CAICT 中国信通院

移动金融应用安全白皮书(2019年)

中国信息通信研究院
云计算与大数据研究所
安全研究所

2019年10月

版权声明

编委会

编委会成员：何阳、廖璇、陈湉、郑威、许一骏、唐明环、董欣明、曹会宾、吕衍、马聪、姜鼎、张学阳、郑晓玲、王榕、郭训平、程智力、马志民、谢勇、魏超、史博、邱寅峰、龙述兵、张融、李洋、苏云

参与单位：中国信息通信研究院、北京智游网安科技有限公司（爱加密）、北京顶象技术有限公司、信通院安全所&腾讯安全联合实验室—产业互联网安全实验室、大数据协同安全技术国家工程实验室—金融行业安全研究中心

前　言

近年来，以移动互联网技术为代表的新一代信息新技术发展迅猛，智能终端得到了广泛的普及，信息化浪潮蓬勃兴起，移动应用在国内甚至全球诸多产业发展中的重要地位逐渐显现。据 App Annie 发布的《2019 年移动市场报告》数据显示，2018 年全球移动应用下载量 1940 亿，其中我国的移动应用下载量占比将近 50%，是目前全球移动应用下载量最大的国家。

在金融领域，随着移动支付的普及，用户通过智能移动终端进行投融资、借贷、交易支付等活动愈加频繁，大部分的金融机构平台通过移动 App 开展业务，移动金融应用的重要性和价值逐渐凸显。移动金融就是将移动性赋予金融服务业，实现金融服务业务移动化。移动金融包括银行、证券、保险等传统金融服务向移动端的转移，也包括移动互联网借贷、理财等新兴金融服务。移动金融能有效提升运营效率，降低管理成本，为客户提供更加便捷、实时、高效的服务。

然而，移动金融应用在给大众生活带来巨大便利的同时，也带来了巨大的安全挑战。移动端操作系统，特别是安卓操作系统，由于其系统本身的开源性，系统漏洞更容易被发现和利用，增加了 App 本身的脆弱性；部分金融行业 App 开发者安全意识淡薄，防护技术手段落后，开发流程不规范，更新修复不及时等，也增加了移动金融 App 的安全风险；同时，由于移动 App 能够收集到大量精准且有价值的用户信息，导致越来越多的移动金融 App 成为不法分子的攻击目标。据

《全球关键信息基础设施网络安全状况分析报告（2017）》统计，金融行业是国家关键信息基础设施行业中遭受网络攻击最多的行业，移动金融应用的安全问题亟需关注。

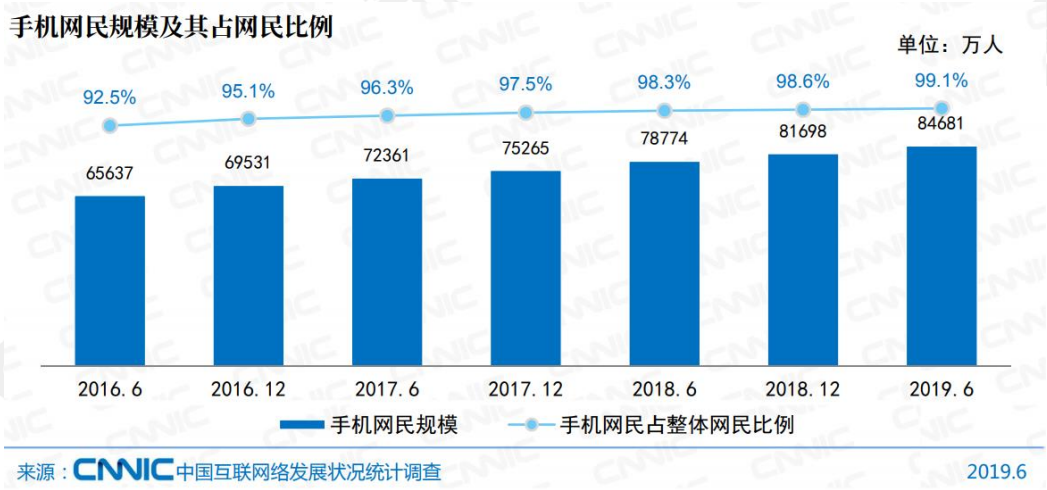
本白皮书聚焦于移动金融应用的安全，详细梳理了移动金融应用安全的政策和技术背景；从地域、应用市场和细分行业三个维度分别介绍了移动金融 App 的分布情况；重点剖析了移动金融 App 面临的高危漏洞、恶意程序、SDK 使用安全、违规索权、缺乏加固五大安全风险；最后，提出了移动金融 App 安全建设的新思路和应对策略，并对移动金融应用安全未来的发展趋势进行了展望。

目 录

一、移动金融应用的安全背景

（一）移动互联网高速发展

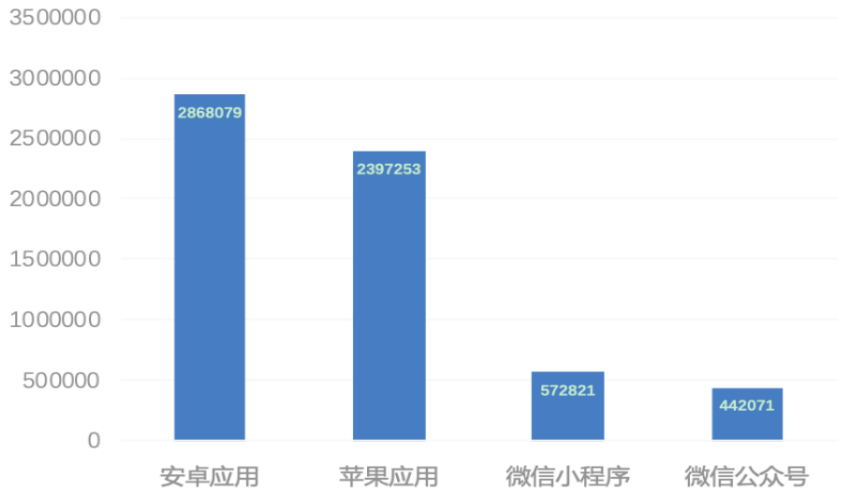
据中国互联网络信息中心（CNNIC）发布的第 44 次《中国互联网络发展状况统计报告》显示，截至 2019 年 6 月，我国网民规模达 8.54 亿，较 2018 年底增长 2598 万，互联网普及率达 61.2%，较 2018 年底提升了 1.6 个百分点；我国手机网民规模达 8.47 亿，较 2018 年底增长 2984 万，网民使用手机上网的比例达 99.1%，较 2018 年底提升了 0.5 个百分点，具体数据如图 1 所示。与五年前相比，移动宽带平均下载速率提升约 6 倍，手机上网流量资费水平降幅超 90%。“提速降费”推动移动互联网流量大幅增长，用户月均使用移动流量达 7.2GB，为全球平均水平的 1.2 倍；移动互联网接入流量消费达 553.9 亿 GB，同比增长 107.3%。以手机为中心的智能设备，成为“万物互联”的基础，车联网、智能家电促进“住行”体验升级，构筑个性化、智能化应用场景。移动互联网服务场景不断丰富、移动终端规模加速提升、移动数据量持续扩大，为移动互联网产业创造更多价值挖掘空间。



数据来源：CNNIC 中国互联网络发展状况统计调查

图 1 手机网民规模及其占网民比例

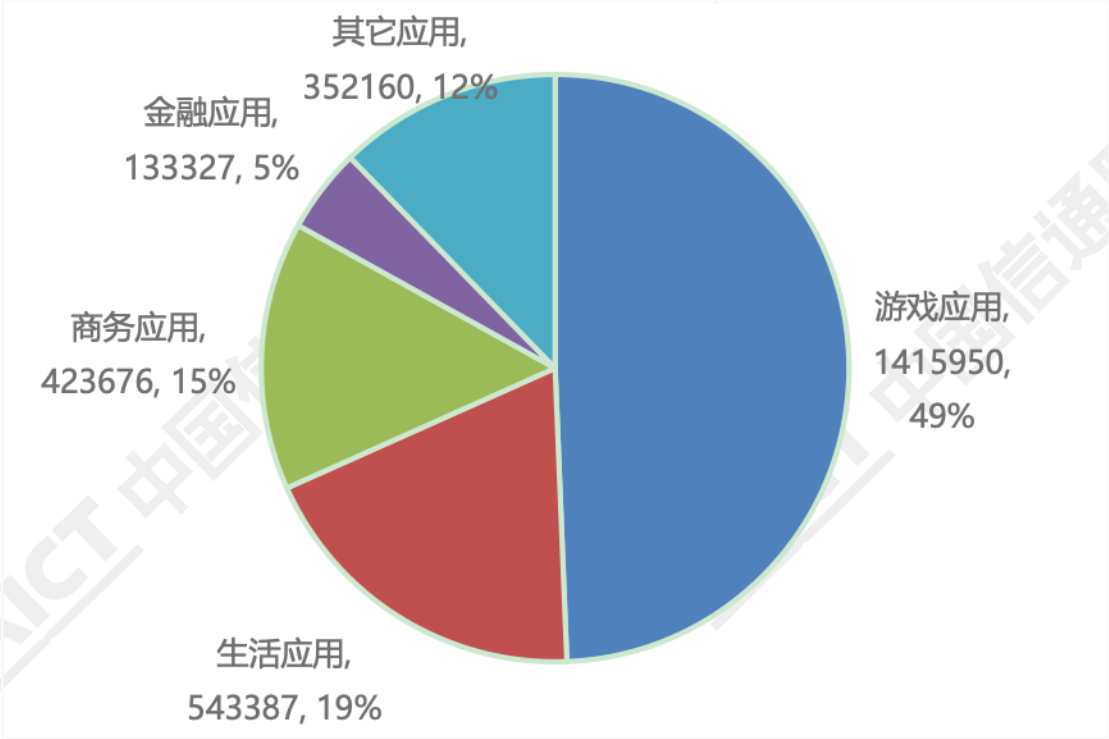
截至 2019 年 10 月，我国本土市场上监测到的移动应用程序（App）在架数量为 525 万款，基于安卓系统的第三方应用商店安卓移动应用数量超过 286 万款，占比为 54.4%，苹果商店（中国区）移动应用数量约 239 万款，微信小程序 57 万款，微信公众号 44 万个。具体数据如图 2 所示。



数据来源：北京智游网安科技有限公司（爱加密）

图 2 中国市场移动 App 数量统计

截至 2019 年 10 月，游戏类应用数量约 141 万款，占比达 50%；生活服务类应用规模达 54.2 万款，排名第二，占比为 19%；电子商务类应用排名第三，规模为 42.1 万款，占比为 15%，金融行业相关移动应用达到 13.3 万款，成为应用市场中极具分量的专项类别。具体数据如图 3 所示。



数据来源：北京智游网安科技有限公司（爱加密）

图 3 中国市场移动应用类型统计

（二）移动应用监管政策日趋严格

1. 金融监管部门发布多项规定保障 App 安全

近年来，金融科技行业安全整体态势稳定，监管框架逐步完善。中国金融科技行业的发展已从单纯的市场开拓阶段进入到了基于安

全风险防范的发展阶段。未来,随着监管框架与安全意识进一步提高，金融科技行业的安全性将进一步提升，整个行业也将实现平稳增长。

2017 年 6 月，中国人民银行印发了《中国金融业信息技术“十三五”发展规划》，确立了“十三五”期间金融业信息技术工作的发展目标，提出将健全网络安全防护体系，增强安全生产和安全管理能力作为重点任务之一，要求不仅要提高金融信息系统安全生产能力，提高金融网络安全管理水平，还要全面推进金融业落实《中华人民共和国网络安全法》（以下简称《网络安全法》）。

2019 年 3 月，《中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》发布，提出健全紧急止付和快速冻结机制，加强账户实名制管理等要求，抑制金融欺诈等犯罪活动的发生。

2019 年 8 月 22 日，中国人民银行印发《金融科技(FinTech)发展规划(2019-2021 年)》（以下简称《规划》），明确提出未来三年金融科技工作的指导思想、基本原则、发展目标、重点任务和保障措施。《规划》在提升金融业务风险防范能力上，明确提出组织建设统一的金融风险监控平台，引导金融机构加强金融领域 App 与门户网站实名制和安全管理，增强网上银行、手机银行、直销银行等业务系统的安全监测防护水平，提升对仿冒 App、钓鱼网站的识别处置能力。

移动金融应用相关法律法规的密集颁布和出台，体现了政府对保

障移动金融 App 网络安全的重视和治理移动金融 App 网络安全的决心，也反映出当前移动金融 App 安全面临着严峻的形势。

2. 等保 2.0 对移动金融应用安全提出新要求

2019 年 5 月 13 日，公安部正式发布《信息安全技术 网络安全等级保护基本要求》等系列国家标准（以下简称“等保 2.0”），标志着“等保 2.0”时代正式到来。等保 2.0 系列国家标准的发布，对加强我国网络安全保障工作，提升网络安全保护能力具有重要意义。

移动互联安全作为网络安全等级保护技术体系的一个重要内容，近年来逐渐成为大众关注的焦点。《网络安全等级保护基本要求——移动互联安全扩展要求》从技术要求和管理要求两个维度对采用移动互联技术的等级保护对象如何进行定级和有效防护进行了明确描述。以一个三级移动互联系统为例，系统既要满足三级的安全通用要求，又要满足三级的移动互联安全扩展要求。移动互联部分通常由移动终端、移动应用和无线网络三部分组成。移动性和便捷性是采用移动互联技术等级保护的企业与传统等级保护企业的最大区别，移动终端可以远程通过运营商基站或公共 Wi-Fi 接入等级保护企业，也可以通过本地无线接入设备接入等级保护企业。与传统信息系统相比，采用移动互联技术的系统将面对更大的攻击面。因此，对移动互联环境主要增加包括“无线接入点的物理位置”、“移动终端管控”、“移动应用管控”、“移动应用软件采购”和“移动应用软件开发”等方面要求。等保 2.0 移

动互联安全扩展要求针对移动终端、移动应用和无线网络部分提出特殊安全要求，与安全通用要求一起构成对采用移动互联技术的等级保护对象的完整安全要求。

《网络安全法》和等保 2.0 系列国家标准的出台，对整体互联网环境、移动金融 App 安全建设工作的稳步推进提供了催化剂。移动金融 App 企业应该切实落实相应的法律法规，从技术和管理两方面着手，打造绿色的网络环境。

3. 移动 App 个人信息安全成监管重点

针对移动 App 安全及个人信息安全问题，国家、行业主管部门等相关单位陆续出台了多项法律法规和标准规范，用于净化移动 App 个人信息安全市场。

《网络安全法》的第 41 条至 43 条明确规定了个人信息和个人隐私保护方面的内容，规定网络运营者收集、使用个人信息时，应当遵循相关的法律法规，并经被收集者同意。

2018 年 5 月 1 日，全国信息安全标准化技术委员会发布《GB/T 35273-2017 信息安全技术个人信息安全规范》，针对个人信息面临的安全问题，规范个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄漏等乱象的发生，最大程度地保障个人的合法权益和社会公共利益。

2019 年 1 月 25 日，中央网信办、工业和信息化部、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》，成立 App 专项治理工作组，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行动。3 月 1 日，App 专项治理工作组发布《App 违法违规收集使用个人信息自评估指南》，对 App 的隐私政策文本、App 收集使用个人信息行为、App 运营者对用户权利的保障等合计 32 个评估点和评估标准作出定义。3 月 15 日，中央网信办、市场监管总局正式对外发布公告，将依据《移动互联网应用程序（App）安全认证实施规则》开展 App 安全认证工作。5 月 5 日，App 专项治理工作组起草了《App 违法违规收集使用个人信息行为认定方法（征求意见稿）》（以下简称《认定方法》），并在其官网和公众号公开，向社会各界公开征求意见，《认定方法》明确界定了 App 收集使用个人信息方面的违法违规行为，为 App 运营者自查自纠提供指引，为 App 评估和处置提供参考。

2019 年 6 月 1 日，全国信息安全标准化技术委员会发布《移动互联网应用基本业务功能必要信息规范》，针对当前移动互联网应用中存在的超范围收集、强制授权、过度索权等个人信息安全问题，结合当前移动互联网技术及应用现状，围绕用户数据量大、社会关注度高的移动互联网应用基本业务功能，给出了保障其正常运行需收集的个人信息的最小范围。

2019 年 7 月 1 日，工业和信息化部印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》，强调为深化 App 违法违规专项治理，将持续推进 App 违法违规采集使用个人信息专项治理行动。

2019 年 8 月 8 日，为落实《网络安全法》对个人信息保护的相关要求的同时，加快相应标准化工作，全国信息安全标准化技术委员会秘书处发布《信息安全技术 移动互联网应用（App）收集个人信息基本规范（草案）》，向社会公开征求意见。

相关法律法规和标准文件的出台，规范了移动应用收集、使用、存储、传输、销毁个人信息数据的各类行为，定义了个人信息安全条款的必要标准和格式以及在第三方使用数据时必要的流程。同时，相关法律法规和标准规范也为监管机构和检测机构等提供了合规检测标准，为相关检测工具定义了检测依据。

（三）5G 时代移动金融应用发展

随着 5G 时代来临，移动互联网将会以全新的形象展现。作为万物互联时代的新型基建底层技术,5G 是连接物联网和人工智能的纽带,其特性将促进物联网向智能网络的过渡,最终实现智能社会。截至目前，中行、工行、浦发银行都已对外宣布推出 5G 网点，5G 网络的高速传输和低延迟性可为金融业务流程带入更多的“实时属性”，如人脸识别的更广泛应用、基于微表情的实时风控、新的支付手段、人机交

互的普及以及远程开户等，都在 5G 环境下都有了更大的想象空间。

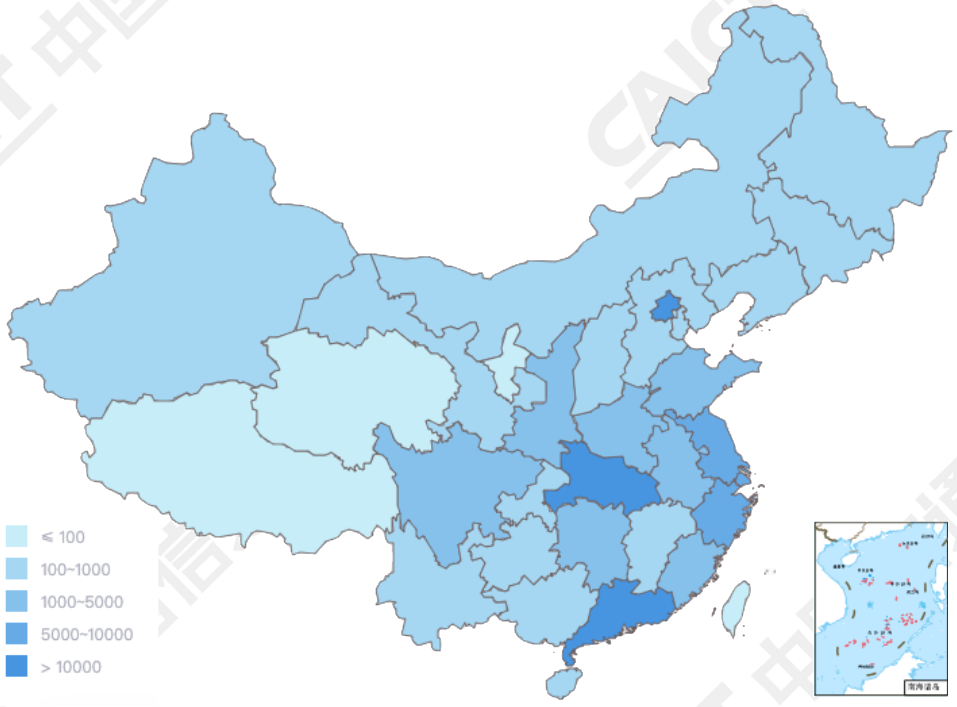
基于 5G 的移动金融应用形式也将变得多样化，不管是原生应用、混合式应用还是 WEB 应用，都会伴随着 5G 技术的成熟，实现更多的创新应用场景，如视频呼叫、定位、交易、查找、上传和下载等。随着更多新型移动应用出现，移动应用安全也将成为金融机构关注的焦点。相比现有相对封闭的移动通信系统，5G 时代接入的用户、设备种类将更加复杂，风险也随之增大，金融机构在运用新技术的同时，需要进一步完善风险管理体系，防范新技术带来的跨界安全风险、操作风险等，如此才能更好地发挥新技术的积极作用。

二、移动金融应用的分布情况

截止 2019 年 9 月 11 日，报告团队已从 232 个安卓应用市场中收录了 133327 款金融行业 App。

（一）移动金融应用的地域分布不均

从观测对象的地域分布来看，有 130022 款可以明确归属省份，全国 34 个省级行政区均有金融行业 App 生成（金融行业 App 地域分布详细数据参见附录 A），平均每个省份生成金融行业 App3824 款。金融行业 App 地域分布不均，广东、湖北和北京分别以 29.60%、21.30%和 12.96%的高占比排名金融行业 App 生成数量前三，而西藏、青海等 6 省份总占比仅有 0.18%。具体数据如图 4 所示。

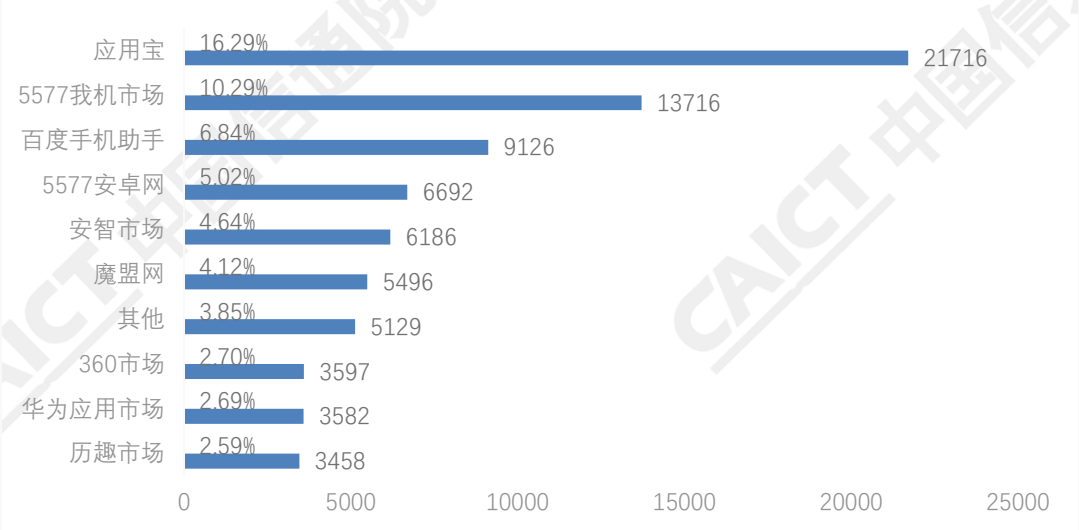


数据来源：北京智游网安科技有限公司（爱加密）

图 4　App 地域分布情况

（二）移动金融应用的应用市场集中度高

从应用市场的分布来看（金融行业 App 分类逻辑及典型应用参见附录 B），本次研究的 App 共来自 232 个应用市场，而 59.03%的 App 集中在应用宝、5577、百度手机助手等排名前十的应用市场，远超其它 222 个应用市场之和。应用宝以 16.29%的高收录占比拔得头筹；5577 我机市场则以 13716 的收录量位居第二，占比 10.29%；百度手机助手排行第三，App 收录量占监测总数的 6.84%。具体数据如图 5 所示。



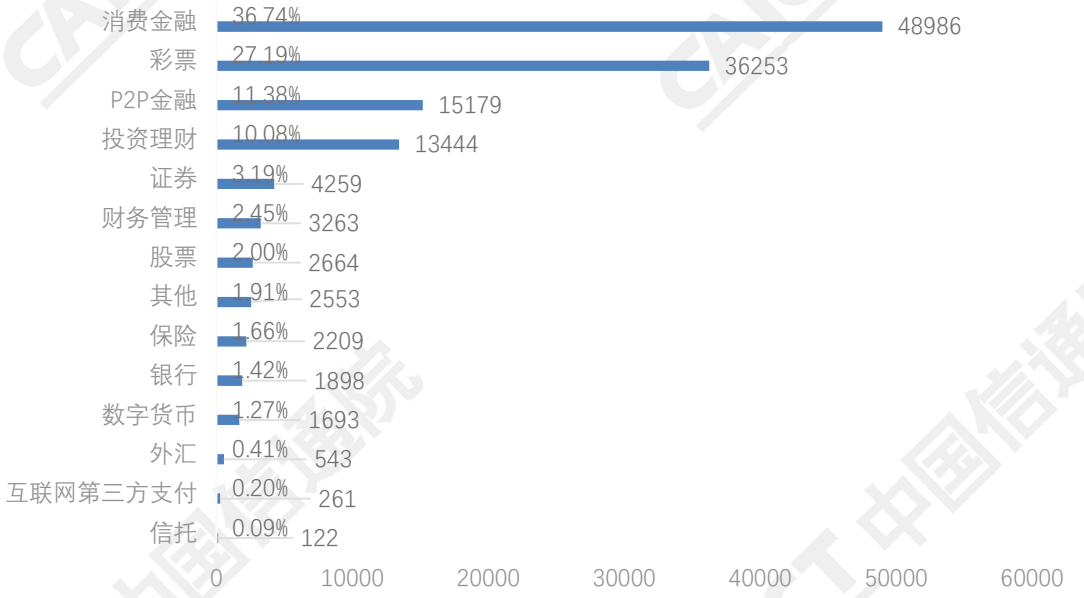
数据来源：北京智游网安科技有限公司（爱加密）

图 5 移动金融应用市场分布统计

（三）借贷领域移动应用持续发展占据半数市场

从金融行业 App 细分领域来看（金融行业 App 分类逻辑及典型应用参见附录 B），借贷类 App 包揽前三名中的两个席位。其中，面向个人用户的消费金融类 App 数量最多，占观测总数的 36.74%；面

向企业的 P2P 金融类 App 排名第三，占观测总数的 11.38%；彩票类 App 排名第二，占观测总数的 27.19%。不同细分领域 App 占比如图 6 所示。



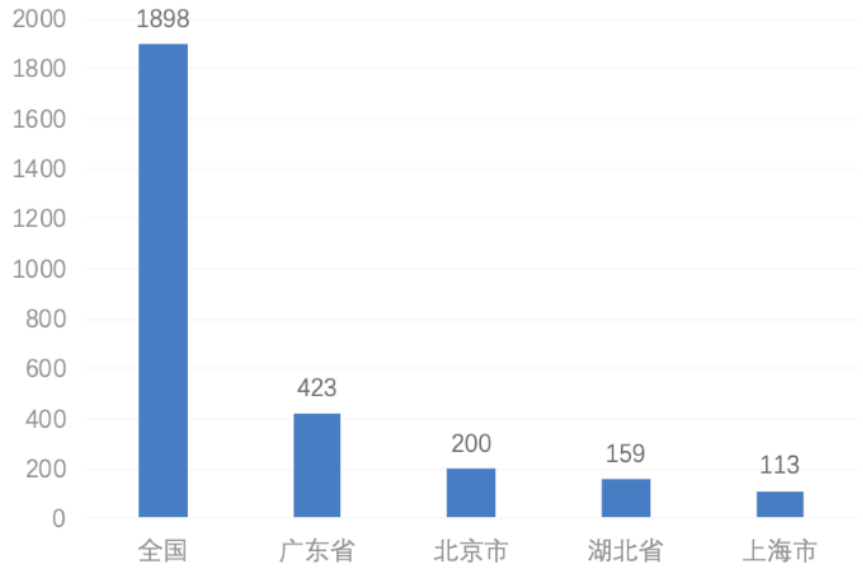
数据来源：北京智游网安科技有限公司（爱加密）

图 6 不同细分领域 App 数量及占比

（四）典型细分行业移动应用分布情况

1．银行类移动应用分布情况

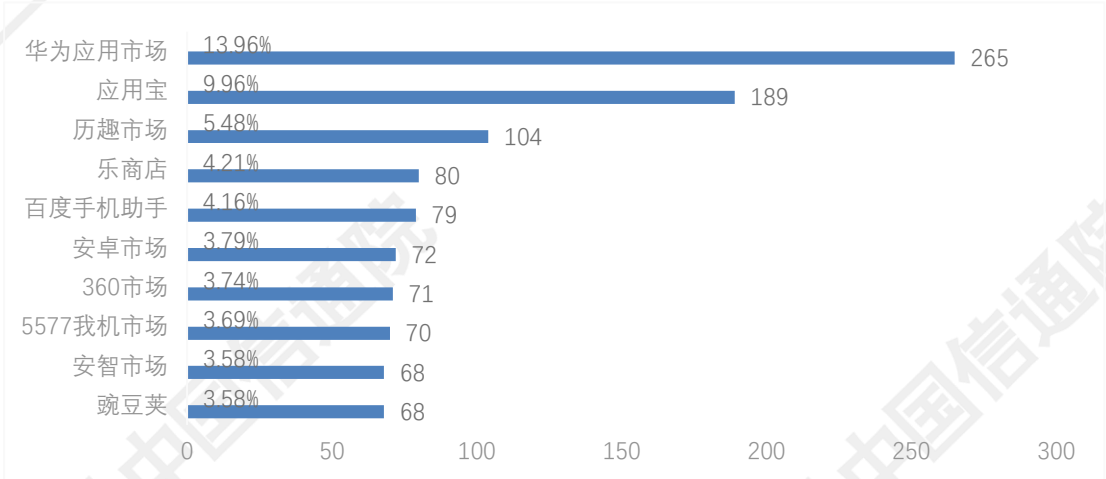
本次收录的银行类 App 共 1898 款，其中，广东省以 423 款排名第一，占全部银行类 App 的 22.29%；北京市则以 10.54%的占比位居第二；排行第三的是湖北省，其 App 数量占监测总数的 8.38%。App 数量较多的省份还有沪鲁闽三地，三者拥有的金融移动 App 数量均超过 100 款。具体数据如图 7 所示。



数据来源：北京智游网安科技有限公司（爱加密）

图 7 银行类移动 App 地域数量统计

银行业 App 收录量排名前十的应用市场中，华为应用市场收录银行类 App 数量最多，占监测总数的 13.96%；其次是应用宝，收录量占监测总数的 9.96%；历趣市场排名第三，收录 5.48%的 App 应用。具体数据如图 8 所示。

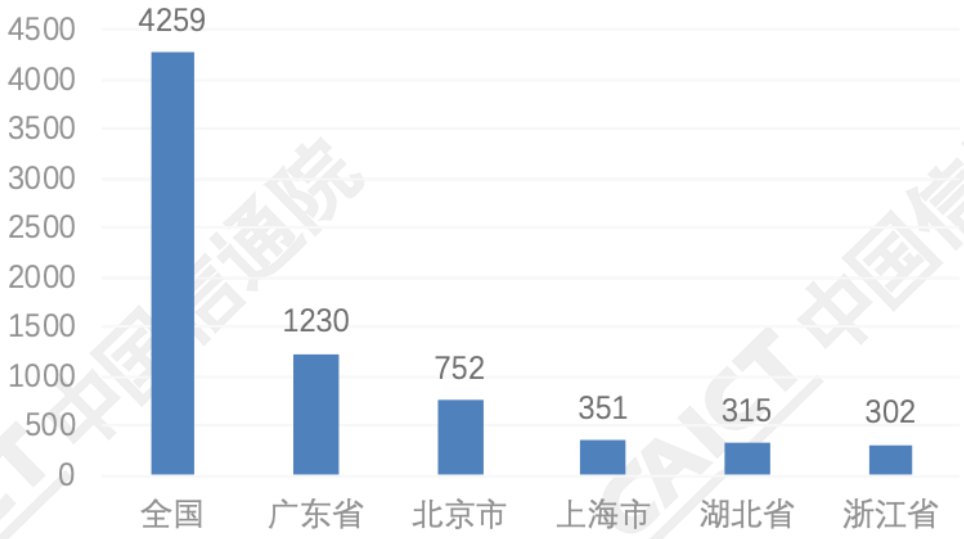


数据来源：北京智游网安科技有限公司（爱加密）

图 8 银行类移动 App 应用市场分布情况

2．证券类移动应用分布情况

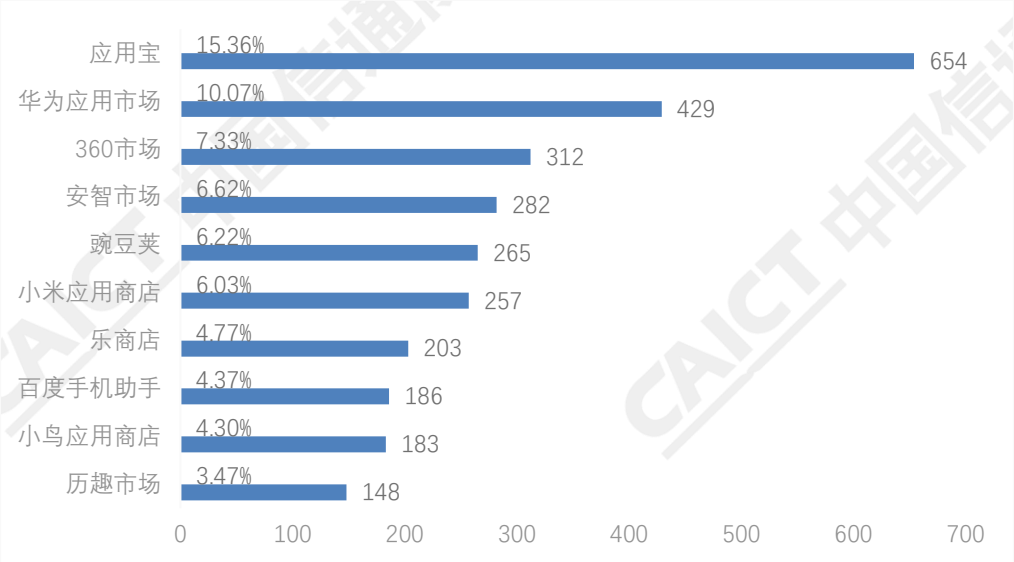
本次收录的证券类 App 共 4259 款，广东省占据了全国 28.88%的证券类 App，排名第一；北京以 17.66%的占比率排名第二；上海排行第三，占比率为 8.24%。App 数量较多的还有湖北与浙江，二者 App 数量均超过 300 个。具体数据如图 9 所示。



数据来源：北京智游网安科技有限公司（爱加密）

图 9 证券类移动 App 地域数量统计

证券类 App 分布在 112 个应用市场，收录量排名前十的应用市场共计收录了 68.54%的移动应用。其中，应用宝收录的 App 数量最多，占监测总数的 15.36%；其次是华为应用市场，收录量占监测总数的 10.07%；360 市场排名第三，收录 7.33%的 App 应用。具体数据如图 10 所示。

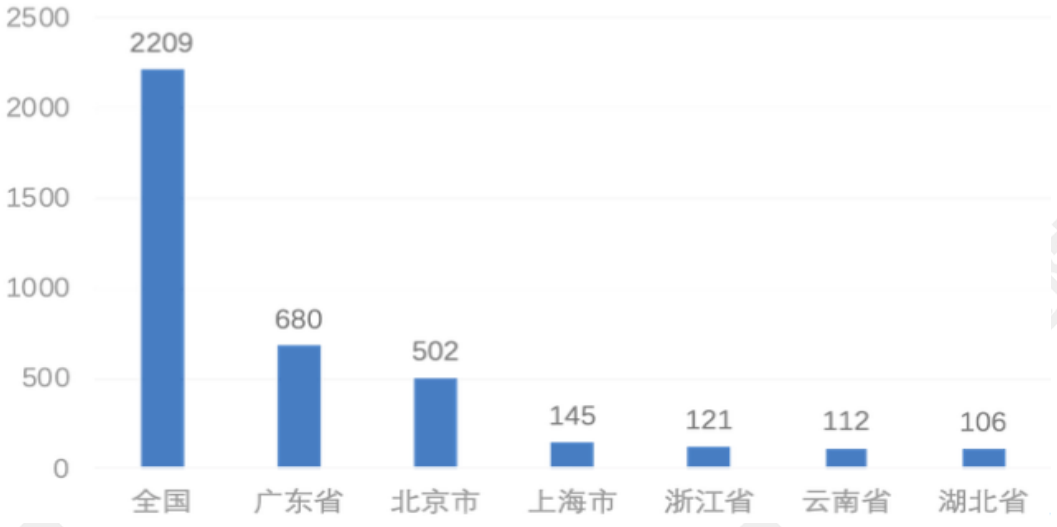


数据来源：北京智游网安科技有限公司（爱加密）

图 10 证券类 App 应用市场分布情况

3. 保险类移动应用分布情况

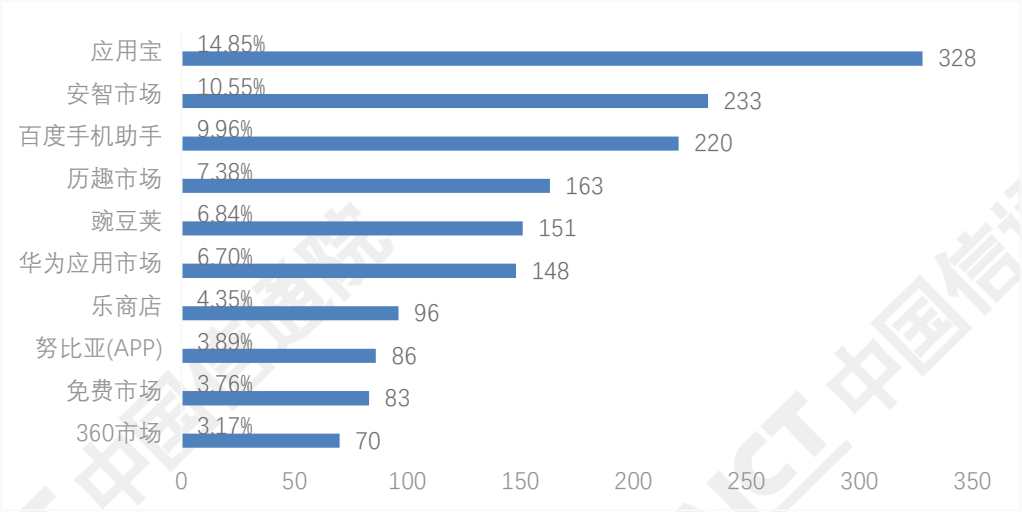
本次收录的保险类 App 共 2209 款，广东和北京两地占据 53.51%的市场份额。此外，就 App 数量而言，超过 100 款 App 的省份还有上海、浙江、云南和湖北四个省份。具体数据如图 11 所示。



数据来源：北京智游网安科技有限公司（爱加密）

图 11 保险类移动 App 地域数量统计

保险业 App 分布在 101 个应用市场，收录量排名前十的应用市场共计收录 71.44%的移动应用。其中，应用宝收录 App 数量最多，占监测总数的 14.85%;其次是安智市场,收录量占监测总数的 10.55%;百度手机助手排名第三，收录 9.96%的 App 应用。具体数据如图 12 所示。



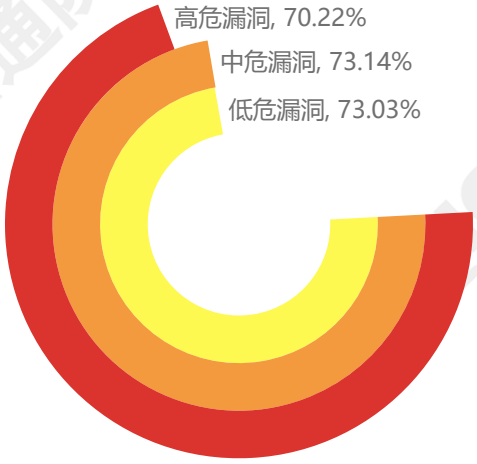
数据来源：北京智游网安科技有限公司（爱加密）

图 12　保险类 App 应用市场分布情况

三、移动金融应用的安全风险

（一）以数据泄露为代表的高危漏洞风险

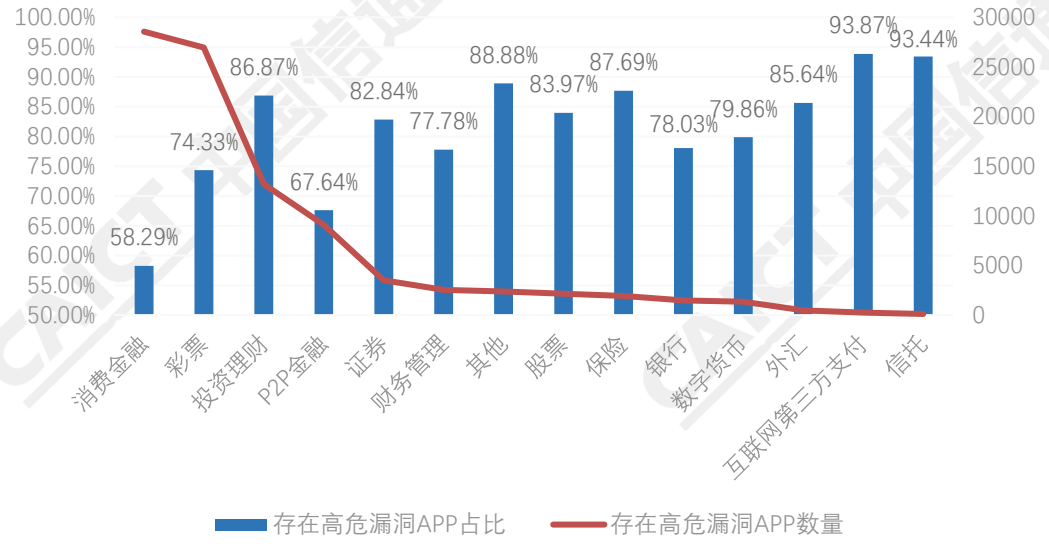
报告团队对 133327 款金融行业 App 进行扫描，共计检测出 1979696 条漏洞记录，涉及 60 种漏洞类型，其中有 21 种为高危漏洞。金融行业 App 中，73.23%存在不同程度的安全漏洞，70.22%存在高危漏洞。平均每款金融行业 App 存在 20.3 个安全漏洞，其中 6.7 个为高危漏洞。具体数据如图 13 所示。



数据来源：北京智游网安科技有限公司（爱加密）

图 13 金融行业 App 各等级漏洞情况

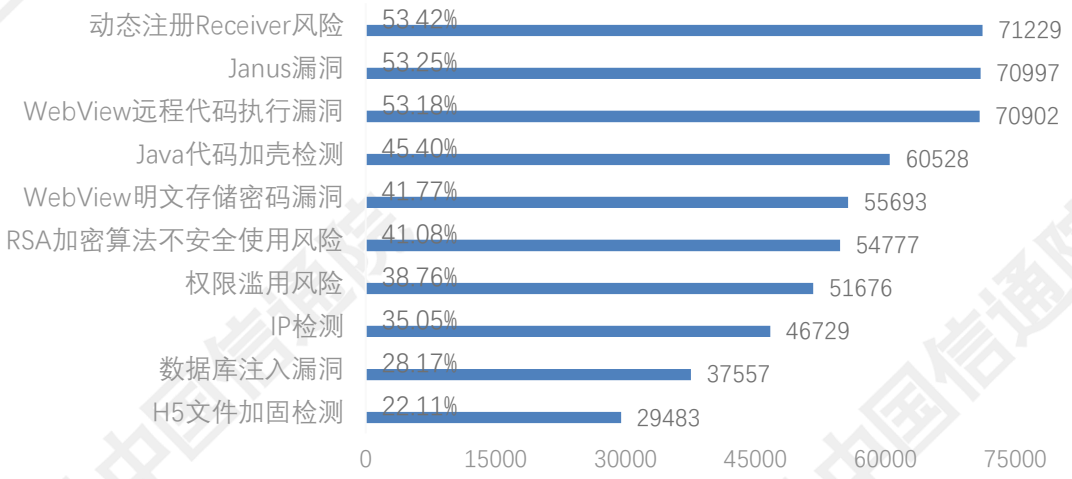
从 App 分类角度来看，互联网第三方支付和信托类 App 的高危漏洞问题较为突出，存在高危漏洞 App 的比例 93.87%和 93.44%。保险、投资理财、外汇等分类的 App 高危漏洞问题也相对严重，存在高危漏洞的 App 比例超过 85%。具体数据如图 14 所示。



数据来源：北京智游网安科技有限公司（爱加密）

图 14 不同细分领域高危漏洞 App 数量及占比情况

从高危漏洞类型来看（Top10 高危漏洞介绍及危害说明参见附录 C），存在动态注册 Receiver 风险 App 数量最多，占观测总数的 53.42%；Janus 漏洞的与 Web View 远程代码执行漏洞紧随其后，分别占据观测总数的 53.25%与 53.18%。具体数据如图 15 所示。



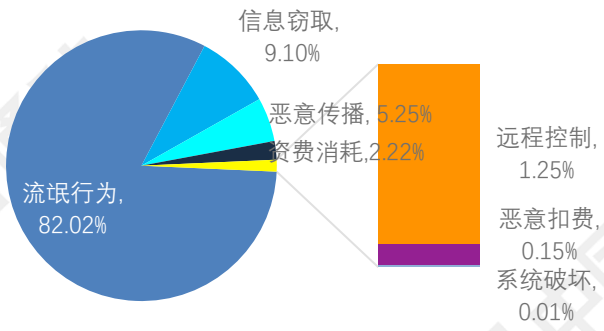
数据来源：北京智游网安科技有限公司（爱加密）

图 15 高危漏洞类型分布（Top10）

（二）以流氓行为为代表的恶意程序风险

经报告团队使用的恶意程序检测系统检测发现，共有 8217 款金融行业 App 被检测出含有恶意程序，恶意程序感染率为 6.16%。主要涉及移动用户的隐私数据收集、恶意扣费、流量资源消耗、广告推送等多种恶意行为，对移动用户的个人信息及财产安全带来巨大威胁。

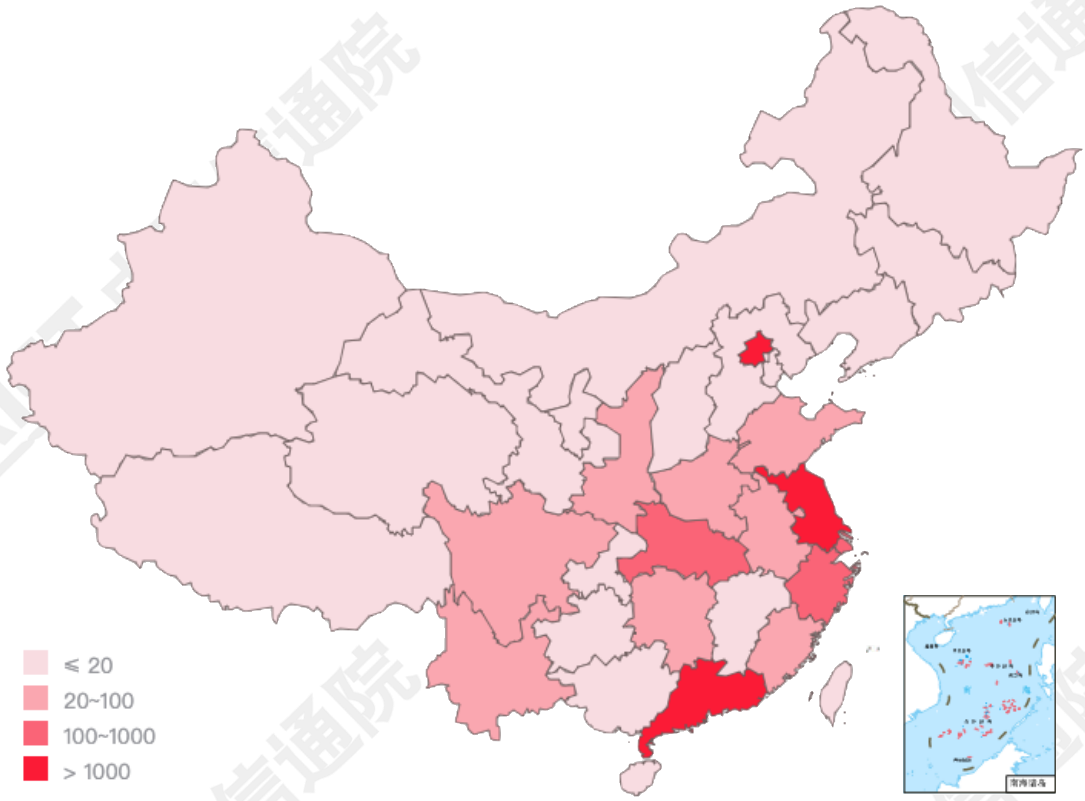
从恶意程序类型来看（恶意程序类型及说明参加附录 D），有 82.02%的 App 已经受到具有流氓行为的恶意程序感染，这类恶意程序会在用户未授权的情况下，弹出广告窗口等，不仅影响用户使用体验，而且如用户误触点击可能带来进一步隐私风险和安全问题；9.10%的 App 受到具有信息窃取行为的恶意程序感染，这类恶意程序会窃取用户短信、通讯录、通话记录、位置等敏感信息，导致用户信息泄露；5.25%的 App 受到具有恶意传播行为的恶意程序感染，这类恶意程序的特征是在用户不知情或未授权的情况下，将自身、自身的衍生物或其它恶意程序扩散到正常设备。具体数据如图 16 所示。



数据来源：北京智游网安科技有限公司（爱加密）

图 16　App 恶意程序类型分布情况（一款 App 可能存在多种病毒）

从地域分布来看，除 19 款归属省份不明的 App 之外，其余 8198 款受到恶意程序感染的 App 分布除香港外的 33 个省级行政区（受到恶意程序感染的 App 地域分布数据参见附录 E）。其中，江苏受到恶意程序感染的 App 数量最多，占全部受到恶意程序感染的 App 总数的 37.63%；广东其次，有 30.16%的 App 受到恶意程序感染；北京排行第三，有 12.56%的 App 受到恶意程序感染。受到恶意程序感染的 App 的地域分布情况如图 17 所示：

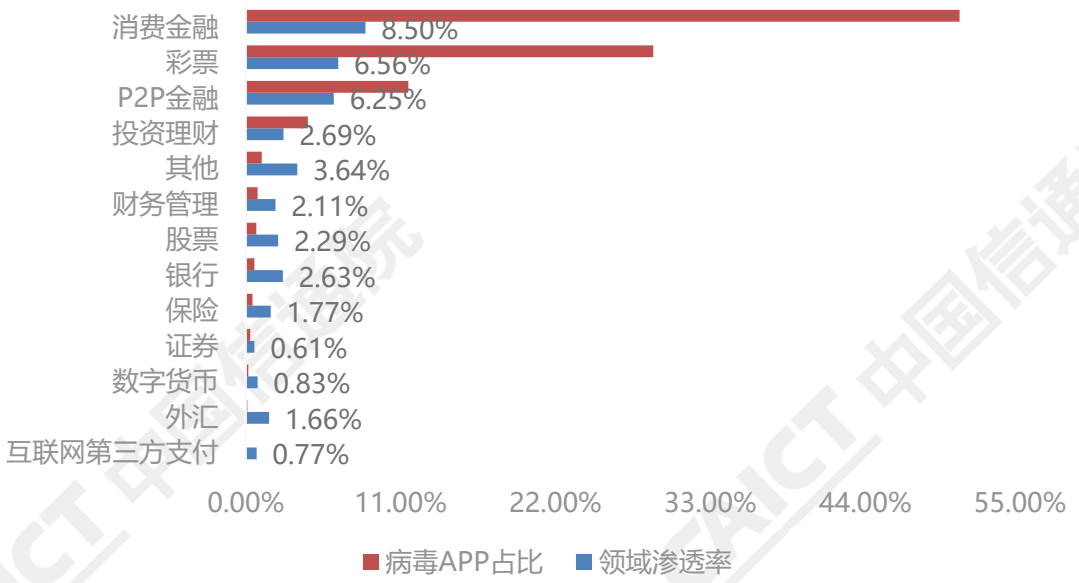


数据来源：北京智游网安科技有限公司（爱加密）

图 17 受到恶意程序感染的 App 区域分布情况

从 App 细分领域角度来看，受到恶意程序感染的 App 数量前三

的类别分别为消费金融类、彩票类、P2P 金融类 App，分别有 4166 款、2378 款、949 款 App 已经受到恶意程序感染。而从各个分类受到恶意程序感染的 App 比例来看，消费金融类、彩票类、P2P 金融类受到恶意程序感染的比例相对较高，均超过 6%。具体数据如图 18 所示。



数据来源：北京智游网安科技有限公司（爱加密）

图 18 各细分领域受到恶意程序感染的 App 分布情况

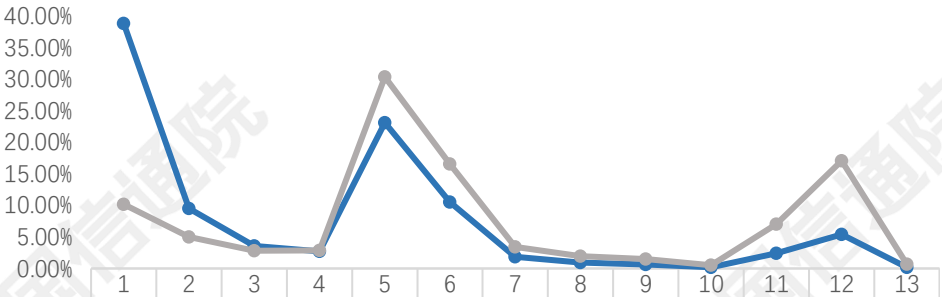
（三）使用第三方 SDK 引入安全风险

SDK 是 Software Development Kit 的缩写，即“软件开发工具包”，它是辅助开发某一类应用软件的相关文档、范例和工具的集合。随着移动互联网的快速迭代发展，越来越多的服务提供商选择将其服务封装成 SDK 供开发者使用。而开发者为了提升效率、降低成本，往往会在开发过程中嵌入第三方 SDK。但是，第三方 SDK 常存在安全漏

洞、恶意程序、隐蔽收集个人信息等安全问题，进而给嵌入 SDK 的 App 带来相应的安全隐患。

据爱加密发布的《全国移动应用 SDK 市场占有率分析报告》统计，有超过 60%的 SDK 含有多种漏洞，且由于 SDK 被广泛使用到大量 App 中，漏洞造成的影响范围极广。不法分子可以通过制作、发布、吸引 App 开发者嵌入含有恶意代码的 SDK，造成短时间、大范围的恶意程序传播和感染，且此类恶意程序具有很强的隐蔽性和对抗杀毒软件的能力。SDK 作为独立的软件开发工具包，具有收集个人信息的能力，但 SDK 收集哪些个人信息，用户往往难以感知，甚至 App 开发者也未必知晓，给用户个人信息安全带来严重威胁。

报告团队观测发现，有 27300 款金融行业 App 嵌入了第三方 SDK，占全部金融行业 App 的 20.48%。这些 App 共嵌入 104005 个第三方 SDK，平均每款 App 嵌入 3.8 个。金融行业 App 第三方 SDK 使用情况如图 19 所示。



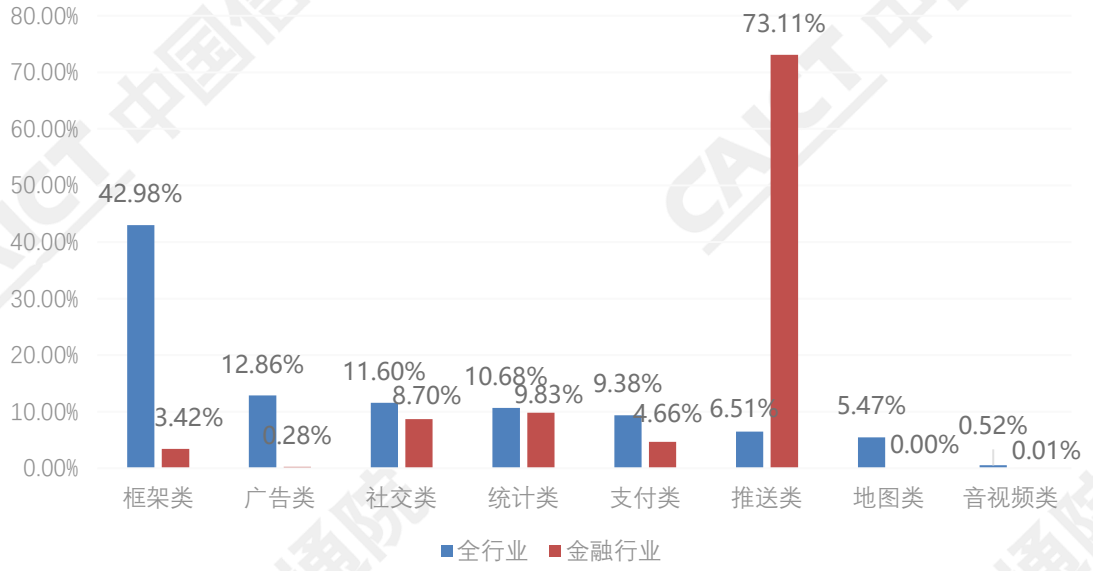
	1	2	3	4	5	6	7	8	9	10	11	12	13
APP占比	38.83%	9.53%	3.58%	2.72%	23.12%	10.51%	1.88%	0.93%	0.63%	0.20%	2.43%	5.42%	0.20%
SDK数量占比	10.19%	5.00%	2.82%	2.86%	30.35%	16.55%	3.45%	1.96%	1.50%	0.52%	7.01%	17.09%	0.69%

数据来源：北京智游网安科技有限公司（爱加密）

图 19 不同 SDK 个数区间对应的 App 分布情况

从 App 使用的 SDK 类型来看，金融行业与全行业在 SDK 使用类型上有较大差异。金融行业 App 使用排名前三的 SDK 分别是推送类、统计类和社交类，占比分别为 73.11%、9.83%和 8.70%；全行业 App 使用排名前三的 SDK 为框架类、广告类和社交类，占比分别为 42.98%、12.86%和 11.60%。而框架类和广告类 SDK 在金融行业 App 的 SDK 使用占比仅有 3.42%和 0.28%。具体数据如图 20 所示。

基于以上研究发现，与金融交易高度相关的支付类 SDK 在金融行业 App 的使用频次相对较低，而推送类 SDK 在金融行业 App 中使用十分广泛，安全风险问题需要重点关注。



数据来源：北京智游网安科技有限公司（爱加密）

图 20 全行业和金融行业 App 使用的各类 SDK 分布对比

（四）违规索权带来的隐私泄露风险

敏感权限获取和隐私信息泄漏是近年来 App 安全关注和防范的

重点。App 索取用户设备的敏感权限和用户的隐私信息，可能导致用户设备被植入恶意程序、用户账户和隐私信息泄露等一系列安全风险。本次调研抽样选取了 12 款下载量过亿的典型金融行业 App，分别对敏感权限的获取情况和在隐私政策方面存在的问题进行了分析，发现多款 App 存在不同程度的超范围索取用户权限的情况，在隐私政策方面也存在多种违法违规行为，给用户个人隐私信息安全带来了隐患。

1．超范围获取敏感权限

研究发现，12 款 App 均存在不同程度的超范围权限采集现象。这些 App 共获取了 29 种高敏感权限、15 种中敏感权限、33 种低敏感权限。不同敏感等级的隐私权限获取数量如表 1 所示。

表 1 调研的 12 款 App 隐私权限获取情况

序号	App 名称	版本号	包名	所属渠道	高敏感	中敏感	低敏感
1	中国建设银行	4.2.0	com.chinamworld.main	华为应用市场	18	10	22
2	交通银行	3.3.10	com.bankcomm.Bankcomm	华为应用市场	18	10	22
3	工银融 e 联	3.4.0	com.icbc.im	华为应用市场	16	10	19
4	中国工商银行	4.1.0.8.1	com.icbc	华为应用市场	15	9	20

序号	App 名称	版本号	包名	所属渠道	高敏感	中敏感	低敏感
5	华为钱包	9.0.3.300	com.huawei.wallet	华为应用市场	15	9	16
6	中国农业银行	4.1.0	com.android.bankabc	iTools	16	9	14
7	中国银行	6.0.6	com.chinamworld.bocmbci	华为应用市场	10	9	19
8	全能中彩彩票	3.2.8	com.qnzc.sls_App.activity	应用宝	12	7	16
9	快乐宝彩票	3.2.8	com.klb.sls_App.activity	应用宝	12	7	16
10	彩运宝彩票-快 3	3.2.8	com.cyb.sls_App.activity	应用宝	12	7	16
11	草根投资	4.2.0	cgtz.com.cgtz	其他	10	11	12
12	无忧钱包	1.1.6	com.chuangle.clwy	应用宝	4	2	7

数据来源：北京智游网安科技有限公司（爱加密）

9 款及 9 款以上的应用获取的权限类型有 25 种，其中，高敏感权限 8 种，中敏感权限 7 种，低敏感权限 10 种。详细数据如表 2 所

示。

表 2 9 款及 9 款以上 App 获取的权限列表

序号	权限类别	敏感度	权限名	获取权限 App 占比
1	读取手机状态和身份	高敏感	READ_PHONE_STATE	100%
2	修改或删除存储卡中的内容	高敏感	WRITE_EXTERNAL_STORAGE	100%
3	读取系统日志	高敏感	READ_LOGS	91.67%
4	拍摄照片和录制视频	高敏感	CAMERA	91.67%
5	修改系统设置	高敏感	WRITE_SETTINGS	91.67%
6	发起电话呼叫	高敏感	CALL_PHONE	75%
7	录制音频	高敏感	RECORD_AUDIO	75%
8	重启程序	高敏感	REBOOT	75%
9	访问确认位置信息	中敏感	ACCESS_FINE_LOCATION	100%
10	更改 WLAN 状态	中敏感	CHANGE_WIFI_STATE	100%
11	访问大致位置	中敏感	ACCESS_COARSE_LOCAT	91.67%

序号	权限类别	敏感度	权限名	获取权限App 占比
	信息		ION	
12	改变网络状态	中敏感	CHANGE_NETWORK_STATE	91.67%
13	获取任务信息	中敏感	GET_TASKS	91.67%
14	装载和卸载文件系统	中敏感	MOUNT_UNMOUNT_FILESYSTEMS	91.67%
15	显示系统窗口	中敏感	SYSTEM_ALERT_WINDOW	83.33%
16	查看 WLAN 状态	低敏感	ACCESS_WIFI_STATE	100%
17	查看获取网络状态	低敏感	ACCESS_NETWORK_STATE	100%
18	防止处理器休眠或屏幕变暗	低敏感	WAKE_LOCK	100%
19	访问互联网权限	低敏感	INTERNET	100%
20	开机时自动启动	低敏感	RECEIVE_BOOT_COMPLETED	100%
21	控制振动器	低敏感	VIBRATE	100%
22	读取设备外部存储空间	低敏感	READ_EXTERNAL_STORAGE	91.67%

序号	权限类别	敏感度	权限名	获取权限 App 占比
23	使用蓝牙	低敏感	BLUETOOTH	91.67%
24	创建快捷方式	低敏感	SHORTCUT	83.33%
25	更改您的音频设置	低敏感	MODIFY_AUDIO_SETTINGS	83.33%

数据来源：北京智游网安科技有限公司（爱加密）

由上表可知，所有 App 均获取两项高敏感权限,一是获取了“READ_PHONE_STATE”读取手机状态和身份权限，有此权限的应用允许访问设备的任意手机功能；二是获取了“WRITE_EXTERNAL_STORAGE”写入外置存储器权限，有此权限的应用可以修改或删除存储卡中的内容。全国信息安全标准化技术委员会于 2019 年 6 月发布的《网络安全实践指南——移动互联网应用基本业务功能必要信息规范》明确规定，金融行业 App 基本业务功能收集的必要信息包括：“手机号码”、“账号信息”、“身份信息”、“银行账户信息”、“个人征信信息”、“紧急联系人信息”以及“借贷交易记录”7 项内容。应用程序访问设备的手机功能及修改或删除存储卡中的内容涉嫌超范围获取权限。

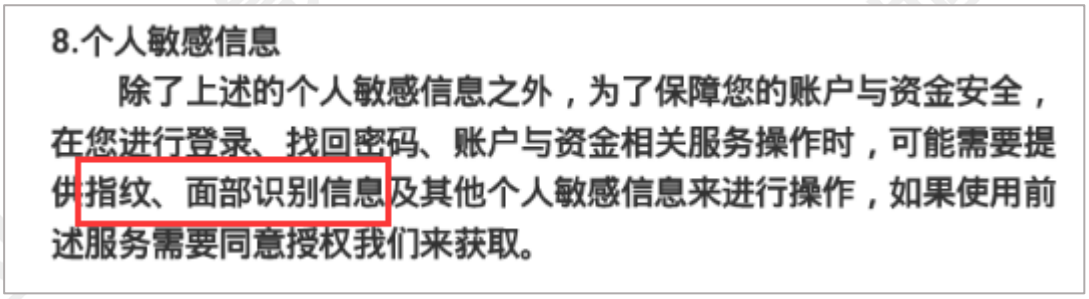
此外，App 惯常获取的高敏感权限还包括：发起电话呼叫、录制音频、拍摄照片和录制视频、读取系统日志等，给用户隐私带来巨大

安全隐患。

2．未严格遵守隐私政策法规

隐私政策法规是 App 在对个人信息进行收集、使用、存储、分享等各种操作环节的行为规范，需要 App 用户对其充分知晓和同意。《网络安全法》第 41 条规定“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”。然而，在隐私政策方面，抽样的部分 App 中也涉嫌存在违法违规问题。

（1）超范围获取个人指纹及面部识别信息等非必要敏感信息。


8.个人敏感信息

除了上述的个人敏感信息之外，为了保障您的账户与资金安全，在您进行登录、找回密码、账户与资金相关服务操作时，可能需要提供指纹、面部识别信息及其他个人敏感信息来进行操作，如果使用前述服务需要同意授权我们来获取。

图 21 某金融 App 隐私政策中收集用户指纹、面部等生物信息

如图 21 所示，某款金融行业 App 隐私政策中出现要求用户提供指纹、面部识别信息等个人敏感信息，实际上进行登录等操作时并不需要。

（2）给用户删除个人信息设置条件，非规定情形下不予理睬。

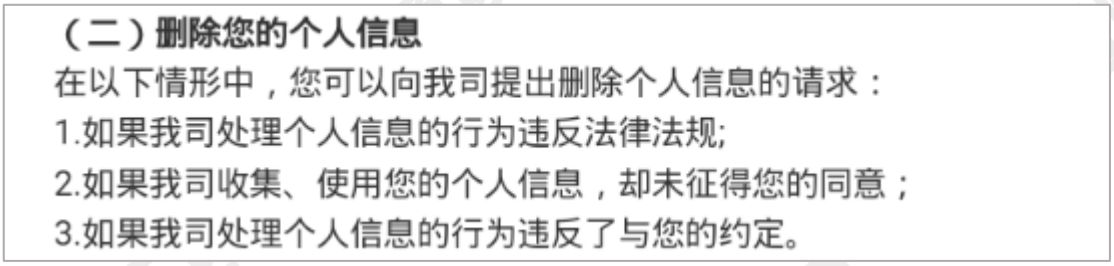


图 22 某金融 App 隐私政策中删除个人信息条款

根据 App 专项治理工作组制定《评估指南》第八条规定：“支持用户注销账号，更正或删除个人信息”。如图 22 所示，某炒股类 App 设置条件阻止用户删除个人信息。

（3）未提供单独的《隐私政策》，违反了隐私政策要以单独成文形式发布的要求。

图 23 某金融 App 未单独提供隐私政策

如图 23 所示，某借贷类 App 将隐私政策作为《用户注册服务协

议》文件中的一部分存在，违法了隐私政策单独成文的要求。

（4）超范围获取读取通讯录、摄像头、通话录音等与服务无关权限，未对收集到的相关信息所对应的功能进行说明。

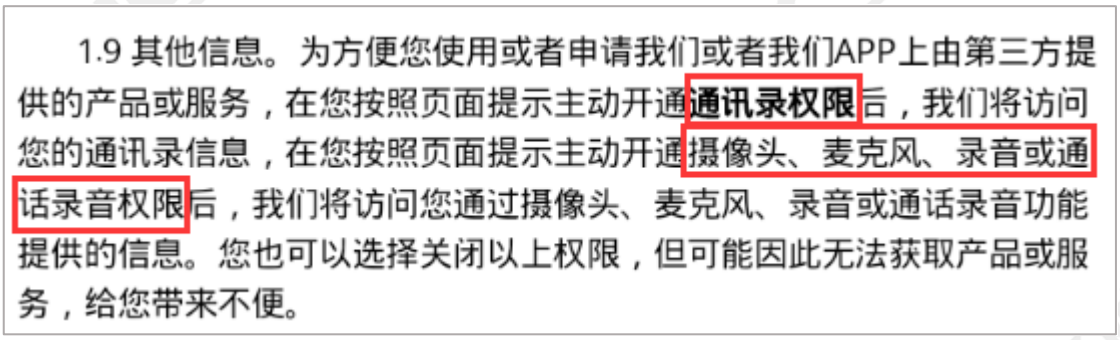
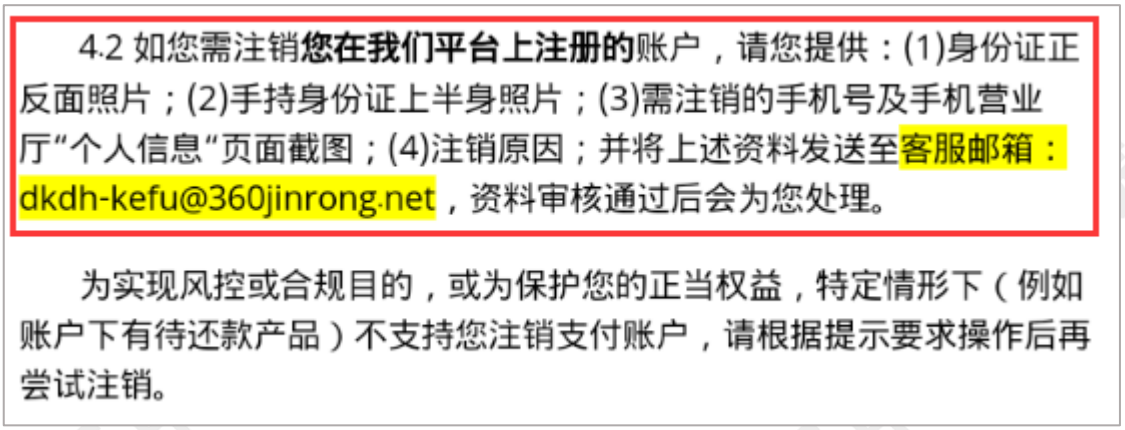

1.9 其他信息。为方便您使用或者申请我们或者我们APP上由第三方提供的产品或服务，在您按照页面提示主动开通**通讯录权限**后，我们将访问您的通讯录信息，在您按照页面提示主动开通摄像头、麦克风、录音或通话录音权限后，我们将访问您通过摄像头、麦克风、录音或通话录音功能提供的信息。您也可以选择关闭以上权限，但可能因此无法获取产品或服务，给您带来不便。

图 24 某金融 App 隐私政策中未说明收集信息的用途

如图 24 所示，某借贷类 App 声称关闭这些权限则影响用户获取应用提供的产品或服务。

（5）注销账号程序繁琐且涉嫌收集与该操作无关的个人信息。违反《评估指南》：“App 不应收集与业务功能无任何关系的个人信息。”


4.2 如您需注销**您在我们平台上注册的**账户，请您提供：(1)身份证正反面照片；(2)手持身份证上半身照片；(3)需注销的手机号及手机营业厅“个人信息”页面截图；(4)注销原因；并将上述资料发送至客服邮箱：dkdh-kefu@360jinrong.net，资料审核通过后会为您处理。

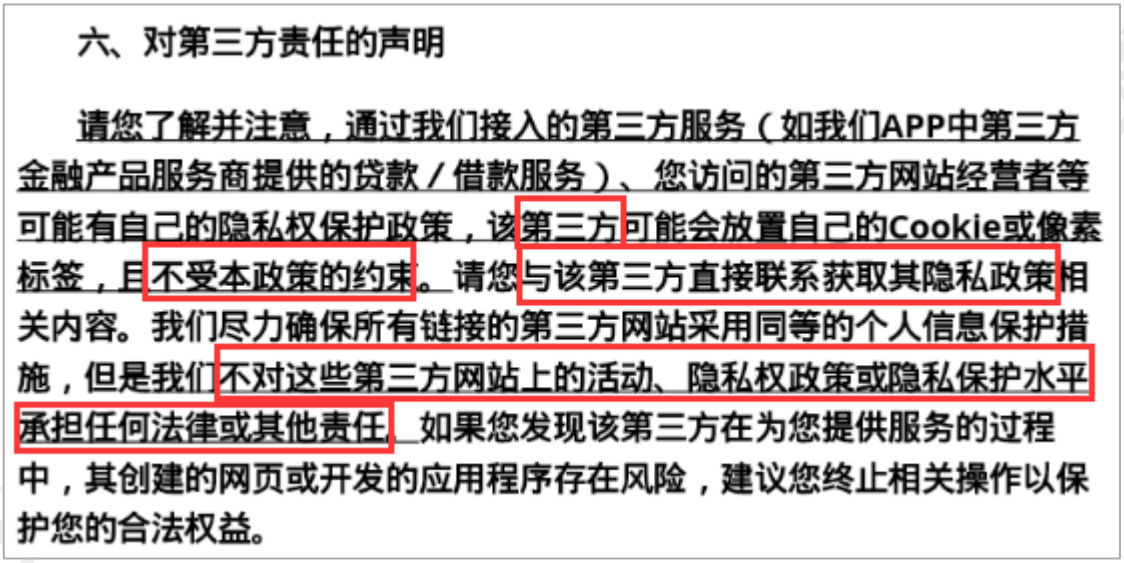
为实现风控或合规目的，或为保护您的正当权益，特定情形下（例如账户下有待还款产品）不支持您注销支付账户，请根据提示要求操作后再尝试注销。

图 25 某金融 App 隐私政策中注销账号相关条款

如图 25 所示，某金融 App 隐私政策要求注销账号时需提供身份

正反面照片、个人手持身份证上半身照片及手机营业厅“个人信息”页面截图等敏感信息，违规获取个人隐私的同时，增加了注销难度。

（6）应用程序接入的第三方服务不受该隐私政策限制，且需主动与第三方联系方能获取其隐私政策相关内容，存在隐私信息泄露的风险。而且，应用主体声称对此可能产生的一系列结果并不负责。如图 26 所示。



六、对第三方责任的声明

请您了解并注意，通过我们接入的第三方服务（如我们APP中第三方金融产品服务商提供的贷款／借款服务）、您访问的第三方网站经营者等可能有自己的隐私权保护政策，该第三方可能会放置自己的Cookie或像素标签，且不受本政策的约束。请您与该第三方直接联系获取其隐私政策相关内容。我们尽力确保所有链接的第三方网站采用同等的个人信息保护措施，但是我们不对这些第三方网站上的活动、隐私权政策或隐私保护水平承担任何法律或其他责任。如果您发现该第三方在为您提供服务的过程中，其创建的网页或开发的应用程序存在风险，建议您终止相关操作以保护您的合法权益。

图 26 某金融 App 隐私政策中关于第三方服务隐私政策条款

（7）部分 App 的隐私政策通篇未注明隐私政策时效。违反《评估指南》中“应明确标识隐私政策发布、生效、更新日期”。

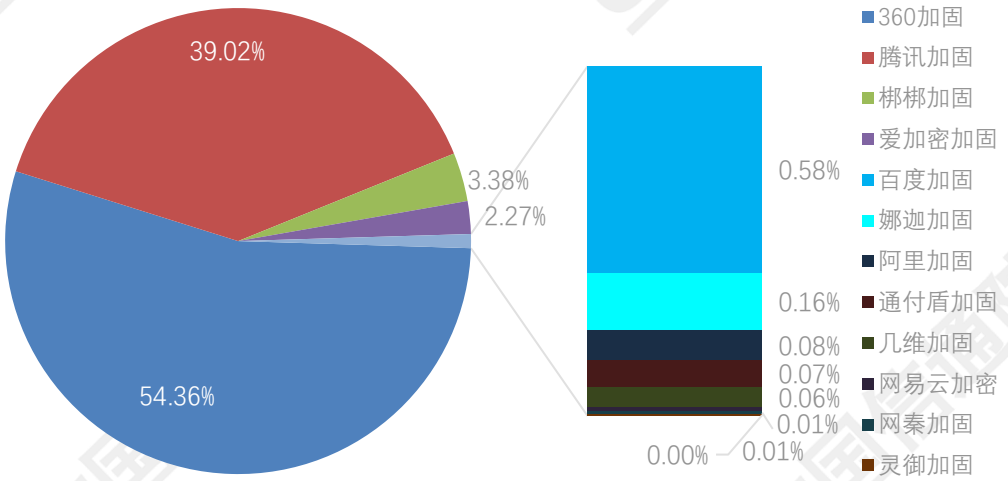
（五）安全加固不足带来的安全风险

基于 Java 编写的安卓 App 容易被破解暴露 App 源代码，进而带来 App 盗版、二次打包、注入等安全问题。“安全加固”是维护 App 安全的重要防护手段，它能够有效阻止对 App 的反汇编分析。经过安

全加固的 App，不仅其系统稳定性得到提升，还拥有规避一定程度安全风险的能力。经检测，22777 款金融行业 App 至少进行过一次安全加固，仅占观测的金融行业 App 总量的 17.08%。金融行业 App 开发者对于安全加固的重视程度不足，仍有超过 8 成的金融行业 App 未进行过安全加固。

1．App 加固集中在主流服务商平台

观测发现，金融行业 App 主要选择 360、腾讯、梆梆、爱加密、百度等 12 家安全服务商进行安全加固。其中，54.36%的金融行业 App 选择 360 加固平台进行安全加固；39.02%的金融行业 App 选择腾讯加固平台，其余 6.62%的金融行业 App 选择其他厂商进行安全加固。加固厂家选择如图 27 所示：

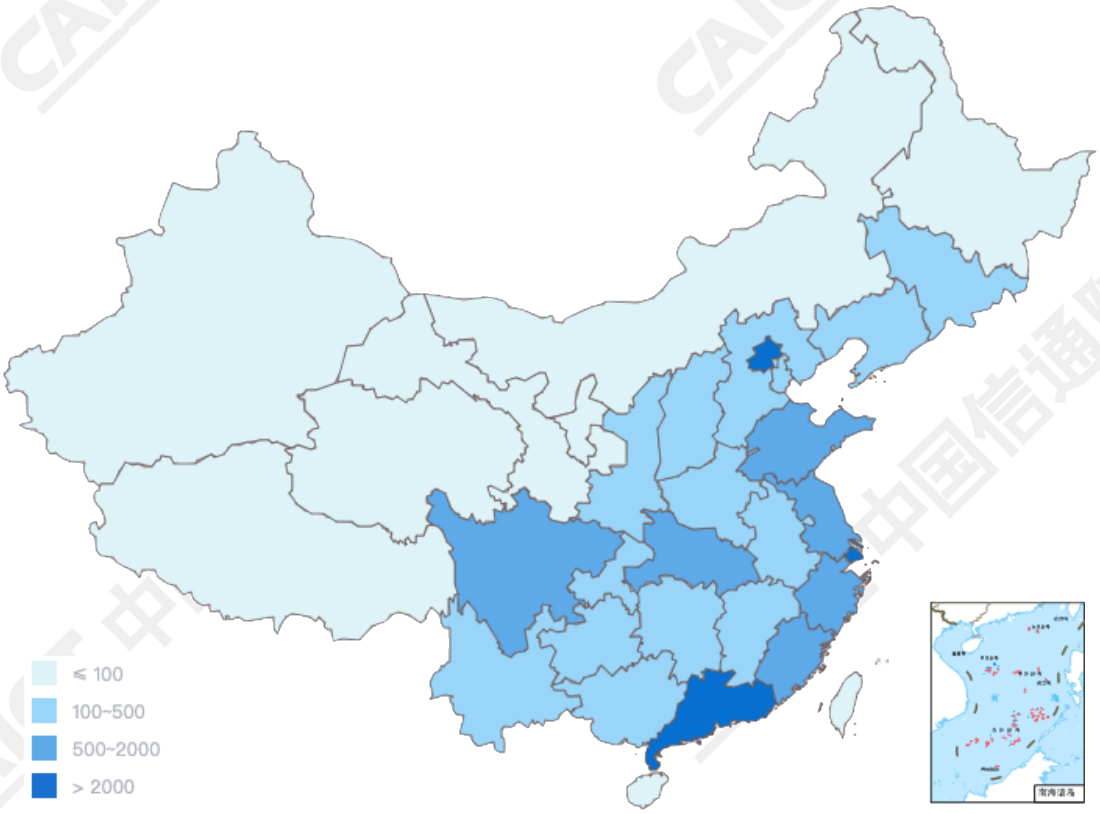


数据来源：北京智游网安科技有限公司（爱加密）

图 27 不同加固厂家服务的 App 占比

2．各省份移动应用加固情况相近

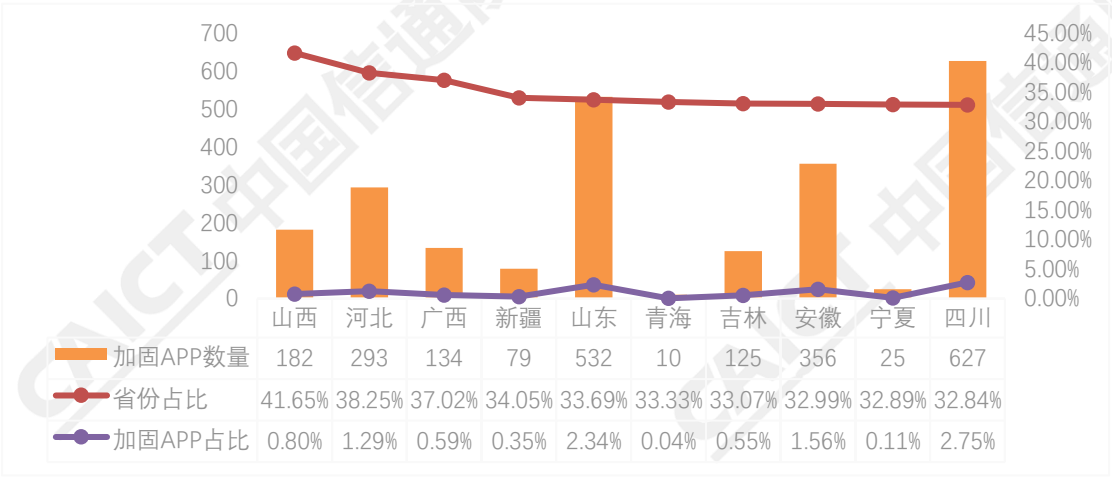
从加固 App 的地域分布来看，发达地区 App 供应商安全意识较强，加固数量最多。具体数据如图 28 所示。



数据来源：北京智游网安科技有限公司（爱加密）

图 28 加固 App 地域分布

除湖北、湖南、广东、内蒙古、陕西 5 省 App 加固比例未达到行业整体加固比例之外，其他 27 个省份 App 加固比例均超过行业整体加固比例 17.08%，其中山西省金融行业 App 加固比例最高，达到 41.65%。具体数据如图 29 所示。



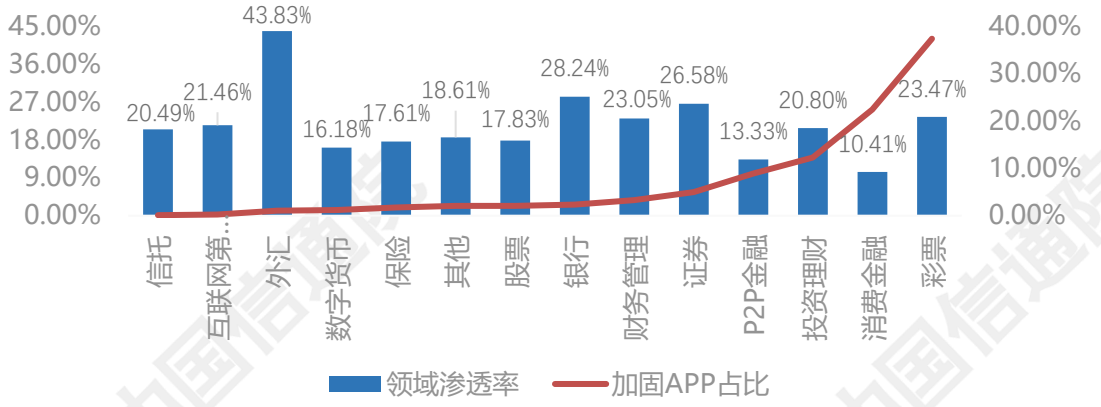
	山西	河北	广西	新疆	山东	青海	吉林	安徽	宁夏	四川
加固APP数量	182	293	134	79	532	10	125	356	25	627
省份占比	41.65%	38.25%	37.02%	34.05%	33.69%	33.33%	33.07%	32.99%	32.89%	32.84%
加固APP占比	0.80%	1.29%	0.59%	0.35%	2.34%	0.04%	0.55%	1.56%	0.11%	2.75%

数据来源：北京智游网安科技有限公司（爱加密）

图 29 加固 App 数量省份占比前十分布

3. 借贷类 App 加固比例相对偏低

从加固 App 所属金融行业细分领域角度分析发现，借贷类 App 加固比例相对偏低，消费金融类和 P2P 金融类 App 加固比例分别为 10.41%和 13.33%，低于金融行业 App 平均加固比例。外汇类、银行类、证券类 App 的加固比例位列前三，分别是 43.83%、28.24%、26.58%，App 开发者安全意识相对较强。具体数据如图 30 所示。



数据来源：北京智游网安科技有限公司（爱加密）

图 30 各金融细分领域 App 加固分布情况

四、移动金融应用安全创新思路

（一）以移动金融应用安全为核心的整体设计

目前国内很多金融机构和企业是围绕 App 单点解决方案来构建安全基础设施的，这在很大程度上是因为此类解决方案投资数额较小且投资周期较短。然而碎片化的解决方案无法为企业提供全面可靠的安全保护，且碎片化的基础设施可能会带来更高的维护成本和维护周期。企业应该寻求应对日常安全威胁更为全面的解决方案，通过建立协同的安全防护体系来实现威胁的监测、预警和响应。将 App 业务与系统协同防御作为安全战略的关键组成部分，需要全面、多维度、多层次的安全意识与能力融合来保障 App 业务全生命周期安全。

首先，程序安全是基础。无论是移动端、第三方 SDK 还是服务器端，软件程序是业务开展的载体，也是移动 App 面临风险最高的环节。程序安全涉及到代码安全、程序执行环境安全、开发规范与代码引用安全等。程序开发者应建立相应的管理机制和安全开发技术能力，从程序开发、代码保护、上线评估及运行环境要求方面加强自身的安全能力。

其次，数据安全是核心。无论是业务开展还是个人信息保护，数据都是核心要素，也是很多非法黑客攻击的最终目的。对于移动 App 来说涉及到的数据处理环节有数据本地存储、数据网络传输、数据输

入与界面数据显示。因此，移动金融 App 要根据自身技术特性和业务特点，就每个数据处理环节制定切实可行的防护策略，保证自身业务的运营安全和用户数据安全。

最后，认证安全是纽带。移动端和服务器端之间的信任是通过身份认证建立的，只有保证认证安全才能保证移动业务系统的完整性。移动金融业务涉及开户、登录、支付等多个认证环节，采用的技术涉及用户名/密码机制、短信验证码机制、数字证书机制等。鉴于移动端的复杂环境和移动 App 的脆弱性，金融机构应加强移动 App 与服务器的认证环节，综合使用多种认证手段，保证移动业务系统的完整性以及业务连续性。

（二）建设符合监管发展的合规检测能力

移动金融面临的监管形势逐步趋严，为保障行业健康有序发展，监管部门应帮助 App 运营单位加强合规性安全检测能力建设，履行网络安全保护责任与义务，保护公民隐私信息，落实安全主体责任和网络实名验证、建立健全安全管理制度，防止数据泄露、窃取或篡改等问题。

1．个人信息安全检测能力

依据《信息安全技术个人信息安全规范》《App 违法违规收集使用个人信息自评估指南》等细则指南，检测移动应用中隐私条款内容的合规性，对 App 隐私条款可能导致的隐私政策文本、App 收集使用

个人信息行为、App 运营者对用户权利保障等多种维度进行检测，及时发现个人信息收集和使用的合规性问题，确保监管政策全面有效落实。

2．恶意行为检测能力

通过动态运行过程中的行为检测，准确、全面的识别 App 是否存在越权行为、网络访问行为、境外 URL 访问行为等敏感内容，防止移动金融 App 在企业和开发者不知情的情况下，被第三方 SDK、插件、组件等恶意利用，私自对个人信息进行采集或进行其他非法行为，全面保障 App 合规性和最终用户个人信息安全。

金融机构同时应加强网络安全知识宣传，提高用户安全意识，提醒用户通过官方网站和正规应用商店下载使用移动应用，避免被恶意软件、山寨应用误导，获取手机过多权限导致个人隐私泄露。

（三）全生命周期的移动金融应用安全防护策略

对于移动金融应用风险的防护，从策略上看，根据防护阶段的不同，可分为事前、事中、事后三大类全生命周期安全防护策略。

1．事前预防

通过设置设备指纹、验证码、数据加密等安全加固手段，增强 App 自身安全性，提高移动应用事前预防能力。同时，要对 App 自身及应用业务开展模拟攻击测试，在各业务场景中针对单个模块或多个模块的组合分别测试，发现潜在风险点。

2．事中决策

事中即在风险发生的同时能够实时感知。通常的做法是基于恶意流量的特征匹配，对网络中的异常流量进行检测，目前也有一些新的思路是通过 AI 技术进行智能判断。

3．事后分析

事后针对存量数据进行分析。通常使用的手段是对大数据进行建模，找出在事中阶段未能检测出的异常流量。

单一种类的防护产品一般都可归属为这三类之一，但是在实际场景中，随着攻击手段的不断升级，已经很难依靠单一手段就能实现有效防护。纵深式防御正成为主流，通过多种技术的结合，在不同的时间点、不同的攻击入口，建立多层防御体系。

（四）主动风险感知替代被动响应的防御思维

如从常见的设备风险、环境风险、账号风险、行为风险等维度，主动对于移动金融应用风险进行感知。

1．设备风险感知

设备端风险的感知依托于设备指纹技术，即通过对设备软硬件信息的采集，通过一定的算法计算出标识该设备的一串唯一码。该技术常用于识别攻击者改机、刷机等欺诈行为。

2．环境风险感知

移动端设备最大特点就是移动性，同一台设备可能频繁的在不同

的网络环境中切换，如 4G/5G 网络、家庭 Wi-Fi、工作 Wi-Fi 等。通过对网络环境的监控，可识别出设备是否进入可疑网络，或是将长期处于可疑网络的设备标识为风险设备。

3．账号风险感知

业务风险中最常见的风险是用户账号风险，账号是业务开展的基础和入口，攻击者通常使用暴力破解、撞库等方式盗取账号。通过对账号的登录频次、登录来源、登录时间、登录地点等因素进行监控，可在账号遭受攻击的第一时间进行感知和阻断，防止风险的进一步发展。

4．行为风险感知

业务风险与传统的网络安全风险、计算机病毒风险的最显著差别是业务风险在用户行为上的表征，用传统的识别方式来看单个操作可能都是合法的，但是综合起来看整体的行为就会发现不合法之处。比如在互联网电商中常见的“薅羊毛”行为，单独看每个账号、每个设备的行为均是合法的，但是综合来看就产生了明显违反业务公平合法性的行为。针对行为风险常用的对抗手段有：

（1）异常操作识别感知

比如异常的转账、交易行为；每个正常用户使用 App 都有一定的规律，例如使用时间、登录地点、常用转账人等，一旦发现异常操作，需及时对用户进行二次认证。

（2）生物探针感知

真人使用移动设备时，设备传感器会采集到各种数据，而反观攻击者通常使用的模拟器、设备牧场等攻击设备则无法产生生物数据，或通过伪造产生类人的生物数据。生物探针就是通过获取生物数据来识别当前操作设备的是否是真人。

五、移动金融应用安全前景展望

（一）安全政策频出，移动应用安全与基础设施安全齐头并进

移动金融服务是架构在各种基础设施上的，我们谈移动金融应用安全，其实谈得更多的是架构在基础设施上的各种移动应用服务的安全。即将实施的《等保 2.0》与刚刚颁布的《密码法》都在强调行业基础设施与整体安全的重要性。未来的网络风险必然是数据化、智能化与团伙化，金融机构面临的不在是单一的攻击威胁。移动金融业务的安全防御也不能只是防范移动应用的风险，而是要对风险进行关联、群体特征进行关联，实现风险关联和传播分析，以应对更多未知威胁挑战。移动金融安全的发展需要服从国家安全战略，移动应用安全厂商与基础安全厂商各方需做好在产业链中的定位，发挥自身优势，共同为移动金融安全提供技术支撑。

（二）合规升级合法，移动金融应用隐私数据安全市场火热

金融机构尤其是支付企业过往出现用户隐私数据泄露事件，由于法律体系不够完善，无法对发生数据泄露的企业、机构、个人进行处罚。2019 年 10 月 25 日，最高人民法院、最高人民检察院联合发布《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助

信息网络犯罪活动等刑事案件适用法律若干问题的解释》，强调泄露500 条以上征信信息、财产信息的情节为“造成严重后果”；泄露其他可能影响人身、财产安全的用户信息五千条以上的情节为“造成严重后果”。在已知的数据泄露案件中泄露数据很少低于百万条，以该条的规定和目前的形势来看，几乎是只要发生数据泄露就属于“造成严重后果”。监管加强的同时给行业创新提供了动力，几乎所有安全厂商都陆续推出隐私数据保护方面的相关产品。移动金融应用作为目前首选的业务载体，如何规避终端数据泄露风险、保障用户金融信息安全成为每家机构信息安全建设的重要组成部分，个人信息合规测评、隐私数据加固成为市场热点。

（三）感知技术升级，驱动安全业务智能创新

传统的软、硬件漏扫工具和问题处理技术目前已无法满足移动互联网环境下的安全需求。金融机构需要充分认识到大数据环境下威胁数据主导安全业务的必要性，将网络态势监测、大数据分析技术越来越多地应用于企业实际工作当中，主动发现移动应用存在的漏洞、主动发现运行过程当中的风险，进而启用适当的防御手段。未来以感知为核心的主动防御架构将成为移动金融应用安全管理的业务新模式。通过对于移动金融应用的用户行为、设备状态、网络环境等资源的实时监测获取分析数据，根据大数据分析技术来进行应用业务安全状态的研究判断，通过全流程节点的响应措施来实现威胁防控与精确响应。

附录 A　金融行业 App 地域分布表

序号	省份	App 数量	占比
1	广东	39464	29.60%
2	湖北	28400	21.30%
3	北京	16857	12.64%
4	江苏	9292	6.97%
5	上海	8516	6.39%
6	浙江	5716	4.29%
7	福建	4135	3.10%
8	湖南	2667	2.00%
9	四川	1909	1.43%
10	河南	1620	1.22%
11	山东	1579	1.18%
12	陕西	1279	0.96%
13	安徽	1079	0.81%
14	重庆	916	0.69%
15	河北	766	0.57%
16	江西	755	0.57%
17	云南	674	0.51%
18	辽宁	648	0.49%
19	贵州	461	0.35%

序号	省份	App 数量	占比
20	天津	442	0.33%
21	山西	437	0.33%
22	吉林	378	0.28%
23	广西	362	0.27%
24	黑龙江	346	0.26%
25	内蒙古	326	0.24%
26	海南	323	0.24%
27	新疆	232	0.17%
28	甘肃	205	0.15%
29	宁夏	76	0.06%
30	西藏	47	0.04%
31	台湾	40	0.03%
32	香港	35	0.03%
33	青海	30	0.02%
34	澳门	10	0.01%

数据来源：北京智游网安科技有限公司（爱加密）

附录 B　金融行业 App 分类逻辑及典型应用

序号	金融分类	分类逻辑	应用名称	版本号	网页链接
1	消费金融	仅面向消费者个人的借贷类应用	云科贷管家	1.0.30L5-XW	https://www.cr173.com/soft/505642.html
			吉利贷	1.5.1	https://www.aomeng.net/ruanjian/1887.html
2	彩票	博彩类应用	快 3	v1.6.2	https://sj.qq.com/myApp/detail.htm?apkName=com.lottery.tisscasdqpcdd
			ok 彩票	v2.5.5	https://www.anfensi.com/down/261210.html
3	投资理财	可进行投资或理财的移动应用，包括贵金属、黄金、白银、期货、原油等专业应用。	现货黄金投资平台	v1.0	http://www.pc6.com/az/418348.html
			朵朵理财	1.32	http://as.sogou.com/detail?pid=34&cid=40&docid=-8315643452636688795
4	P2P 金融	除消费者个人外，还包括面向小微企业、个体工商户等其他集体的借贷类应用	宜人贷手机版	1.0	https://www.zuiben.com/a_soft/124275.html
			猪金贷	v1.0.0	https://sj.qq.com/myApp/detail.htm?apkName=com.zhujindai.p2p.ad3
5	证券	证券公司主持开发可用于证券投资理财活动的应用软件	平安证券	6.20.0.1	https://Appstore.huawei.com/App/C10308911
			国金太阳	5.00.01	http://www.shouji56.com/soft/GuoJinZheng_80379/
6	财务管理	记账、收银、资产管	易收钱 App	1.0	https://www.zuiben.com/a_soft/36445.html

序号	金融分类	分类逻辑	应用名称	版本号	网页链接
		理类应用	传贝收银	3.0.8	https://sj.qq.com/myApp/detail.htm?apkName=com.wuzhenpay.App.chuanbei
7	股票	专业炒股软件	股票配资	1.0	https://www.wandoujia.com/Apps/com.myApp.gppeizis
			牛股王股票	1.0	https://www.zuiben.com/a_soft/1917.html
8	保险	提供各种保险产品的应用	人保财险 App	1.0	https://www.zuiben.com/a_soft/27821.html
			中国人寿 App	1.0	https://www.zuiben.com/a_soft/35312.html
9	银行	银行主持开发或为银行开发的用于各类银行服务的应用	龙里国丰村镇银行	1.4	http://www.xz7.com/downinfo/381780.html
			工银融 e 行客户端	1.0	https://www.zuiben.com/a_soft/8492.html
10	数字货币	专注虚拟货币交易投资服务的应用	FOTA 方图 App	1.0.0	http://www.aiskycn.com/az/1099977.html
			币峰 befong	1.0.0	https://www.11773.com/App/bifengApp/
11	外汇	专注外汇交易投资应用	外汇宝软件	1.0	https://www.zuiben.com/a_soft/37276.html
			MT4 外汇中文版	v1.0.4	https://sj.qq.com/myApp/detail.htm?apkName=cc.yswebportal.ahpt.m
12	互联网第三方支付	仅包含互联网支付（商户收银等未纳入此范围）	壹钱包	V4.3.1	http://www.289.com/azrj/279183.html
			易生支付	2.4.4	http://os-android.liqucn.com/rj/

序号	金融分类	分类逻辑	应用名称	版本号	网页链接
					288175.shtml
13	信托	专业信托公司开发用于帮助客户进行理财投资的应用软件	华润信托	1.8.1	https://Appstore.huawei.com/App/C100127841
			钱景信托管家	1.0.0.2	https://os-android.liqucn.com/rj/302384.shtml

附录 C　Top10 高危漏洞说明

序号	恶意程序	检测目的	类型说明
1	Janus 漏洞	检测应用是否存在 Janus 漏洞。	Google 在 2017 年 12 月发布的安卓系统安全公告中披露“Janus”漏洞（漏洞编号：CVE-2017-13156）。该漏洞可以让攻击者绕过安卓系统的 signature scheme V1 签名机制，直接对 App 进行篡改。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。攻击者可以在正常应用中植入恶意代码，可替代原有的 App 做下载、更新。安装这些仿冒 App 后，攻击者可以窃取用户的账号、密码等敏感信息；或者植入木马病毒，导致手机被 ROOT，甚至被远程操控。
2	WebView 远程代码执行漏洞	检测应用是否存在 WebView 远程代码执行漏洞。	Android API level 17 以及之前的版本，由于程序没有正确限制使用 addJavascriptInterface 方法，远程攻击者可通过使用 Java Reflection API 利用该漏洞执行任意 Java 对象的方法。通过 addJavascriptInterface 给 WebView 加入一个 JavaScript 桥接接口，JavaScript 通过调用这个接口可以直接与本地的 Java 接口进行交互。导致手机被安装木马程序，发送扣费短信，通信录或者短信被窃取，甚至手机被远程控制。
3	动态注册 Receiver 风险	检测应用是否存在动态注册 Receiver 风险。	BroadcastReceiver 组件可动态注册，即在代码中使用 registerReceiver()方法注册 BroadcastReceiver，只有当 registerReceiver()的代码执行到了才进行注册，取消时则调用 unregisterReceiver()方法。但 registerReceiver()方法注册的 BroadcastReceiver 是全局的并且默认可导出的，如果没有限制访问权限，可以被任意外部 App 访问，向其传递 Intent 来执行特定的功能。因此，动态注册的 BroadcastReceive 可能导致拒绝服务攻击、App 数据泄漏或是越权调用等风险。

序号	恶意程序	检测目的	类型说明
4	WebView 明文存储密码漏洞	检测应用的 WebView 组件中是否使用明文保存用户名及密码。	WebView 组件默认开启了密码保存功能，会提示用户是否保存密码，当用户选择保存在 WebView 中输入的用户名和密码，则会被明文保存到应用数据目录的 databases/webview.db 中。攻击者可能通过 root 的方式访问该应用的 WebView 数据库，从而窃取本地明文存储的用户名和密码。
5	IP 检测	检测应用代码中是否硬编码了 IP 地址。	将 IP 地址硬编码在代码中，使得变量不易改变，一旦服务器主机 IP 地址变化，对应也要把代码中所有变化的硬编码的 IP 地址修改，维护起来比较繁琐。
6	Java 代码加壳检测	检测应用程序中 Java 代码是否加壳。	Java 代码加壳即在 Java 代码外面包裹上另外一段代码，保护里面的 Java 代码不被非法修改或反编译。Java 文件未进行加壳保护，可能面临被反编译的风险。攻击者通过 baksmali/apktool/dex2jar 等反编译工具得到应用程序的代码，导致代码逻辑泄露、重要数据加密代码逻辑泄露等。
7	数据库注入漏洞	检测应用是否存在数据库注入漏洞。	Content Provider 组件是 Android 应用的重要组件之一，管理对数据的访问，主要用于不同的应用程序之间实现数据共享的功能。SQLite 数据库和文件数据是 Content Provider 的数据源。当 Content Provider 的数据源是 SQLite 数据库并且 Provider 组件暴露时（export 属性为“true”），如果 query( )中使用拼接字符串形式构造的 SQL 语句去查询底层 SQLite 数据库时，则容易发生 SQL 注入。攻击者可以利用此漏洞攻击应用的本地数据库，导致存储的敏感数据信息被查询泄露，例如用户名、密码等，或者产生查询异常导致应用崩溃。
8	H5 文件加固检测	检测应用资源文件中的 H5 文件是否加固。	应用中如果存在明文存储的 H5 资源文件，则会泄露页面基本布局和一些重要的信息，如登录界面、支付界面等。攻击者可篡改 H5 资源文件，可能植入钓鱼页面或者恶意代码，导致用户账号、密码、支付密码等敏感信息泄露。更有甚者，通过 H5 代码暴露相关活动的业务逻

序号	恶意程序	检测目的	类型说明
			辑，可能被黑产团队用来刷红包、薅羊毛等，造成经济损失。
9	RSA 加密算法不安全使用风险	检测应用中是否存在 RSA 加密算法不安全使用情况。	RSA 加密算法是一种非对称加密算法，是第一个既能用于数据加密也能用于数字签名的算法。当其密钥长度过短，通常认为长度小于 512 位时，就会存在较高的被破解风险；没有使用正确的工作模式和填充方式，将会存在重放攻击的风险。因 RSA 加密算法不安全使用造成的加密方法失效，可能造成客户端隐私数据泄露、加密文件破解、传输数据被获取、中间人攻击等后果，导致用户敏感信息被窃取。
10	权限滥用风险	检测应用中是否存在权限滥用情况。	权限是一种安全机制，主要用于限制应用程序内部某些具有限制性特性的功能使用以及应用程序之间的组件访问。Android 通过在 AndroidManifest.xml 中增加权限来控制限制性功能的使用和组件访问。权限滥用是指应用权限开放过多、自定义权限限制不严格，导致攻击者利用应用权限可以使用某些特殊的功能，如拨打电话、访问摄像头、利用麦克风录音、编写并植入木马等。可能导致隐私数据泄露，钓鱼扣费等风险。

附录 D　App 恶意程序类型解释

序号	恶意程序	类型说明
1	流氓行为	这类应用的特征是用户不在本应用界面内时依然对操作系统或其他应用造成严重影响用户体验的影响，包括但不限于在用户未授权的情况下，在桌面弹出广告窗口等。
2	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。
3	信息窃取	这类病毒会窃取用户隐私信息包括用户的手机号，通讯录等信息，造成短信、GPS 定位、联系人信息等敏感信息被窃取。
4	恶意传播	自动通过复制、感染、投递、下载等方式将自身的衍生物或其它恶意代码进行扩散的恶意行为，使用户蒙受数据流量损失和成为恶意程序的传播者。
5	诱骗欺诈	自动通过伪造、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恶意行为，产生的危害后果是通过欺骗使用户利益受损失。
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行为；其危险后果主要表现为系统破坏，导致用户手机无法正常使用，损害用户利益。
7	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。 此类危险具有恶意扣费属性，导致用户直接经济损失。
8	远程控制	是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 ，具有远程控制属性;受此类病毒感染的个人手机会成为控制者的肉鸡，完全被对方控制。

附录 E　受到恶意程序感染的 App 地域分布表

序号	省份	病毒 App 数量	病毒感染率（/当地 App 总量）	病毒数量占比
1	江苏	3092	33.28%	37.63%
2	广东	2478	6.28%	30.16%
3	北京	1032	6.12%	12.56%
4	湖北	629	2.21%	7.65%
5	上海	305	3.58%	3.71%
6	浙江	154	2.69%	1.87%
7	四川	68	3.56%	0.83%
8	福建	62	1.50%	0.75%
9	湖南	58	2.17%	0.71%
10	陕西	52	4.07%	0.63%
11	山东	39	2.47%	0.47%
12	云南	31	4.60%	0.38%
13	安徽	29	2.69%	0.35%
14	河南	28	1.73%	0.34%
15	贵州	20	4.34%	0.24%
16	江西	19	2.52%	0.23%
17	重庆	18	1.97%	0.22%
18	内蒙古	17	5.21%	0.21%

序号	省份	病毒 App 数量	病毒感染率（/当地 App 总量）	病毒数量占比
19	河北	13	1.70%	0.16%
20	天津	8	1.81%	0.10%
21	山西	8	1.83%	0.10%
22	吉林	7	1.85%	0.09%
23	广西	6	1.66%	0.07%
24	甘肃	6	2.93%	0.07%
25	新疆	4	1.72%	0.05%
26	辽宁	4	0.62%	0.05%
27	黑龙江	4	1.16%	0.05%
28	台湾	2	5.00%	0.02%
29	西藏	1	2.13%	0.01%
30	青海	1	3.33%	0.01%
31	宁夏	1	1.32%	0.01%
32	海南	1	0.31%	0.01%
33	澳门	1	10.00%	0.01%

数据来源：北京智游网安科技有限公司（爱加密）

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62304911

传真：010-62300264

网址：www.caict.ac.cn