 8 款违法有害 APP 的网络服务，并通知相关应用商店下架（详见附件 2）。

本批被责令整改的 201 款侵害用户权益和安全隐患问题 APP，游戏类 30 款、金融类 30 款、工具类 26 款、生活服务类 19 款、聊天社交类 18 款、购物类 17 款、音乐视频类 15 款、旅行交通类 13 款、拍照摄影类 8 款、教育类 7 款、医疗健康类 7 款、办公类 6 款、新闻阅读类 5 款。

本批 APP 侵害用户权益的典型表现有：一是未在隐私政策等公示文本中逐一列明 APP 所集成第三方 SDK 收集使用个人信息的目的、方式和范围（146 款，占比 72.6%），二是 APP 未通过弹窗告知隐私政策等方式公开收集使用个人信息的规则并征得用户同意前就开始收集个人信息或索取终端相关权限（79 款，占比 39.3%），三是 APP 在用户未使用相关功能或服务时，提前申请开启通讯录、定位、短信、录音、相机等权限（51 款，占比 25.4%），四是未按法律规定提供账号注销、删除、更正个人信息功能或未公布相关投诉举报方式（49 款，占比 24.4%）；数据安全隐患问题主要

有 Janus 签名机制漏洞、未移除有风险的 Webview 系统隐藏接口漏洞、界面劫持安全、密钥硬编码漏洞、Java 代码反编译风险等。

被查处关停的 8 款违法有害 APP，“汇聊”“汇乎”“汇魂”“汇查查”4 款 APP 经外汇管理部门认定为非法宣传、引导或开展外汇按金交易，“富游网”APP 经财政部门认定为非法利用互联网销售彩票并涉嫌从事网络赌博活动，“依依直播”“柠檬”“火山阅读”3 款 APP 经网信部门认定为传播淫秽色情、暴恐血腥等违法违规信息。

广东省通信管理局后续将持续加大力度，对问题突出、整改不彻底的 APP 及运营企业，坚决采取下架、停接入、停域名、行政处罚以及纳入电信业务经营不良名单或失信名单并公开曝光等措施，依法严厉处置，切实维护 APP 用户合法权益和网络安全秩序。

附件 1：201 款被广东省通信管理局责令整改的 APP 名单

附件 2：8 款被广东省通信管理局关停的违法 APP 名单

报道九：215 款 APP 被广东省通信管理局责令限期整改（2021 年 1 月）

发布时间：2021 年 2 月 23 日

215 款 APP 被广东省通信管理局责令限期整改（2021 年 1 月）

2021 年 1 月，广东省通信管理局共监测发现 215 款 APP 存在侵害用户权益和安全隐患问题（详见附件 1），并依据《网络安全法》《电信和互联网用户个人信息保护规定》等法律法规对 APP 运营者发出《违法违规 APP 处置通知》，责令限期整改并通知各应用商店督促整改。另外，对于前期已通报 APP 整改进度进行核查复测，发现仍有 7 款 APP 未整改或整改不彻底（详见附件 2），再次公开通报。

本批被责令整改的 215 款侵害用户权益和安全隐患问题 APP 中，游戏类 45 款、工具类 38 款、生活服务类 22 款、购物类 20 款、社交类 19 款，教育类 18 款，旅行交通类 15 款，金融理财类 12 款，健康类 10 款，新闻阅读类 4 款，视音频类 4 款、办公类 5 款、娱乐类 3 款。

本批 APP 侵害用户权益的典型表现有：一是未在隐私政策等公示文本中逐一列明 APP 所集成第三方 SDK 收集使用个人信息的目的、方式和范围（129 款，占比 60%），二是未经用户阅读并同意隐私政策,提前申请获取终端权限（69 款，占比 55.2%），三是 APP 在用户未使用相关功能或服务时，提前申请开启通讯录、定位、短信、录音、相机等权限（49 款，占比 39.2%），四是未提供有效的注销账号功能，且在隐私政策和相关界面上没有注销指引（48 款，占比 21.5%）；数据安全隐患问题主要有 Janus 签名机制漏洞、未移除有风险的 Webview 系统隐藏接口漏洞、界面劫持安全、密钥硬编码漏洞、应用备份风险等。

在 315 消费者权益日即将到来之际，广东省通信管理局将持续加大巡查力度，及时发现并通报侵犯用户权益的 APP，同时加强对已通报 APP 及其运营者关联 APP 进行跟踪复查，如有必要坚决采取下架、停接入、停域名、行政处罚以及纳入电信业务经营不良名单或失信名单并公开曝光等措施，依法严厉处置，切实维护 APP 用户合法权益和网络安全秩序。

附件 1：215 款被广东省通信管理局责令整改 APP 名单

附件 2：7 款前期通报整改未整改或整改不彻底 APP 名单

附录二： APP 监管部分重要依据

依据一：《中华人民共和国网络安全法》（摘录）

……

第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条　个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条　任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条　依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

……

第四十七条　网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条　任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应

当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条　网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条　国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

……

第六十条　违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款:

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

第六十四条　网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

……

依据二：《中华人民共和国民法典》（摘录）

……

第一百一十一条 自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。

……

第一千零三十二条 自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。

隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。

第一千零三十三条 除法律另有规定或者权利人明确同意外，任何组织或者个人不得实施下列行为：

（一）以电话、短信、即时通讯工具、电子邮件、传单等方式侵扰他人的私人生活安宁；

（二）进入、拍摄、窥视他人的住宅、宾馆房间等私密空间；

（三）拍摄、窥视、窃听、公开他人的私密活动；

（四）拍摄、窥视他人身体的私密部位；

（五）处理他人的私密信息；

（六）以其他方式侵害他人的隐私权。

第一千零三十四条 自然人的个人信息受法律保护。

个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。

第一千零三十五条 处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理，并符合下列条件：

（一）征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外；

（二）公开处理信息的规则；

（三）明示处理信息的目的、方式和范围；

（四）不违反法律、行政法规的规定和双方的约定。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等。

第一千零三十六条 处理个人信息，有下列情形之一的，行为人不承担民事责任：

（一）在该自然人或者其监护人同意的范围内合理实施的行为；

（二）合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外；

（三）为维护公共利益或者该自然人合法权益，合理实施的其他行为。

第一千零三十七条 自然人可以依法向信息处理者查阅或者复制其个人信息；发现信息有错误的，有权提出异议并请求及时采取更正等必要措施。

自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除。

第一千零三十八条 信息处理者不得泄露或者篡改其收集、存储的个人信息；未经自然人同意，不得向他人非法提供其个人信息，但是经过加工无法识别特定个人且不能复原的除外。

信息处理者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失；发生或者可能发生个人信息泄露、篡改、丢失的，应当及时采取补救措施，按照规定告知自然人并向有关主管部门报告。

第一千零三十九条　国家机关、承担行政职能的法定机构及其工作人员对于履行职责过程中知悉的自然人的隐私和个人信息，应当予以保密，不得泄露或者向他人非法提供。

……

第一千二百二十六条　医疗机构及其医务人员应当对患者的隐私和个人信息保密。泄露患者的隐私和个人信息，或者未经患者同意公开其病历资料的，应当承担侵权责任。

……

依据三：《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）

为推动移动互联网健康有序发展，构建安全可信的信息通信网络环境，依法维护用户的知情权和选择权，促进大众创业、万众创新，规范移动互联网市场秩序，根据《全国人民代表大会常务委员会关于加强网络信息保护的决定》《中华人民共和国网络安全法》《中华人民共和国电信条例》和《互联网信息服务管理办法》等有关规定，制定本规定。

第一条 工业和信息化部大力推动移动智能终端应用软件发展，鼓励移动智能终端生产企业、互联网信息服务提供者等相关企业积极开发移动智能终端应用软件产品，丰富信息消费内容，引导企业健全相关管理机制。鼓励有关行业协会等依法制定自律性管理制度，共同规范移动智能终端应用软件的预置和分发行为，维护网络安全，加强用户权益保护。

第二条 本规定规范移动智能终端生产企业（以下简称生产企业）的移动智能终端应用软件预置行为，以及互联网信息服务提供者提供的移动智能终端应用软件分发服务。

第三条 工业和信息化部依照本规定对全国范围内移动智能终端应用软件预置与分发服务实施监督管理。省、自治区、直辖市通信管理局（以下统称各地通信主管部门）在

工业和信息化部领导下，按照本规定对本行政区域内的移动智能终端应用软件预置与分发服务实施监督管理。工业和信息化部和各地通信主管部门应进一步完善移动智能终端应用软件预置与分发服务监管制度，强化事中事后管理。

第四条 生产企业和提供移动智能终端应用软件分发服务的互联网信息服务提供者（以下简称互联网信息服务提供者）不得提供或传播含有下列内容的移动智能终端应用软件：

（一）反对宪法所确定的基本原则的；

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（三）损害国家荣誉和利益的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）破坏国家宗教政策，宣扬邪教和封建迷信的；

（六）散布谣言，扰乱社会秩序，破坏社会稳定的；

（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

（八）侮辱或者诽谤他人，侵害他人合法权益的；

（九）含有法律、行政法规禁止的其他内容的。

第五条 生产企业和互联网信息服务提供者应依法依规提供移动智能终端应用软件，采取有效措施，维护网络安全，切实保护用户合法权益。

（一）提供移动智能终端预置软件（以下简称预置软件）的生产企业和互联网信息服务提供者应自觉维护行业公平竞争，依法维护用户的知情权和选择权，不得实施破坏市场竞争秩序、侵犯用户合法权益的行为。

（二）生产企业和互联网信息服务提供者所提供移动智能终端应用软件不得调用与所提供服务无关的终端功能、违法发送商业性电子信息；未经明示且经用户同意，不得实施收集使用用户个人信息、开启应用软件、捆绑推广其他应用软件等侵害用户合法权益或危害网络安全的行为。

（三）为移动智能终端应用软件提供代收费的企业，应当采取必要措施，加强对计费、收费行为的管理，杜绝不明扣费；收费企业应对用户确认信息和计费原始数据至少保存 5 个月，并为用户查询提供方便。

（四）生产企业应约束销售渠道，未经用户同意不得擅自在移动智能终端中安装应用软件，并提示用户终端在销售渠道等环节被装入应用软件的可能性、风险和应对措施。

第六条 生产企业和互联网信息服务提供者均应明示所提供移动智能终端应用软件相关信息。

（一）生产企业和互联网信息服务提供者均应通过用户提示、企业网站等方式明示所提供移动智能终端应用软件的信息，包括名称、功能描述、卸载方法、开发者信息、软件安装及运行所需权限列表等，明确告知用户应用软件收集、使用用户个人信息的内容、目的、方式和范围等。

（二）生产企业应在终端产品说明书中提供预置软件列表信息，并在终端产品说明书或外包装中标示预置软件详细信息的查询方法。生产企业在提交移动智能终端进网申请时，应提供相关产品符合前述要求的声明。

（三）涉及收费的移动智能终端应用软件应严格遵守明码标价等相关规定，明示收费标准、收费方式，明示内容真实准确、醒目规范，经用户确认后方可扣费。

第七条 生产企业和互联网信息服务提供者应确保除基本功能软件外的移动智能终端应用软件可卸载。

（一）移动智能终端的基本功能软件是指保障移动智能终端硬件和操作系统正常运行的应用软件，主要包括操作系统基本组件、保证智能终端硬件正常运行的应用、基本通信应用、应用软件下载通道等。终端中预置的实现同一功能的基本功能软件，至多有一个可设置为不可卸载。

（二）生产企业和互联网信息服务提供者应确保所提供的除基本功能软件之外的移动智能终端应用软件可由用户

方便卸载，且在不影响移动智能终端安全使用的情况下，附属于该软件的资源文件、配置文件和用户数据文件等也应能够被方便卸载。

（三）生产企业应确保已被卸载的预置软件在移动智能终端操作系统升级时不被强行恢复；应保证移动智能终端获得进网许可证前后预置软件的一致性；移动智能终端新增预置软件或有重大功能变化的，应及时向工业和信息化部报告。

第八条 从事应用商店等移动应用分发平台服务的互联网信息服务提供者，以及在移动智能终端中预置了移动应用分发平台的生产企业对所提供的应用软件负有以下管理责任：

（一）应登记应用软件提供者、运营者、开发者的真实身份、联系方式等信息。

（二）应建立应用软件管理机制，对应用软件进行审核及安全、服务等相关检测，对审核和检测中发现的恶意应用软件等违法违规软件，不得向用户提供；对所提供应用软件进行跟踪监测，及时处理违法违规软件，建立完善用户举报投诉处置措施等。

（三）应要求应用软件提供者在提交应用软件时声明其获取的用户终端权限及用途，并将上述信息向软件下载用户明示。

（四）应留存所提供应用软件，以及该软件有关版本、上线时间、功能简介、用途、MD5（消息摘要算法 5）等校验值、服务器接入等信息以备追溯检测，相关信息的留存时间不短于 60 日。

（五）对于违反本规定第四条要求的应用软件，以及在通信主管部门监督检查中发现的恶意应用软件，相关企业应予以及时下架。

（六）应加强网络安全防护以及对相关人员的教育培训，保障自身系统安全和用户个人信息安全。

第九条 通信主管部门应对生产企业和互联网信息服务提供者落实本规定相关要求情况进行监督检查。

（一）通信主管部门应组织专业检测机构对生产企业预置的和互联网信息服务提供者提供的应用软件开展监督检测和恶意应用软件认定工作，相关企业应给予配合，并提供便捷的获取应用软件的条件。

（二）检测机构应及时将检测和认定报告提交通信主管部门。通信主管部门依据报告，要求并监督相关企业进行整改,通知并监督互联网信息服务提供者下架恶意应用软件。

（三）通信主管部门向社会通报监督检查和检测情况。

（四）对于紧急情况以及互联网信息服务提供者未按要求及时下架违法应用软件的，通信主管部门可依法依规要求有关单位采取处置措施。

第十条 相关企业和社会组织应进一步完善服务保障措施，提高用户权益保护水平。

（一）生产企业和互联网信息服务提供者应建立移动智能终端应用软件投诉举报受理制度，为用户提供便捷的投诉举报方式，接受、验证和处理用户投诉举报。如用户发现移动智能终端应用软件违反本规定要求，可向相关企业投诉举报，企业应在规定和公开承诺的时限内妥善处理；对处理结果不满的，用户可向电信用户申诉受理机构申诉。用户发现恶意应用软件，以及含有法律法规规定的禁止性内容或违法发送商业性电子信息的移动终端应用软件，可向网络不良与垃圾信息举报中心举报。

（二）工业和信息化部鼓励移动智能终端应用软件采用依法设立的电子认证服务机构颁发的数字证书进行签名；指导相关企业对已签名的移动智能终端应用软件采用依法设立的电子认证服务机构颁发的数字证书，进行验证并显著标识。

（三）工业和信息化部支持相关社会组织通过行业自律形式，建立恶意应用软件黑名单，实现黑名单信息在相关企业、专业检测机构以及用户之间的共享。

第十一条 违反本规定的，通信主管部门依据职权责令改正，依法进行处罚，并将生产企业、互联网信息服务提供者违反本规定受到行政处罚的情况记入信誉档案，向社会公布。对涉嫌违法犯罪的应用软件线索，各单位应及时报告公安机关。

第十二条 本规定下列用语的含义是：

移动智能终端是指接入公众移动通信网络、具有操作系统、可由用户自行安装和卸载应用软件的移动通信终端产品。

移动智能终端应用软件（英文简称 APP）包括移动智能终端预置应用软件，以及互联网信息服务提供者提供的可以通过网站、应用商店等移动应用分发平台下载、安装、升级的应用软件。

移动应用分发平台是指网站、应用商店等提供移动智能终端应用软件下载、安装、升级的应用软件平台。

移动智能终端预置应用软件是指由生产企业自行或与互联网信息服务提供者合作在移动智能终端出厂前安装的应用软件。

恶意应用软件是指含有信息窃取、恶意扣费、诱骗欺诈、系统破坏等恶意行为及其他危害用户权益和网络安全的应用软件。

商业性电子信息是指利用电信网或互联网，向用户介绍、推销商品、服务或者商业投资机会的电子信息。

第十三条 本规定解释权属于工业和信息化部。

6. **第十四条** 本规定自 2017 年 7 月 1 日起实施。

依据四：《公共互联网网络安全威胁监测与处置办法》（工信部网安〔2017〕202 号）

第一条 为加强和规范公共互联网网络安全威胁监测与处置工作，消除安全隐患，制止攻击行为，避免危害发生，降低安全风险，维护网络秩序和公共利益，保护公民、法人和其他组织的合法权益，根据《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《中华人民共和国电信条例》等有关法律法规和工业和信息化部职责，制定本办法。

第二条 本办法所称公共互联网网络安全威胁是指公共互联网上存在或传播的、可能或已经对公众造成危害的网络资源、恶意程序、安全隐患或安全事件，包括：

（一）被用于实施网络攻击的恶意 IP 地址、恶意域名、恶意 URL、恶意电子信息，包括木马和僵尸网络控制端，钓鱼网站，钓鱼电子邮件、短信/彩信、即时通信等；

（二）被用于实施网络攻击的恶意程序，包括木马、病毒、僵尸程序、移动恶意程序等；

（三）网络服务和产品中存在的安全隐患，包括硬件漏洞、代码漏洞、业务逻辑漏洞、弱口令、后门等；

（四）网络服务和产品已被非法入侵、非法控制的网络

安全事件，包括主机受控、数据泄露、网页篡改等；

（五）其他威胁网络安全或存在安全隐患的情形。

第三条 工业和信息化部负责组织开展全国公共互联网网络安全威胁监测与处置工作。各省、自治区、直辖市通信管理局负责组织开展本行政区域内公共互联网网络安全威胁监测与处置工作。工业和信息化部和各省、自治区、直辖市通信管理局以下统称为电信主管部门。

第四条 网络安全威胁监测与处置工作坚持及时发现、科学认定、有效处置的原则。

第五条 相关专业机构、基础电信企业、网络安全企业、互联网企业、域名注册管理和服务机构等应当加强网络安全威胁监测与处置工作，明确责任部门、责任人和联系人，加强相关技术手段建设，不断提高网络安全威胁监测与处置的及时性、准确性和有效性。

第六条 相关专业机构、基础电信企业、网络安全企业、互联网企业、域名注册管理和服务机构等监测发现网络安全威胁后，属于本单位自身问题的，应当立即进行处置，涉及其他主体的，应当及时将有关信息按照规定的内容要素和格式提交至工业和信息化部和相关省、自治区、直辖市通信管理局。

工业和信息化部建立网络安全威胁信息共享平台，统一汇集、存储、分析、通报、发布网络安全威胁信息；制定相关接口规范，与相关单位网络安全监测平台实现对接。国家计算机网络应急技术处理协调中心负责平台建设和运行维护工作。

第七条 电信主管部门委托国家计算机网络应急技术处理协调中心、中国信息通信研究院等专业机构对相关单位提交的网络安全威胁信息进行认定，并提出处置建议。认定工作应当坚持科学严谨、公平公正、及时高效的原则。电信主管部门对参与认定工作的专业机构和人员加强管理与培训。

第八条 电信主管部门对专业机构的认定和处置意见进行审查后，可以对网络安全威胁采取以下一项或多项处置措施：

（一）通知基础电信企业、互联网企业、域名注册管理和服务机构等，由其对恶意 IP 地址（或宽带接入账号）、恶意域名、恶意 URL、恶意电子邮件账号或恶意手机号码等，采取停止服务或屏蔽等措施。

（二）通知网络服务提供者，由其清除本单位网络、系统或网站中存在的可能传播扩散的恶意程序。

（三）通知存在漏洞、后门或已经被非法入侵、控制、篡改的网络服务和产品的提供者，由其采取整改措施，消除

安全隐患；对涉及党政机关和关键信息基础设施的，同时通报其上级主管单位和网信部门。

（四）其他可以消除、制止或控制网络安全威胁的技术措施。

电信主管部门的处置通知应当通过书面或可验证来源的电子方式等形式送达相关单位，紧急情况下，可先电话通知，后补书面通知。

第九条 基础电信企业、互联网企业、域名注册管理和服务机构等应当为电信主管部门依法查询 IP 地址归属、域名注册等信息提供技术支持和协助，并按照电信主管部门的通知和时限要求采取相应处置措施，反馈处置结果。负责网络安全威胁认定的专业机构应当对相关处置情况进行验证。

第十条 相关组织或个人对按照本办法第八条第（一）款采取的处置措施不服的，有权在 10 个工作日内向做出处置决定的电信主管部门进行申诉。相关电信主管部门接到申诉后应当及时组织核查，并在 30 个工作日内予以答复。

第十一条 鼓励相关单位以行业自律或技术合作、技术服务等形式开展网络安全威胁监测与处置工作，并对处置行为负责，监测与处置结果应当及时报送电信主管部门。

第十二条 基础电信企业、互联网企业、域名注册管理

和服务机构等未按照电信主管部门通知要求采取网络安全威胁处置措施的，由电信主管部门依据《中华人民共和国网络安全法》第五十六条、第五十九条、第六十条、第六十八条等规定进行约谈或给予警告、罚款等行政处罚。

第十三条 造成或可能造成严重社会危害或影响的公共互联网网络安全突发事件的监测与处置工作，按照国家和电信主管部门有关应急预案执行。

第十四条 各省、自治区、直辖市通信管理局可参照本办法制定本行政区域网络安全威胁监测与处置办法实施细则。

第十五条 本办法自 2018 年 1 月 1 日起实施。2009 年 4 月 13 日印发的《木马和僵尸网络监测与处置机制》和 2011 年 12 月 9 日印发的《移动互联网恶意程序监测与处置机制》同时废止。

依据五：《APP 违法违规收集使用个人信息行为认定方法》（国信办秘字〔2019〕191 号）

根据《关于开展 APP 违法违规收集使用个人信息专项治理的公告》，为监督管理部门认定 APP 违法违规收集使用个人信息行为提供参考，为 APP 运营者自查自纠和网民社会监督提供指引，落实《网络安全法》等法律法规，制定本方法。

一、以下行为可被认定为“未公开收集使用规则”

1.在 APP 中没有隐私政策，或者隐私政策中没有收集使用个人信息规则；

2.在 APP 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；

3.隐私政策等收集使用规则难以访问，如进入 APP 主界面后，需多于 4 次点击等操作才能访问到；

4.隐私政策等收集使用规则难以阅读，如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等。

二、以下行为可被认定为“未明示收集使用个人信息的目的、方式和范围”

1.未逐一列出 APP(包括委托的第三方或嵌入的第三方代码、插件)收集使用个人信息的目的、方式、范围等；

2.收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户，适当方式包括更新隐私政策等收集使用规则并提醒用户阅读等；

3.在申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解；

4.有关收集使用规则的内容晦涩难懂、冗长繁琐，用户难以理解，如使用大量专业术语等。

三、以下行为可被认定为“未经用户同意收集使用个人信息”

1.征得用户同意前就开始收集个人信息或打开可收集个人信息的权限；

2.用户明确表示不同意后，仍收集个人信息或打开可收集个人信息的权限，或频繁征求用户同意、干扰用户正常使用；

3.实际收集的个人信息或打开的可收集个人信息权限超出用户授权范围；

4.以默认选择同意隐私政策等非明示方式征求用户同意；

5.未经用户同意更改其设置的可收集个人信息权限状态，如 APP 更新时自动将用户设置的权限恢复到默认状态；

6.利用用户个人信息和算法定向推送信息，未提供非定向推送信息的选项；

7.以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限，如故意欺瞒、掩饰收集使用个人信息的真实目的；

8.未向用户提供撤回同意收集个人信息的途径、方式；

9.违反其所声明的收集使用规则，收集使用个人信息。

四、以下行为可被认定为“违反必要原则，收集与其提供的服务无关的个人信息”

1.收集的个人信息类型或打开的可收集个人信息权限与现有业务功能无关；

2.因用户不同意收集非必要个人信息或打开非必要权限，拒绝提供业务功能；

3.APP 新增业务功能申请收集的个人信息超出用户原有同意范围，若用户不同意，则拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外；

4.收集个人信息的频度等超出业务功能实际需要；

5.仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息；

6.要求用户一次性同意打开多个可收集个人信息的权限，用户不同意则无法使用。

五、以下行为可被认定为“未经同意向他人提供个人信息”

1.既未经用户同意，也未做匿名化处理，APP 客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息；

2.既未经用户同意，也未做匿名化处理，数据传输至 APP 后台服务器后，向第三方提供其收集的个人信息；

3.APP 接入第三方应用，未经用户同意，向第三方应用提供个人信息。

六、以下行为可被认定为“未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”

1.未提供有效的更正、删除个人信息及注销用户账号功能；

2.为更正、删除个人信息或注销用户账号设置不必要或不合理条件；

3.虽提供了更正、删除个人信息及注销用户账号功能，但未及时响应用户相应操作，需人工处理的，未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理；

4.更正、删除个人信息或注销用户账号等用户操作已执行完毕，但 APP 后台并未完成的；

5.未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理的。

依据六：工业和信息化部关于开展 APP 侵害用户权益专项整治工作的通知（工信部信管函〔2019〕337 号）

各省、自治区、直辖市通信管理局，中国信息通信研究院、中国互联网协会，各相关单位：

当前，APP 违规收集个人信息、过度索权、频繁骚扰、侵害用户权益等问题突出，群众反映强烈，社会关注度高。结合 2019 年信息通信行业行风建设暨纠风工作安排，我部决定组织开展 APP 侵害用户权益专项整治行动工作。有关事项通知如下：

一、整治内容

依据《网络安全法》、《电信条例》、《规范互联网信息服务市场秩序若干规定》（工业和信息化部令第 20 号）、《电信和互联网用户个人信息保护规定》（工业和信息化部令第 24 号）和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）等法律法规和规范性文件要求，聚焦人民群众反映强烈和社会高度关注的侵犯用户权益行为，重点对以下四个方面 8 类问题开展规范整治工作。

（一）违规收集用户个人信息方面

1.“私自收集个人信息”。即 APP 未明确告知收集使用个人信息的目的、方式和范围并获得用户同意前，收集用户个人信息。

2.“超范围收集个人信息”。即 APP 收集个人信息，非服务所必需或无合理应用场景，超范围或超频次收集个人信息，如通讯录、位置、身份证、人脸等。

（二）违规使用用户个人信息方面

3.“私自共享给第三方”。即 APP 未经用户同意与其他应用共享、使用用户个人信息，如设备识别信息、商品浏览记录、搜索使用习惯、常用软件应用列表等。

4.“强制用户使用定向推送功能”。即 APP 未向用户告知，或未以显著方式标示，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或精准营销，且未提供关闭该功能的选项。

（三）不合理索取用户权限方面

5.“不给权限不让用”。即 APP 安装和运行时，向用户索取与当前服务场景无关的权限，用户拒绝授权后，应用退出或关闭。

6.“频繁申请权限”。即 APP 在用户明确拒绝权限申请后，频繁申请开启通讯录、定位、短信、录音、相机等与当前服务场景无关的权限，骚扰用户。

7.“过度索取权限”。即 APP 在用户未使用相关功能或服务时，提前申请开启通讯录、定位、短信、录音、相机等权限，或超出其业务功能或服务外，申请通讯录、定位、短信、录音、相机等权限。

（四）为用户账号注销设置障碍方面

8.“账号注销难”。即 APP 未向用户提供账号注销服务，或为注销服务设置不合理的障碍。

二、整治对象

本次专项整治工作主要面向两类对象：一是 APP 服务提供者，主要检查是否存在前述 8 类问题；二是 APP 分发服务提供者，含应用商店和基础电信企业营业厅等承担 APP 分发功能的各类企业，主要检查是否落实《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）等有关要求。

三、工作安排

专项整治工作时间为通知印发之日至 2019 年 12 月 20 日。分三个阶段实施：

（一）企业自查自纠阶段（通知印发之日起至 11 月 10 日）。APP 服务提供者对照前述 8 类问题认真开展自查，发现问题及时整改；APP 分发服务提供者组织对所分发 APP 进行全面检查，对存在问题的违规应用软件予以督促整改，拒不改正的应组织予以下架处理。

（二）监督抽查阶段（2019 年 11 月 11 日至 11 月 30 日）。我部将组织第三方检测机构对 APP 进行技术检测和检查，重点抽测与群众生活密切相关、下载使用量较大的 APP 产品和分发平台。对群众反映强烈、难以接受、认为不合理的 APP，我部将组织电信用户委员会、中国互联网协会以及相关媒体机构开展用户和专家评议。各省、自治区、直辖市通信管理局可根据本地实际情况开展检查工作，并将结果报部（信息通信管理局）。

（三）结果处置阶段（2019 年 12 月 1 日至 12 月 20 日）。我部将对存在问题的 APP 统一进行通报，依法依规予以处理，具体措施包括责令整改、向社会公告、组织 APP 下架、停止 APP 接入服务，以及将受到行政处罚的违规主体纳入电信业务经营不良名单或失信名单等。

四、工作要求

（一）切实提高思想认识。各单位要坚决贯彻落实以人民为中心的发展思想，切实提高政治站位，高度重视本次专项整治工作，精心组织、周密部署，细化整治措施，着力解决群众最关心最直接最现实的利益问题，务求取得实效。

（二）畅通用户投诉渠道。专项整治工作期间，各企业应畅通用户投诉渠道，完善投诉处理服务机制和流程。中国互联网协会应通过互联网信息服务投诉平台（https://ts.isc.org.cn/）或 12321 举报中心接受群众投诉，及时汇总处理用户反映的相关问题。

（三）巩固建立长效机制。APP 用户量大、影响面广、耦合性强，规范管理工作涉及主体多、链条长，需要企业自律、社会监督和政府监管的协同共治。各单位要以此次专项整治工作为契机，不断总结经验、分析原因、举一反三、巩固成效，为后续规范行业管理奠定基础。

特此通知。

（联系电话：010-66011239/68206119）

工业和信息化部

2019 年 10 月 31 日

依据七：工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知

（工信部信管函〔2020〕164 号）

各省、自治区、直辖市通信管理局，中国信息通信研究院、中国互联网协会，各相关单位：

按照 2020 年信息通信行业行风建设暨纠风工作部署，为切实加强用户个人信息保护，为人民群众提供更安全、更健康、更干净的信息环境，我部决定开展纵深推进 APP 侵害用户权益专项整治行动。专项整治时间为通知印发之日至 2020 年 12 月 10 日。具体事项通知如下：

一、整治目标

依据《网络安全法》、《电信条例》、《规范互联网信息服务市场秩序若干规定》（工业和信息化部令第 20 号）、《电信和互联网用户个人信息保护规定》（工业和信息化部令第 24 号）和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）等规定，深入推进技管结合，加强监督检查，督促相关企业强化 APP 个人信息保护，及时整改消除违规收集、使用用户个人信息和骚扰用户、欺骗误导用户、应用分发平台管理责任落实不到位等突出问题，净化 APP 应用空间。2020 年 8 月底前上线运行全

国 APP 技术检测平台管理系统，12 月 10 日前完成覆盖 40 万款主流 APP 检测工作。

二、整治对象

（一）APP 服务提供者，即互联网信息服务提供者提供的可以下载、安装、升级的应用软件,包括快应用和小程序等新应用形态。

（二）软件工具开发包（SDK）提供者，即集成在手机 APP 里的第三方工具集合。

（三）应用分发平台，包括网站、应用商店、APP 等承担下载、安装、升级等分发服务的各类平台。

三、整治任务

（一）APP、SDK 违规处理用户个人信息方面。

1.违规收集个人信息。重点整治 APP、SDK 未告知用户收集个人信息的目的、方式、范围且未经用户同意，私自收集用户个人信息的行为。

2.超范围收集个人信息。重点整治 APP、SDK 非服务所必需或无合理应用场景，特别是在静默状态下或在后台运行时，超范围收集个人信息的行为。

3.违规使用个人信息。重点整治 APP、SDK 未向用户告知且未经用户同意，私自使用个人信息，将用户个人信息用于其提供服务之外的目的，特别是私自向其他应用或服务器发送、共享用户个人信息的行为。

4.强制用户使用定向推送功能。重点整治 APP、SDK 未以显著方式标示且未经用户同意，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或广告精准营销，且未提供关闭该功能选项的行为。

（二）设置障碍、频繁骚扰用户方面。

5.APP 强制、频繁、过度索取权限。重点整治 APP 安装、运行和使用相关功能时，非服务所必需或无合理应用场景下，用户拒绝相关授权申请后，应用自动退出或关闭的行为。重点整治短时长、高频次，在用户明确拒绝权限申请后，频繁弹窗、反复申请与当前服务场景无关权限的行为。重点整治未及时明确告知用户索取权限的目的和用途，提前申请超出其业务功能等权限的行为。

6.APP 频繁自启动和关联启动。重点整治 APP 未向用户告知且未经用户同意，或无合理的使用场景，频繁自启动或关联启动第三方 APP 的行为。

（三）欺骗误导用户方面。

7.欺骗误导用户下载 APP。重点整治通过“偷梁换柱”“移花接木”等方式欺骗误导用户下载 APP，特别是具有分发功能的移动应用程序欺骗误导用户下载非用户所自愿下载 APP 的行为。

8.欺骗误导用户提供个人信息。重点整治非服务所必需或无合理场景，通过积分、奖励、优惠等方式欺骗误导用户提供身份证号码以及个人生物特征信息的行为。

（四）应用分发平台责任落实不到位方面。

9.应用分发平台上的 APP 信息明示不到位。重点整治应用分发平台上未明示 APP 运行所需权限列表及用途，未明示 APP 收集、使用用户个人信息的内容、目的、方式和范围等行为。

10.应用分发平台管理责任落实不到位。重点整治 APP 上架审核不严格、违法违规软件处理不及时和 APP 提供者、运营者、开发者身份信息不真实、联系方式虚假失效等问题。

四、工作要求

（一）开展检测检查。我部将于即日起组织第三方检测机构对 APP、SDK 进行技术检测，对应用分发平台的主体责任落实情况进行监督检查。对第一次检查发现存在问题的企业，

我部将责令 5 个工作日内完成整改，对整改不彻底仍然存在问题的，将采取向社会公告、组织下架、行政处罚以及将受到行政处罚的违规主体纳入电信业务经营不良名单或失信名单等措施；对在 APP 不同版本中反复出现问题的企业，我部将向社会公告，并依法依规开展后续处置工作。

（二）抓好执行落实。各地通信管理局要结合实际开展检查工作，每月 15 日前将违规线索录入全国 APP 技术检测平台管理系统，并按照部工作要求开展相关问题处置。相关企业要及时开展自查自纠，对发现的问题立行立改，举一反三，切实有效保护个人信息。APP 企业要完善用户权益保障制度，加强对所集成 SDK 的管理。应用分发平台要强化平台管理责任，积极配合电信主管部门开展相关监管工作。

（三）推动行业自律。鼓励行业协会组织 APP 开发运营者、应用分发平台、第三方服务提供者、电信设备生产企业、安全厂商等相关单位，制定行业自律公约和技术检测标准，健全第三方评议机制，强化行业规范。

（四）强化手段建设。中国信息通信研究院要大力推进全国 APP 技术检测平台管理系统建设，进一步凝聚产业力量，鼓励有条件的企业积极参与平台建设，提升自动化检测水平和能力。各地通信管理局要尽快接入，用好相关技术手段，

做到关口前移，及时发现解决问题，不断提升行业治理能力和水平。

（五）畅通投诉渠道。专项整治工作期间，各企业应畅通用户投诉渠道，完善投诉处理服务机制和流程。中国互联网协会应通过互联网信息服务投诉平台（https://ts.isc.org.cn/）或 12321 举报中心接受群众投诉，及时汇总处理用户反映的相关问题。

工业和信息化部

2020 年 7 月 22 日

依据八：《 YD/T 2439-2012 移动互联网恶意程序描述格式》

1 范围

本标准规定了移动互联网恶意程序的定义、行为属性、判定及命名格式。

本标准适用于移动互联网恶意程序认定及恶意程序信息数据交换。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

3 术语和定义

下列术语和定义适用于本标准。

3.1 移动互联网恶意程序

在用户不知情或未授权的情况下，在移动终端系统中安装、运行以达到不正当目的，或具有违反国家相关法律

法规行为的可执行文件、程序模块或程序片段。

3.2 移动互联网恶意程序样本

存放移动互联网恶意程序的文件实体，可以是独立的恶意程序载体文件、被感染型恶意程序感染后的文件，也可以是非文件载体恶意程序的文件镜像（包括但不限于引导型恶意程序的文件镜像、内存恶意程序的文件镜像）。

3.3 移动互联网恶意程序主体

能够完成恶意程序行为的全部可执行文件及其必要的关联文件（包括但不限于库文件、配置文件等）的集合。

3.4 移动互联网恶意程序安装包

包含移动互联网恶意程序主体的安装载体，可以在相应版本的移动终端系统中安装运行。

4 移动互联网恶意程序行为属性及判定

4.1 用户不知情或未授权情况

本文所述“用户不知情或未授权的情况”包括但不限于以下情况：

——未向用户明确提示所要执行的全部功能及可能产生的资费，并请用户做出选择的；

——用户选择“否”、“不同意”、“取消”、“不允许”、“卸载”

等选项的；

——用户选择“是”、“同意”、“确认”、“允许”、“安装”等选项，但并未对其隐藏的行为明确知情或授权的；

——通过捆绑、诱骗等手段致使用户点击“是”、“同意”、“确认”、“允许”、“安装”等按钮的。

4.2 移动互联网恶意程序行为属性分类

4.2.1恶意扣费

在用户不知情或未授权的情况下，通过隐蔽执行、欺骗用户点击等手段，订购各类收费业务或使用移动终端支付，导致用户经济损失的，具有恶意扣费属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有恶意扣费属性：

——在用户不知情或未授权的情况下，自动订购移动增值业务的；

——在用户不知情或未授权的情况下，自动利用移动终端支付功能进行消费的；

——在用户不知情或未授权的情况下，自动拨打收费声讯电话的；

——在用户不知情或未授权的情况下，自动订购其它

收费业务的；

——在用户不知情或未授权的情况下，自动通过其它方式扣除用户资费的。

4.2.2信息窃取

在用户不知情或未授权的情况下，获取涉及用户个人信息、工作信息或其它非公开信息的，具有信息窃取属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有信息窃取属性：

——在用户不知情或未授权的情况下，获取短信内容的；

——在用户不知情或未授权的情况下，获取彩信内容的；

——在用户不知情或未授权的情况下，获取邮件内容的；

——在用户不知情或未授权的情况下，获取通讯录内容的；

——在用户不知情或未授权的情况下，获取通话记录的；

——在用户不知情或未授权的情况下，获取通话内容的；

——在用户不知情或未授权的情况下，获取地理位置信息的；

——在用户不知情或未授权的情况下，获取本机手机号码的；

——在用户不知情或未授权的情况下，获取本机已安装软件信息的；

——在用户不知情或未授权的情况下，获取本机运行进程信息的；

——在用户不知情或未授权的情况下，获取用户各类帐号信息的；

——在用户不知情或未授权的情况下，获取用户各类密码信息的；

——在用户不知情或未授权的情况下，获取用户文件内容的；

——在用户不知情或未授权的情况下，记录分析用户行为的；

——在用户不知情或未授权的情况下，获取用户网络交易信息的；

——在用户不知情或未授权的情况下，获取用户收藏夹信息的；

——在用户不知情或未授权的情况下，获取用户联网信息的；

——在用户不知情或未授权的情况下，获取用户下载信息的；

——在用户不知情或未授权的情况下，利用移动终端麦克风、摄像头等设备获取音频、视频、图片信息的；

——在用户不知情或未授权的情况下，获取用户其它个人信息的；

——在用户不知情或未授权的情况下，获取用户其它工作信

息的；

——在用户不知情或未授权的情况下，获取其它非公开信息的。

4.2.3远程控制

在用户不知情或未授权的情况下，能够接受远程控制端指令并进行相关操作的，具有远程控制属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有远程控制属性：

——由控制端主动发出指令进行远程控制的；

——由受控端主动向控制端请求指令的。

4.2.4恶意传播

自动通过复制、感染、投递、下载等方式将自身、自身的衍生物或其它恶意程序进行扩散的行为， 具有恶意传播属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有恶意传播属性：

——自动发送包含恶意程序链接的短信、彩信、邮件、WAP 信息等；

——自动发送包含恶意程序的彩信、邮件等；

——自动利用蓝牙通讯技术向其它设备发送恶意程序的；

——自动利用红外通讯技术向其它设备发送恶意程序的；

——自动利用无线网络技术向其它设备发送恶意程序的；

——自动向存储卡等移动存储设备上复制恶意程序的；

——自动下载恶意程序的；

——自动感染其它文件的。

4.2.5资费消耗

在用户不知情或未授权的情况下，通过自动拨打电话、发送短信、彩信、邮件、频繁连接网络等方式，导致用户资费损失的，具有资费消耗属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有资费消耗属性：

——在用户不知情或未授权的情况下，自动拨打电话的；

——在用户不知情或未授权的情况下，自动发送短信的；

——在用户不知情或未授权的情况下，自动发送彩信的；

——在用户不知情或未授权的情况下，自动发送邮件的；

——在用户不知情或未授权的情况下，频繁连接网络，产生异常数据流量的。

4.2.6系统破坏

通过感染、劫持、篡改、删除、终止进程等手段导致移动终端或其它非恶意软件部分或全部功能、用户文件等无法正常使用的，干扰、破坏、阻断移动通信网络、网络服务或其它合法业务正常运行的， 具有系统破坏属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有系统破坏属性：

——导致移动终端硬件无法正常工作的；

——导致移动终端操作系统无法正常运行的；

——导致移动终端其它非恶意软件无法正常运行的；

——导致移动终端网络通讯功能无法正常使用的；

——导致移动终端电池电量非正常消耗的；

——导致移动终端发射功率异常的；

——导致运营商通信网络无法正常工作的；

——导致其它合法业务无法正常运行的；

——对用户文件、系统文件或其它非恶意软件进行感染、劫持、篡改的；

——在用户不知情或未授权的情况下，对系统文件或其它非

恶意软件进行删除、卸载、终止进程或限制运行的；

——在用户不知情或未授权的情况下，对用户文件进行删除的。

4.2.7诱骗欺诈

通过伪造、篡改、劫持短信、彩信、邮件、通讯录、通话记录、收藏夹、桌面等方式，诱骗用户， 而达到不正当目的的，具有诱骗欺诈属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有诱骗欺诈属性：

——伪造、篡改、劫持短信，以诱骗用户，而达到不正当目的的；

——伪造、篡改、劫持彩信，以诱骗用户，而达到不正当目的的；

——伪造、篡改、劫持邮件，以诱骗用户，而达到不正当目的的；

——伪造、篡改通讯录，以诱骗用户，而达到不正当目的的；

——伪造、篡改收藏夹，以诱骗用户，而达到不正当目的的；

——伪造、篡改通讯记录，以诱骗用户，而达到不正当目的的；

——伪造、篡改、劫持用户文件，以诱骗用户，而达到不正当目的的。

——伪造、篡改、劫持用户网络交易数据，以诱骗用户，而达到不正当目的的；

——冒充国家机关、金融机构、移动终端厂商、运营商或其它机构和个人，以诱骗用户，而达到不正当目的的；

——伪造事实，诱骗用户退出、关闭、卸载、禁用或限制使用其它合法产品或退订服务的。

4.2.8流氓行为

执行对系统没有直接损害，也不对用户个人信息、资费造成侵害的其它恶意行为具有流氓行为属性。包括但不限于具有以下任意一种行为的移动互联网恶意程序具有流氓行为属性：

——在用户不知情或未授权的情况下，长期驻留系统内存的；

——在用户不知情或未授权的情况下，长期占用移动终端中央处理器计算资源的；

——在用户不知情或未授权的情况下，自动捆绑安装的；

——在用户不知情或未授权的情况下，自动添加、修改、删除收藏夹、快捷方式的；

——在用户未授权的情况下，弹出广告窗口的；

——导致用户无法正常退出程序的；

——导致用户无法正常卸载、删除程序的；

——在用户未授权的情况下，执行其它操作的。

4.3 移动互联网恶意程序判定

当一个可运行于移动终端上的程序具有4.2节所述一种或多种行为属性时，可判定为移动互联网恶意程序。

5 移动互联网恶意程序命名格式

5.1 移动互联网恶意程序命名格式

移动互联网恶意程序采用分段式格式命名，前四段为必选项，使用英文（不区分大小写）或数字标识；第五段起为扩展字段，扩展字段为可选项，内容使用中括号“[]”标识，可使用任何Unicode字符， 扩展字段可增加多个。命名格式如下：

受影响操作系统编码.恶意程序属性主分类编码.恶意程序名称.变种名称. [扩展字段]

如：

——s.remote.dumusicplay.b.[毒媒]

——a.remote.adrd.a.[红透透]

——s.remote.dumusicplay.f.[毒媒].[已升级]

——w.privacy.mobilespy.c

——i.spread.ikee.a

——b.privacy.txsbbspy.a

——p.remote.vapor.a

——j.payment.swapi.e

5.2 受影响操作系统编码

受影响操作系统及编码包括但不限于以下类型：

——a：Android

——b：Black Berry

——bd：Bada

——i：IPhone IOS

——j：J2ME(Java 2 Micro Edition)

——m：MTK

——p：Palm OS

——s：Symbian

——w：Windows Mobile\WinCE\Windows Phone

——o：其它类型的平台

5.3 恶意程序属性主分类编码

本标准将移动互联网恶意程序属性按危害程度及包含关系排序，如某恶意程序具有多个属性，则以排序靠前的属性作为主分类，以便于对其进行描述，方便公众识别。

移动互联网恶意程序属性主分类编码及排序如表1所示：

表格 1 主分类编码

排序	编码	属性主分类
1	payment	恶意扣费
2	privacy	信息窃取
3	remote	远程控制
4	spread	恶意传播
5	expense	资费消耗
6	system	系统破坏
7	fraud	诱骗欺诈
8	rogue	流氓行为

5.4 恶意程序名称

移动互联网恶意程序主体功能不相同的，可命名为不同名称。移动互联网恶意程序名称可使用解开安装包或压缩格式后的恶意程序主程序的可执行文件名、主要进程的名称或特征字符串命名，亦可使用主程序体中第一个可用的ASCII码串命名。原则上应遵循使用第一个公开报告的名称。

恶意程序的中文名称可参见5.6节，置于扩展字段内。

5.5 变种名称

移动互联网恶意程序主体功能相同，但配置不同的，则认为是同一家族的恶意程序，这时需要用变种名称来区分。变种名称根据样本发现顺序采用英文字母依次命名。第一个发现的样本命名为a，第二个命名为b，第27个发现的样本命名为aa，第28个命名为ab，以此类推。

移动互联网恶意程序主体功能相同，配置也相同，但HASH值不完全相同，则认为是不同HASH值的同一恶意程序的同一变种，其名称及变种名称均应完全相同。

5.6 扩展字段

扩展字段主要用于补充标识前四段必选项无法标示的其它重要信息，如中文通用名称等。

扩展字段中的通用中文名称可使用安装包的中文名称、可执行文件运行界面的中文名称、进程连接的网站名称等。原则上应遵循使用第一个公开报告的名称。