https://www.qianxin.com

奇安信

BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

App违规收集
个人信息风险分析报告

（2022年第一季度）

THE REPORT

发布机构：

奇安信病毒响应中心

主要观点

- ✧ App 违规收集个人信息的现象仍然十分普遍，平均每 5 个 App 中，就有一个存在违规收集个人信息的风险。其中，“无提示收集个人信息”和“高频次收集个人信息”问题最为显著，也是本次报告关注的重点问题。个别 App 平均约每 0.7 秒就会无提示收集一次用户个人信息，可谓是对用户个人信息的“不间断”的收集。
- ✧ 部分存在违规收集个人信息风险的 App 社会影响面巨大，仅下载量排名靠前的 24 款 App 就至少影响国内超过 2 亿用户。网上购物、生活休闲、办公商务等常用 App 的违规风险问题最为突出。
- ✧ 八成以上的违规个人信息收集行为，实际上是由于 App 集成了某些不规范的第三方 SDK，或者是没有对第三方 SDK 收集个人信息的行为进行声明造成的。作为软件开发者，在集成第三方 SDK 时，应当遵守相关法律法规，拒绝使用存在违规风险的 SDK，从而努力规避自身的违规风险。

摘　　要

- 21.3%的新增活跃 App 样本存在“无提示收集个人信息”风险，14.7%存在“高频次收集个人信息”风险。平均每 5 个 App 中，就有一个存在违规收集个人信息风险。
- 在本季度检出的所有存在违规风险的 App 中，至少有 1 款下载量超过 1 亿次，4 款下载量超过 1000 万次，19 款下载量超过 100 万次。仅这 24 款 App 就至少影响超过 2 亿用户。
- 存在违规风险最多的是网上购物类 App,，约占所有存在违规风险 App 总数的 20.1%；其次是生活休闲类，占比为 15.6%。办公商务类排名第三，占比 13.6%。
- 在所有存在“无提示收集个人信息”风险的 App 中，87.6%会无提示收集 IMEI 信息，50.6%会无提示收集 MAC 地址，16.7%会无提示收集 IMSI 信息。
- 在所有存在高频次收集个人信息风险的 App 中，每一百秒收集个人信息 2~5 次的 App 约占 44.0%；6~10 次的占比 28.7%,11~20 次的占比 18.8%，大于 20 次的占比 8.5%。个别 App 竟然会在一百秒内对 IMEI 信息收集多达 138 次，相当于平均约每 0.7 秒就收集一次，可谓是对用户个人信息的“不间断”收集。
- 对用户信息进行违规收集的，84.0%属于第三方 SDK 行为，仅有 16.0%属于 App 自身行为。
- 在所有集成了违规收集个人信息 SDK 的 App 中，只集成了 1 款违规 SDK 的 App 占比为 84.4%，集成了 2 款违规 SDK 的 App 占比为 12.7%，另有 2.9%的 App 集成 3 款及以上的违规 SDK。

关键词：App、个人信息、SDK、违规风险

目　　录

研究背景

随着互联网和移动设备的发展，手机已成为人人都拥有的设备，各式各样的 App 更是丰富了人们的生活：从社交到出行、从网购到外卖，从办公到娱乐等，App 已成为大众生活必需品。然而，App 的流行使人们对 App 违规收集个人信息的风险更加担忧。

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，国家工业和信息化部为此发布了一系列的相关法律法规和监管标准通知，并在全国范围内组织开展 App 违法违规收集使用个人信息专项治理工作。

2022 年第一季度，奇安信病毒响应中心共收录全国应用市场新增 App 活跃样本近 30 万个。本报告依据《App 违法违规收集使用个人信息行为认定方法》等内容要求，使用奇安信自研安卓动态引擎 QADE 对新增 APP 样本进行抽样检测，重点评估“无提示收集个人信息”和“高频次收集个人信息”两种最为常见、影响较深的合规性问题。

1） 检测引擎

本次检测采用奇安信完全自主研发安卓动态引擎 QADE（后文统称奇安信 QADE 引擎）。奇安信 QADE 引擎既支持对 App 进行传统恶意检测，同时也支持对 App 违规收集个人信息及索权等合规性问题的检测，是“综合一体化”动态引擎。

2） 检测依据

本次报告主要参考以下相关的国家法律法规作为检测标准依据：

《网络安全法》、《电信和互联网用户个人信息保护规定》、《GB/T 35273-2020 信息安全技术个人信息安全规范》、《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）、《App 违法违规收集使用个人信息行为认定方法》

3） 检测内容

本次报告重点检测了相关 App 在以下两方面的合规性问题：

无提示收集个人信息

无提示收集个人信息是指存在无隐私说明提示或者未点同意隐私协议便开始收集用户个人信息的情况。

无提示收集个人信息，实际上就是在不告知用户，或用户不知情的情况下，秘密收集用户的各种个人信息，从而给用户带来个人信息泄露、个人信息被滥用等网络安全风险。很多 App 为了实现自身不当的商业利益，会选择不告知用户个人信息收集规则，或只告知用户部分个人信息收集规则。

高频次收集个人信息

高频次收集个人信息是指存在高频率（每百秒的收集次数）收集用户个人信息的情况。

高频次收集个人信息，会导致用户个人活动信息被过渡收集，从而危害用户个人信息和隐私安全，同时还会快速消耗用户手机电量和网络流量。

关于什么样的收集频次属于高频次收集，相关法律法规并没有特别明确的具体规定。在本报告中，每百秒内收集个人信息超过 2 次（包含 2 次），即认定为高频次收集。

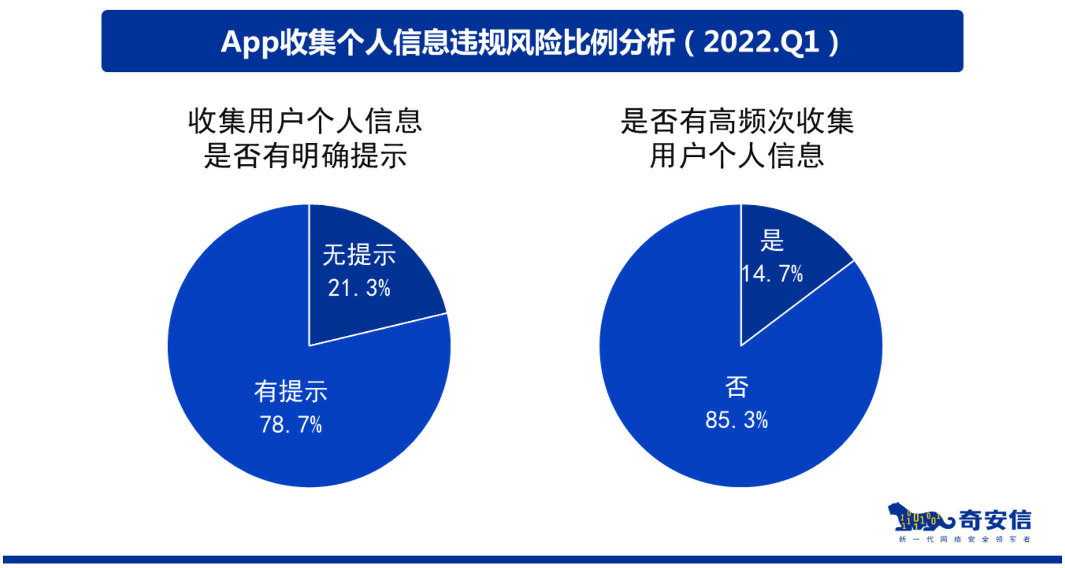
4） 数据范围

本次报告的检测周期为 2022 年 1 月 1 日至 2022 年 3 月 31 日，国内四个应用市场的新收录及更新的 APP 样本共近 30 万个。这四个应用市场分别是：豌豆荚、多多软件站、pc6 应用市场和 2265 应用市场。

第一章　流行 App 违规风险形势分析

一、　存在违规风险的 App 规模

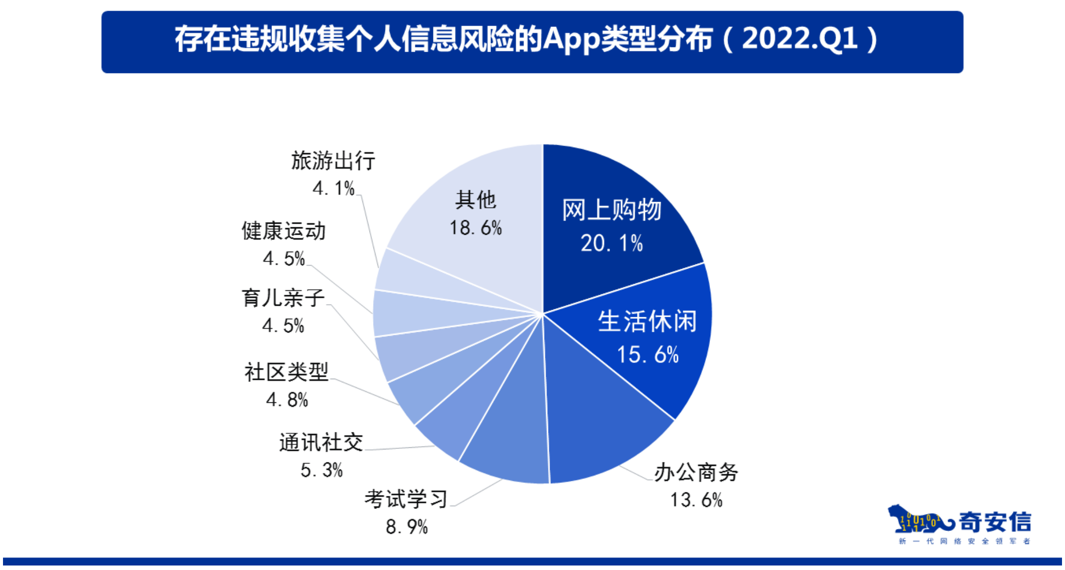
2022 年第一季度，在针对近 30 万个新增活跃 App 样本的抽样检测中，存在“无提示收集个人信息”风险和“高频次收集个人信息”风险的 App，分别占到检测样本总量的 21.3%和 14.7%。总体来看，平均每 5 个 App 中，就会有一个存在个人信息收集方面的违规风险。


App收集个人信息违规风险比例分析（2022.Q1）

本季度检出的所有存在违规风险的 App 中，至少有 1 款下载量超过 1 亿次，4 款下载量超过 1000 万次，19 款下载量超过 100 万次。仅这 24 款 App 就至少影响国内超过 2 亿用户。

二、　存在违规风险的 App 类型

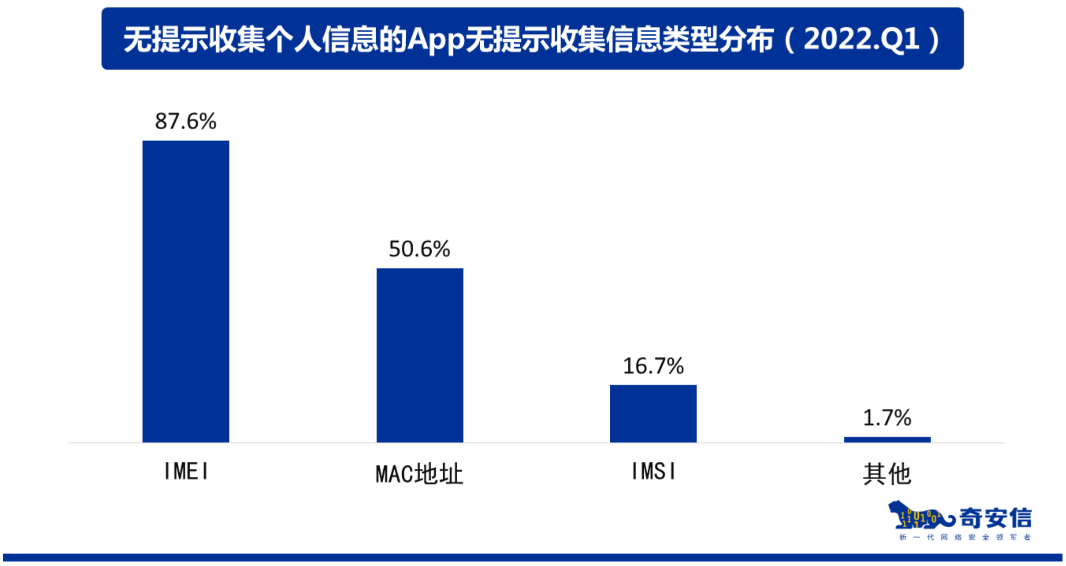
从 App 类型来看，在 2022 年第一季度的检测中，存在违规风险最多的 App 是网上购物类 App,约占所有存在违规风险 App 总数的 20.1%；其次是生活休闲类，占比为 15.6%。办公商务类排名第三，占比 13.6%。


存在违规收集个人信息风险的App类型分布（2022.Q1）

第二章　典型 App 违规风险行为分析

一、　无提示收集个人信息类型分析

检测显示，在所有存在“无提示收集个人信息”风险的 App 中，IMEI、MAC 地址和 IMSI 是 App 静默收集个人信息最主要的三个类型。其中，87.6%会无提示收集 IMEI 信息，50.6%会无提示收集 MAC 地址，16.7%会无提示收集 IMSI 信息，而无提示收集其他个人信息的情况，仅占 1.7%。


无提示收集个人信息的App无提示收集信息类型分布（2022.Q1）

名词解释

IMEI

国际移动设备识别码（英语：IMEI，International Mobile Equipment Identity），是用于在移动电话网络中识别每一部独立的手机等移动通信设备。

MAC 地址

硬件位址（英语：Media Access Control Address），也称为局域网地址、MAC 位址、以太网地址或物理地址，它是一个用来确认网络设备位置的位址。

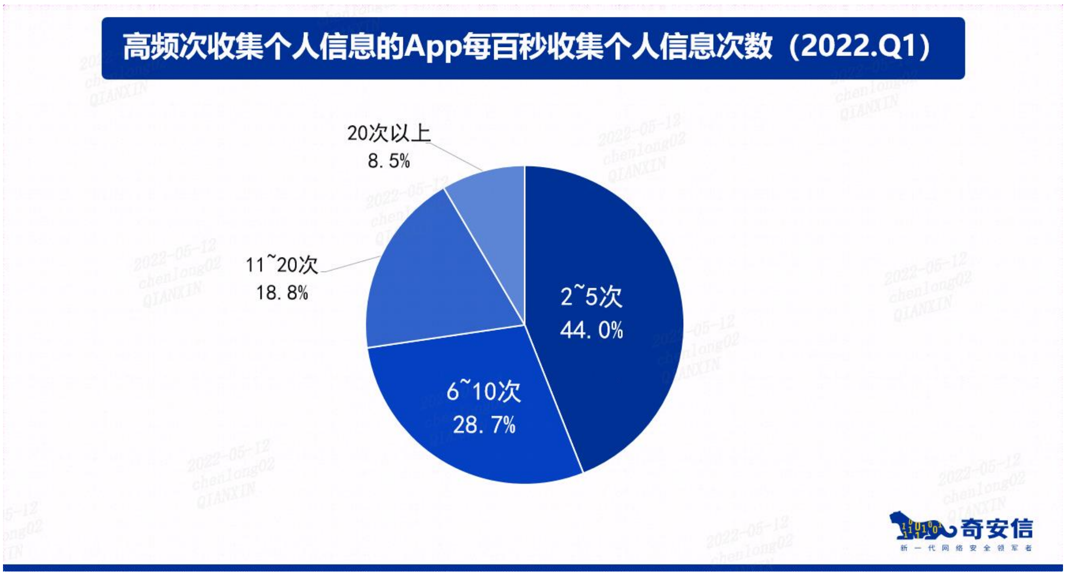
IMSI

国际移动用户识别码（英语：IMSI，International Mobile Subscriber Identity），是用于区分蜂窝网络中不同用户的、在所有蜂窝网络中不重复的识别码。

二、　高频次收集个人信息情况分析

如前所述，在 2022 年第一季度检测的所有新增活跃 App 样本中，一百秒内收集用户个人信息超过 2 次（包含 2 次）的 App 占到了所有被检测 App 总量的 14.7%。在所有存在高频次收集个人信息风险的 App 中，每一百秒收集个人信息次数大于等于 2 次，但低于 5 次的 App 约占 44.0%；6~10 次的占比 28.7%,11~20 次的占比 18.8%，大于 20 次的占比 8.5%。

特别的，我们在本季度的检测中，发现某款收集个人信息最为频繁 App，竟然在一百秒内对 IMEI 信息收集了 138 次，平均每秒 1.38 次，相当于平均约每 0.7 秒就收集一次，可谓是对用户个人信息的“不间断”收集。



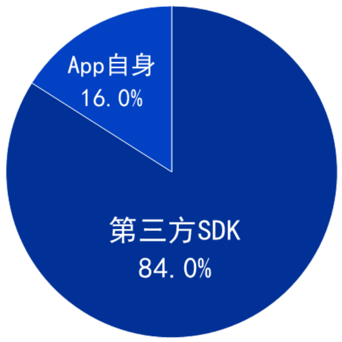
高频次收集个人信息的App每百秒收集个人信息次数（2022.Q1）

第三章　违规个人信息收集者分析

App 对于用户个人信息的收集，未必都是由 App 自身来完成的，很多时候是因为 App 集成了第三方 SDK，而第三方 SDK 存在个人信息收集行为。如果相关 App 在用户协议中，没有告知其集成的第三方 SDK 存在的个人信息收集情况，同样也会构成“无提示收集个人信息”的违规风险。如果第三方 SDK 存在“高频次收集个人信息”的情况，那么相关 App 也会存在同样的违规风险。

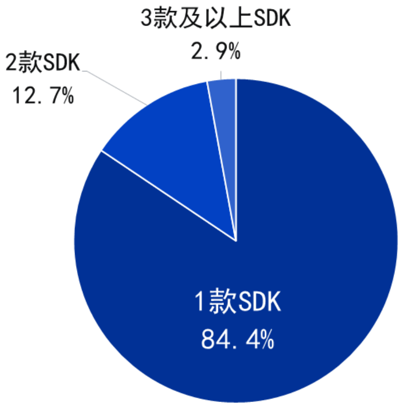
统计显示，在所有存在“无提示收集个人信息”和“高频次收集个人信息”风险的 App 中，对用户信息进行违规收集的，84.0%属于第三方 SDK 行为，仅有 16.0%属于 App 自身行为。也就是说，对第三方 SDK 的不规范使用，以及第三方 SDK 自身的不规范行为，是导致当前部分 App 存在违规收集用户个人信息风险的主要原因。检测还发现，有两款知名的第三方 SDK，分别覆盖了存在违规行为的 App 总量的 29.0%和 21.0%。

违规收集用户个人信息的App中信息收集者身份分析（2022.Q1）



研究还发现，在某些存在违规收集用户个人信息风险的 App 中，集成了不止一款存在违规收集用户信息行为的第三方 SDK。统计显示，在所有集成了违规收集个人信息 SDK 的 App 中，只集成了 1 款违规 SDK 的 App 占比为 84.4%，集成了 2 款违规 SDK 的 App 占比为 12.7%，另有 2.9%的 App 集成 3 款及以上的违规 SDK。

违规收集个人信息App集成违规第三方SDK的数量分布（2022.Q1）



附录 1 奇安信病毒响应中心

奇安信病毒响应中心是奇安信集团旗下的专业病毒鉴定及响应团队。中心以奇安信核心云平台为基础，拥有每日千万级样本检测及处置能力、每日亿级安全数据关联分析能力。结合多年反病毒核心安全技术、运营经验，基于集团自主研发的 QOWL 和 QDE 引擎，形成跨平台木马病毒查杀能力与漏洞修复能力，并且具有强大的大数据分析能力，可以实现全平台安全和防护预警能力。

奇安信病毒响应中心支撑奇安信全线安全产品的病毒检测，积极响应客户侧的安全反馈问题，可第一时间为客户排除疑难杂症。中心曾多次处置重大病毒传播事件，多次参与重大活动安全保障工作，受到客户的高度认可。

附录 2 奇安信病毒响应中心移动安全团队

奇安信病毒响应中心移动安全团队一直致力移动安全领域及 Android 安全生态的研究，不仅可以为奇安信移动安全产品提供常见的移动端病毒木马查杀能力，也可以精准识别时下流行的刷量、诈骗、博彩、违规、色情等黑产类软件，并支持对 App 的合规化安全检测。

团队创新研发的高价值移动端攻击发现流程，已成功捕获到国内外多起针对移动平台的重大攻击事件，并发布了多篇移动黑产报告，披露了多个通过移动平台发起攻击的 APT 组织及其活动。特别的，近两年来，团队首发披露了包括诺崇狮组织 SilencerLion、利刃鹰组织 BladeHawk、艾叶豹组织 SnowLeopard 和金刚象组织 VajraEleph 在内的多个全新的 APT 组织。团队的高级威胁的分析与追踪溯源能力在国内外均处于领先水平。

附录 3 奇安信移动安全产品介绍

奇安信移动终端安全管理系统（天机）是面向公安、司法、政府、金融、运营商、能源、制造等行业客户，具有强终端管控和强终端安全特性的移动终端安全管理产品。产品基于奇安信在海量移动终端上的安全技术积淀与运营经验，从硬件、OS、应用、数据到链路等多层次的安全防护方案，确保企业数据和应用在移动终端的安全性。

奇安信移动态势感知系统是由奇安信集团态势感知团队与奇安信病毒响应中心移动团队合力推出的一个移动态势感知管理产品，主要面向具有监管责任的政企机构客户，着重于监测 App 的下载与使用环节，协助相关监管机构摸清辖区范围内 App 的使用情况，给客户提供 App 违法检测、合规性分析及 App 溯源等功能。