CAICT 中国信通院

爱加密

数字金融 App 安全观测报告

（2020 年）

中国信息通信研究院安全研究所

北京智游网安科技有限公司

2020年10月

版权声明

本报告版权属于中国信息通信研究院，并受法律保护。转载、摘编或利用其它方式使用本报告文字或者观点的，应注明“来源：中国信息通信研究院”。违反上述声明者，本院将追究其相关法律责任。

CAICT 中国信通院

前　言

新型冠状病毒肺炎疫情发生以来，为疏解因疫情冲击造成线下业务难以开展的难题，金融机构大力推进数字化转型，从而促进了数字金融 App 的进一步应用和普及。然而，App 在给大众生活带来巨大便利的同时，也带来了相应的安全隐患。

为了进一步贯彻落实习近平总书记网络强国的战略思想，助力金融行业的平稳安全发展，中国信息通信研究院金融科技安全实验室联合北京智游网安科技有限公司组成研究团队，在有关部门的指导下，依据相关法律法规和文件精神，对基于安卓系统的数字金融 App 的安全现状进行了观测分析，形成本报告。

本报告研究团队升级了《2019 金融行业移动 App 安全观测报告》的技术手段和分析维度，经过持续半年的观测，对 2020 年上半年数字金融 App 存在的高危漏洞、恶意程序、使用 SDK 引入风险以及缺乏有效安全加固等四类主要风险变化情况进行了对比分析，并在工业和信息化部《关于开展纵深推进 App 侵害用户权益专项整治行动的通知》等顶层设计的文件精神与工作指南的指导下，围绕数字金融 App “侵害用户权益” 等问题进行了抽样检测与安全研究。

本报告旨在通过对数字金融 App 进行持续、全面、客观的安全观测与风险分析，为相关监管部门、App 开发运营者、应用分发平台和用户提供数字金融 App 安全工作的思路与建议，共同促进数字金融 App 的网络安全生态体系建设。

目 录

一、数字金融 App 安全观测背景.....1
（一）移动应用安全的政策背景.....1
（二）数字金融 App 的安全现状.....3
二、数字金融 App 安全观测结果.....5
（一）观测对象分布情况.....5
（二）安全风险对比分析.....6
三、数字金融 App 侵害用户权益专项检测结果.....15
（一）违规处理用户个人信息.....16
（二）设置障碍、频繁骚扰用户.....17
（三）应用分发平台责任落实不到位.....20
四、数字金融 App 的安全工作思路与建议.....21
（一）App 相关监管部门.....21
（二）App 开发运营者.....21
（三）App 应用分发平台.....22
（四）App 用户.....22
附录 A　数字金融 App 地域分布表.....24
附录 B　Top10 高危漏洞说明.....25
附录 C　App 恶意程序类型说明.....27
附录 D　受恶意程序感染的数字金融 App 地域分布表.....28

CAICT 中国信通院

图 目 录

图 1　App 区域分布 Top10 5
图 2　不同细分领域 App 数量及占比 6
图 3　金融行业 App 各等级漏洞情况 6
图 4　不同细分领域高危漏洞 App 占比情况 7
图 5　高危漏洞类型分布 Top10 8
图 6　App 恶意程序类型占比情况 9
图 7　受到恶意程序感染的 App 区域分布 Top10 10
图 8　各细分领域受到恶意程序感染的 App 分布情况 10
图 9　各细分领域受到恶意程序感染的 App 占比情况 11
图 10　不同 SDK 个数区间对应的 App 分布情况 12
图 11　金融行业 App 使用的各类 SDK 占比情况 12
图 12　不同加固厂家服务的 App 分布 13
图 13　加固 App 地域分布 Top10 14
图 14　各金融细分领域 App 加固分布情况 14
图 15　抽样 App 检测发现问题数量占比 15
图 16　某保险类 App 超范围收集个人信息 17
图 17　某银行类 App 频繁索取权限 18
图 18　某保险类 App 过度索取权限 19
图 19　某银行类 App 强制索取权限 20
图 20　某应用分发平台收录的某银行类 App 存在恶意程序 20

CAICT 中国信通院

一、数字金融 App 安全观测背景

（一）移动应用安全的政策背景

近年来，随着新一代信息技术的蓬勃发展，网络空间在促进社会和经济发展，保障和改善民生方面发挥着越来越重要的作用，网络空间安全在迎来前所未有的发展机遇的同时，也面临着日趋严峻的风险挑战。自十八大以来，以习近平同志为核心的党中央和国务院高度重视网络安全，并形成网络强国的战略思想。习近平总书记指出，“没有网络安全就没有国家安全”，将网络安全的重要性提升至国家战略层面。

2019 年，中央网信办、工业和信息化部、公安部、国家市场监督管理总局等行业监管部门重拳出击，对 App 违法违规收集使用个人信息行为采取“零容忍”政策，成立专项组开展专项治理行动，陆续“点名”几个批次的违规违法 App，责令违规 App 进行整改，体现了监管部门对综合治理 App 网络安全的决心。

2019 年 11 月，中国人民银行发布了《关于发布金融行业标准 加强移动金融客户端应用软件安全管理的通知》（银发〔2019〕237 号），并随通知发布了《移动金融客户端应用软件安全管理规范》，要求各金融机构提升客户端软件的安全防护能力，加强个人金融信息保护，提高风险监测能力，健全投诉处理机制等。

2019 年 12 月，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局四个部门联合印发《App 违法违规收集使

用个人信息行为认定方法》，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依据，为 App 运营者自查自纠和网民社会监督提供指引。

2020 年 2 月，中国人民银行发布了《个人金融信息保护技术规范》，要求与个人金融信息相关的客户端应用软件及应用软件开发工具包（SDK）应符合《移动金融客户端应用软件安全管理规范》《网上银行系统信息安全通用规范》客户端应用软件有关安全技术要求，并在上线前进行安全评估。

2020 年 4 月，中国人民银行办公厅发布了《关于开展金融科技应用风险专项摸排工作的通知》（银办发〔2020〕45 号），要求各地人民银行分支机构及相关监管机构依据相关法律制度、标准规范开展专项摸排工作，“移动金融客户端应用软件”成为主要摸排对象之一。

2020 年 7 月，工业和信息化部印发《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），决定深入推进技管结合，加强监督检查，通过专项整治行动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。

2020 年 9 月，全国信息安全标准化技术委员会先后发布《移动互联网应用程序（App）系统权限申请使用指南》《移动互联网应用程序（App）个人信息保护常见问题及处置指南》等一系列网络安全标准实践指南，进一步帮助 App 运营者规范 App 申请使用系统权限行为，采取相应措施持续提升 App 个人信息保护水平，为用户营造

绿色、安全、可信的 App 使用环境。

App 网络安全及个人信息保护相关政策法规和标准规范的密集出台，体现了政府相关部门对于保障 App 网络安全的重视和治理 App 安全风险的决心，也侧面反映出当前 App 网络安全面临的严峻形势。

（二）数字金融 App 的安全现状

近年来，随着移动互联网的快速发展和移动支付的广泛普及，移动互联网应用程序（App）已经深入应用到大众生活的方方面面，并发挥着不可或缺的重要作用。据中国互联网络信息中心（CNNIC）发布的第 46 次《中国互联网络发展状况统计报告》显示，截至 2020 年 6 月，我国手机网民规模已达 9.32 亿，网民使用手机上网的比例高达 99.2%。

新型冠状病毒肺炎疫情发生以来，为保证国民经济运行平稳发展，相关金融监管部门多次强调加强线上业务服务，大力倡导金融机构业务数字化转型，鼓励金融机构引导企业和个人客户通过互联网、App 等线上方式办理金融业务，以疏解因疫情冲击造成线下业务难以开展的难题，从而促进了金融行业 App 的进一步应用和普及。然而，App 在给大众生活带来巨大便利的同时，也带来了相应的安全隐患。

近两年，App 安全已成为多方关注的重点，各监管部门正加紧完善 App 网络安全相关的法律法规和标准规范体系，对企业监督执法力度持续加强，但数字金融 App 的安全形势依然严峻。某些第三方应用分发平台管理存在漏洞，对 App 上线审核不规范的情况时有发生；部分金融行业 App 开发运营者法律意识和安全意识淡薄，未对

App 进行安全加固，或者技术手段落后，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，导致 App 存在高危漏洞或恶意程序等风险；部分 App 用户缺乏安全意识，未主动采取安全防护，或存在不安全的使用习惯，往往会带来信息泄露等安全隐患。据国家互联网应急中心（CNCERT）发布的《2019 年中国互联网网络安全报告》显示，2015-2019 年移动互联网恶意程序样本数量持续高速增长，2019 年新增移动互联网恶意程序样本数量为 279 万余个，安卓平台用户成为最主要的攻击对象。

为了进一步贯彻落实习近平总书记网络强国的战略思想，助力新冠肺炎疫情影响下金融行业的平稳安全发展，中国信息通信研究院金融科技安全实验室组织对基于安卓系统的数字金融 App 的安全情况进行了观测分析，形成本报告。报告对 2020 年上半年数字金融 App 的安全风险问题现状及变化趋势进行了重点分析和研究，并在工业和信息化部《关于开展纵深推进 App 侵害用户权益专项整治行动的通知》等顶层设计的文件精神与工作指南的指导下，围绕数字金融 App “侵害用户权益”等问题进行了抽样检测与安全研究，为金融行业相关监管部门、App 开发运营者、应用分发平台和 App 用户掌握金融 App 安全态势和评估金融 App 安全风险提供参考。

二、数字金融 App 安全观测结果

（一）观测对象分布情况

截至 2020 年 6 月 30 日，报告团队对从 842 个安卓应用市场中收录的 29065 款金融行业 App 进行了安全观测。

从观测对象的地域分布来看，有 27883 款可以明确所归属的省份，全国 34 个省级行政区均有金融行业 App 发布（若 App 无运营、无开发主体，则按其应用分发平台所属区域确定其归属省份，详细数据参见附录 A），平均每个省份含金融行业 App 820 款。金融行业 App 数量在地域分布显著不均，广东、湖北和北京分别以 35.21%、21.91%和 8.37%的高占比排名前三，而占比最少的西藏、宁夏、青海等 6 省份总占比仅有 0.37%，具体数据如图 1 所示。

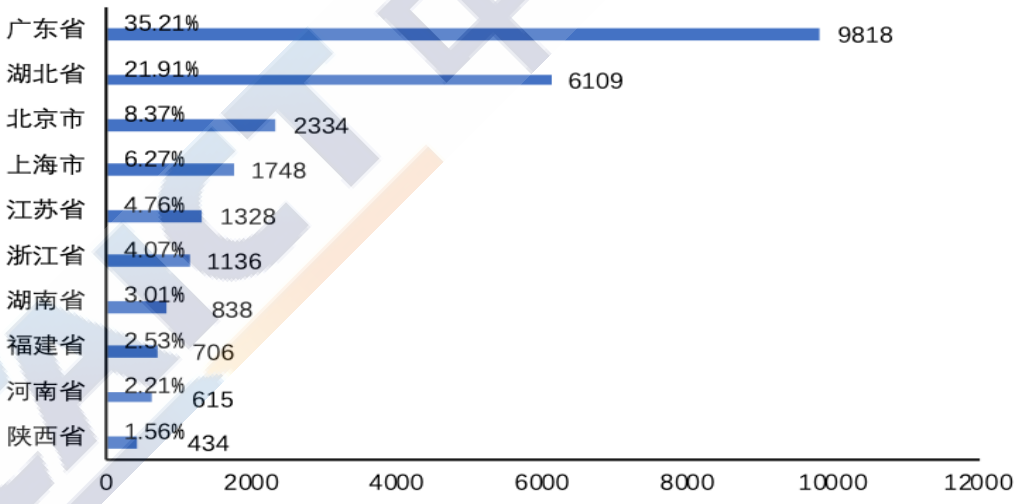


图 1　App 区域分布 Top10

从金融行业 App 细分领域来看，投资理财类 App 数量最多，占观测总数的 46.04%；消费金融类 App 排名第二，占比 17.15%；证券类 App 排名第三，占比 8.97%。具体数据如图 2 所示。

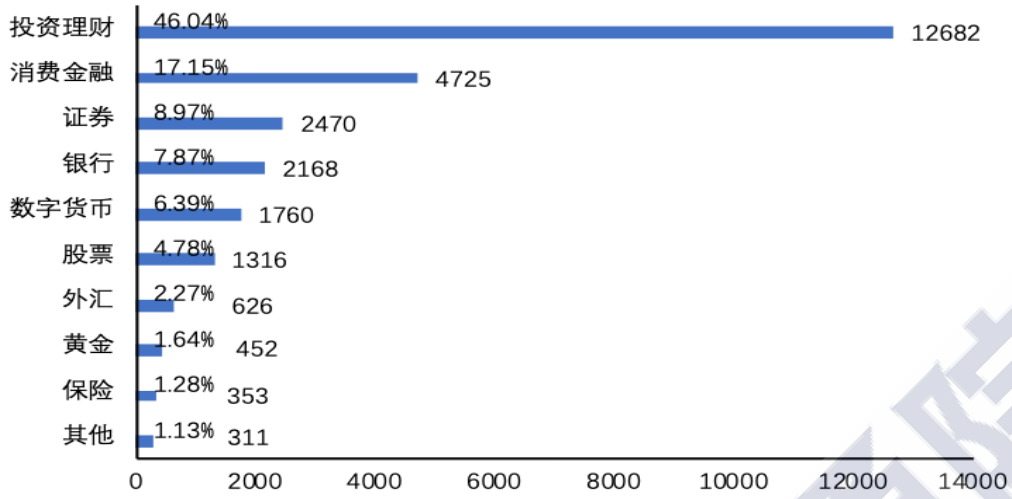


图 2　不同细分领域 App 数量及占比

（二）安全风险对比分析

1．高危漏洞对比分析

报告团队对 25392 款金融行业 App 进行扫描，共计检测出 1861160 条漏洞记录，涉及 63 种漏洞类型，其中有 21 种为高危漏洞；共有 22884 款 App 存在不同程度的安全漏洞，占比由 2019 年的 73.23%提升至 90.12%，且高、中、低各等级安全漏洞占比均有明显增长，具体数据如图 3 所示。

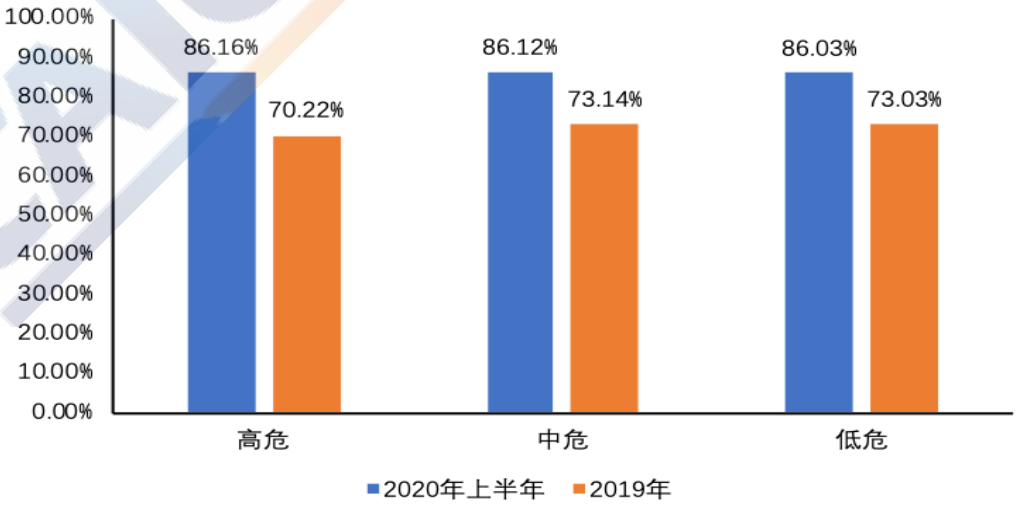


图 3　金融行业 App 各等级漏洞情况

从 App 分类角度来看，证券类、外汇类 App 的高危漏洞问题较为突出，存在高危漏洞 App 的比例高达 96%以上。与 2019 年观测数据相比，银行类、消费金融类 App 的高危漏洞占比增长显著，而信托类 App 的占比则有明显下降，具体数据如图 4 所示。

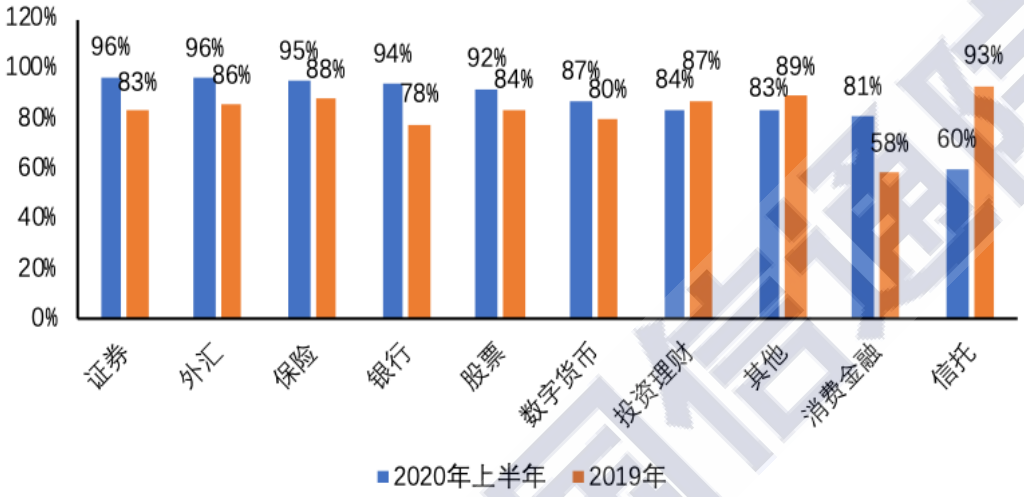


图 4　不同细分领域高危漏洞 App 占比情况

从高危漏洞类型来看，2020 年上半年的高危漏洞 Top10 与 2019 年的观测结果相比变化不大（Top10 高危漏洞介绍及危害说明参见附录 B），其中，系统键盘使用风险漏洞、ZipperDown 漏洞和 SO 文件加固检测漏洞首次出现在 Top10，并分别占据了第一、第二和第六位。存在这三种高危漏洞的 App 数量分别占据观测总数的 78.52%、65.58%和 34.90%，具体数据如图 5 所示。系统键盘使用风险是移动用户在 App 的登录、注册、支付等敏感界面输入信息时，使用了不安全的系统键盘，存在数据被拦截与监听的风险，容易导致账号、密码等敏感数据泄露，从而成为当前 App 面临的主要安全问题。

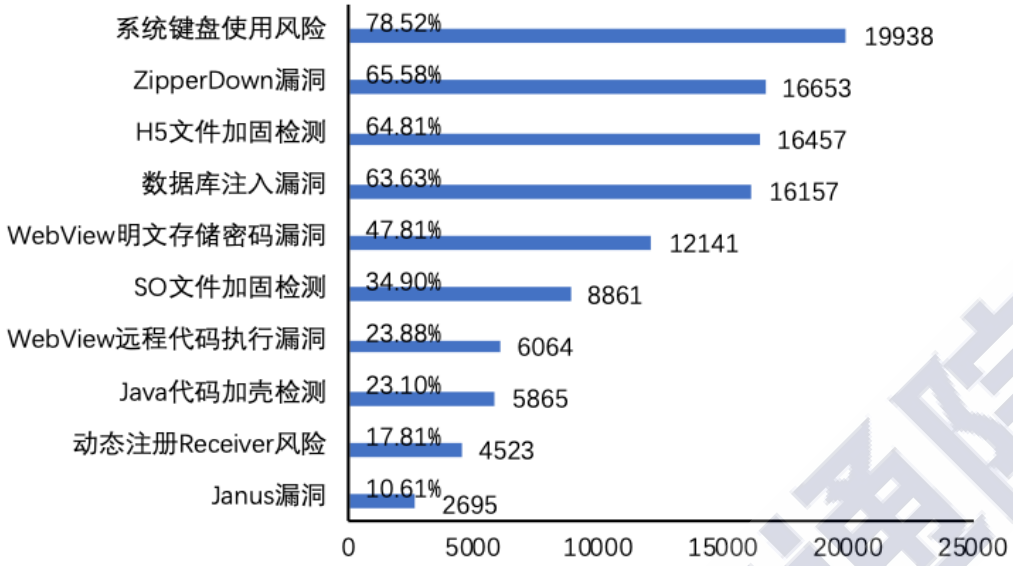


图 5　高危漏洞类型分布 Top10

2．恶意程序对比分析

报告团队使用恶意程序检测系统对 29065 款金融行业 App 进行了安全检测，共发现有 8563 款 App 存在恶意程序，感染率高达 29.46%。检测发现的恶意程序主要涉及流氓行为、隐私窃取、恶意扣费、资费消耗、恶意传播、诱骗欺诈、系统破坏和远程控制等多种恶意行为，对移动用户的个人信息及财产安全带来了巨大威胁。

从恶意程序类型来看（App 恶意程序类型说明参见附录 C），在检测发现的恶意程序中，具有流氓行为的恶意程序极为突出，占恶意程序总数的 93.83%，这类恶意程序对系统没有直接损害，但会严重影响用户体验，包括但不限于在用户不知情或未授权的情况下，自动捆绑安装的；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、卸载、删除的；执行用户未授权的其他操作等。具有隐私窃取行为的恶意程序占比 5.41%，这类恶意程序会在用户不知情或未授权的情况下窃取用户隐私信息，包括用户的手机号、通讯录、短

信内容、通话记录、通话内容、地理位置、本机已安装软件等信息。与 2019 年的观测情况相比，流氓行为类恶意程序感染率增长明显，隐私窃取类和恶意传播类恶意程序感染率有所下降。具体数据如图 6 所示。

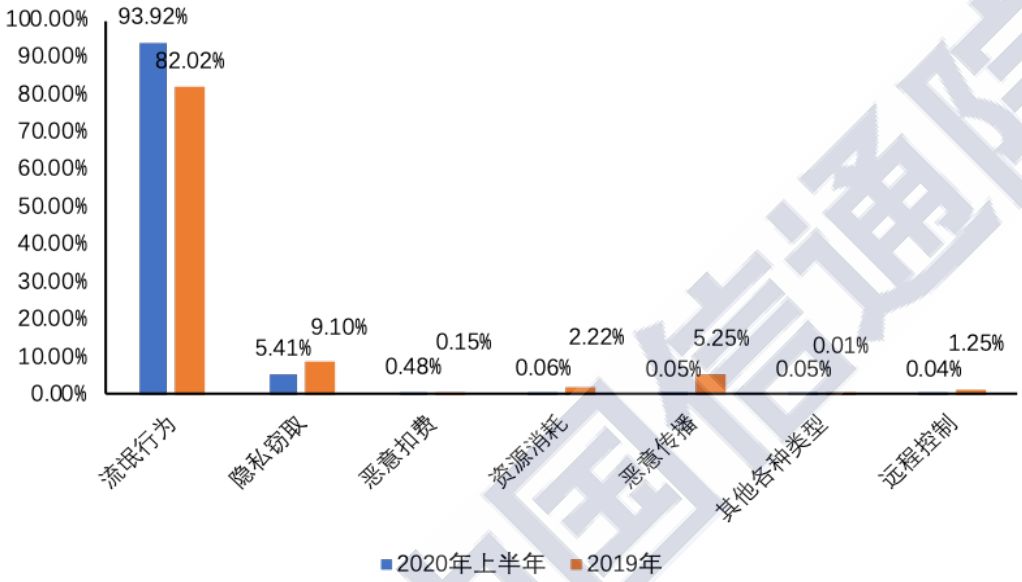


图 6　App 恶意程序类型占比情况

从地域分布来看，恶意程序感染的 App 分布在除宁夏回族自治区外的 33 个省级行政区（受恶意程序感染的数字金融 App 地域分布数据参见附录 D）。其中，广东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 45.21%；湖北其次，占比 17.59%；江苏排行第三，占比为 12.73%。受到恶意程序感染的 App 数量最多的十大省份占据了感染 App 总数的 96.72%，如图 7 所示。

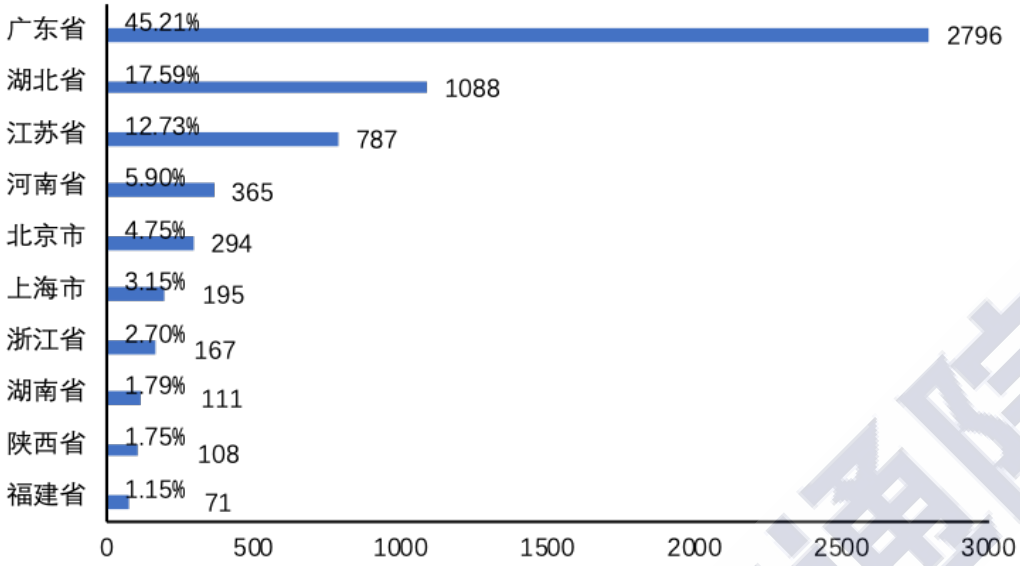


图 7　受到恶意程序感染的 App 区域分布 Top10

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投资理财类、消费金融类和数字货币类，分别有 3586 款、1475 款、543 款 App 已经受到恶意程序感染。与 2019 年观测数据相比，这三类 App 感染恶意程序的占比均有大幅提升，如图 8、图 9 所示。

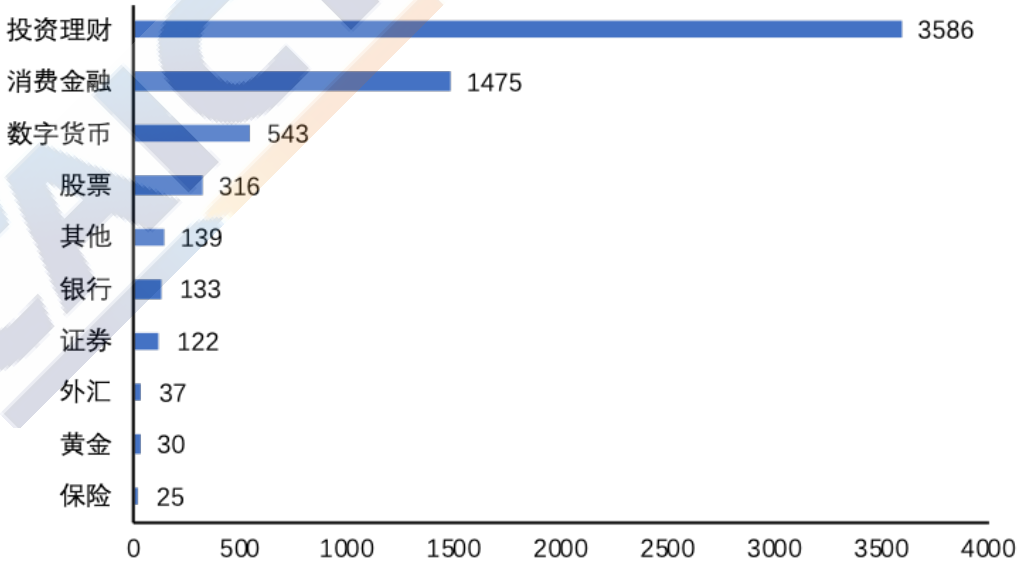


图 8　各细分领域受到恶意程序感染的 App 分布情况

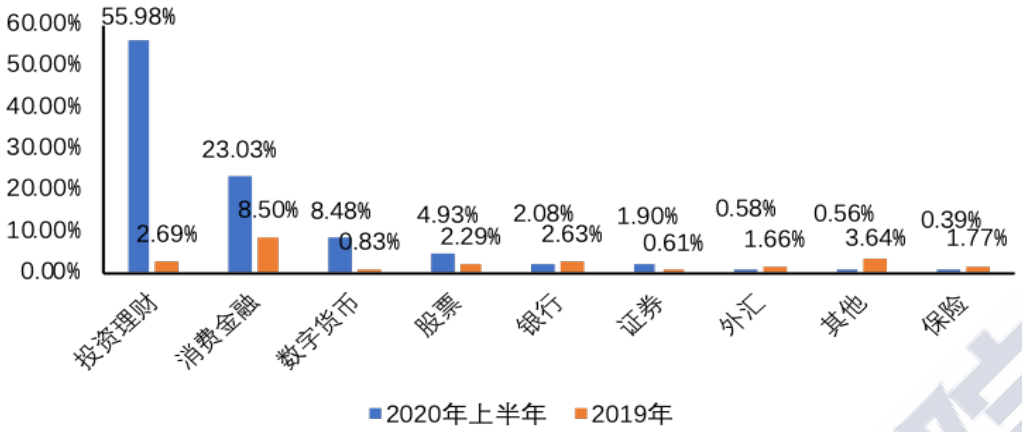
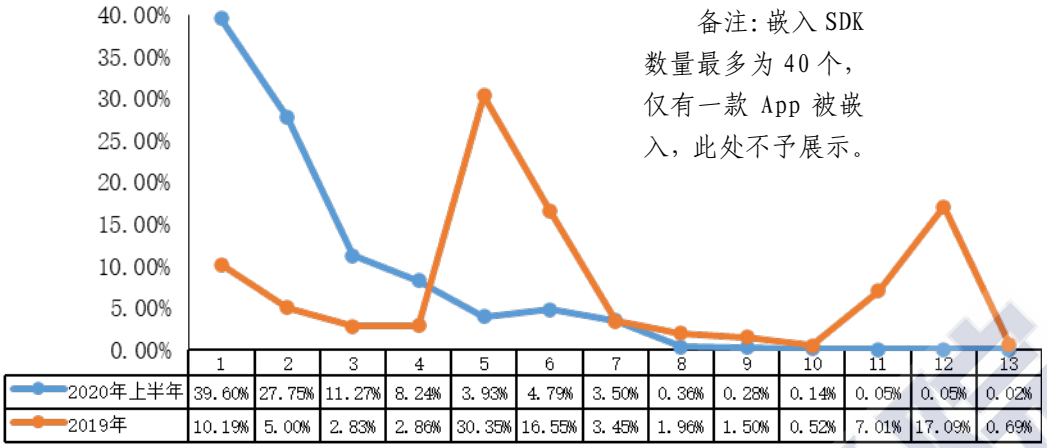


图 9　各细分领域受到恶意程序感染的 App 占比情况

3．使用 SDK 对比分析

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（Software Development Kit 的缩写，即“软件开发工具包”）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、个人信息泄露等安全问题，进而给嵌入 SDK 的 App 带来相应的安全隐患。自 2019 年下半年起，不论是立法动态还是监管角度，均将 SDK 违法违规作为审查的重点之一。

报告团队观测发现，有 6435 款金融行业 App 嵌入了第三方 SDK，占观测总数的 22.14%。这些 App 共嵌入 22818 个第三方 SDK，平均每款 App 嵌入 3.5 个，其中 39.6%的 App 只嵌入了 1 个 SDK，仅有 13.15%的 App 嵌入了 5 个及以上的 SDK。从 2019 年的观测数据可以看出，嵌入 5 个及以上 SDK 的 App 占比高达 79.12%。可见，2020 年上半年，金融行业 App 对 SDK 的使用明显减少，由嵌入第三方 SDK 引入的安全风险得到一定程度缓解。金融行业 App 第三方 SDK 使用情况如图 10 所示。



	1	2	3	4	5	6	7	8	9	10	11	12	13
2020年上半年	39.60%	27.75%	11.27%	8.24%	3.93%	4.79%	3.50%	0.36%	0.28%	0.14%	0.05%	0.05%	0.02%
2019年	10.19%	5.00%	2.83%	2.86%	30.35%	16.55%	3.45%	1.96%	1.50%	0.52%	7.01%	17.09%	0.69%

图 10　不同 SDK 个数区间对应的 App 分布情况

从 App 使用 SDK 的主要类型来看，金融行业 App 使用的排名前三的 SDK 分别是推送类、统计类和社交类，占比分别为 36.29%、22.48%和 13.92%；而音频类和广告类 SDK 在金融行业 App 的 SDK 使用占比仅有 1.18%和 0.22%。与 2019 年的观测数据相比，排名前三的 SDK 种类并无变化，但推送类 SDK 的占比大幅下降，统计类、社交类、框架类和地图类 SDK 的占比均有提升，相关类别 SDK 的安全性问题需要加强关注。具体数据如图 11 所示。

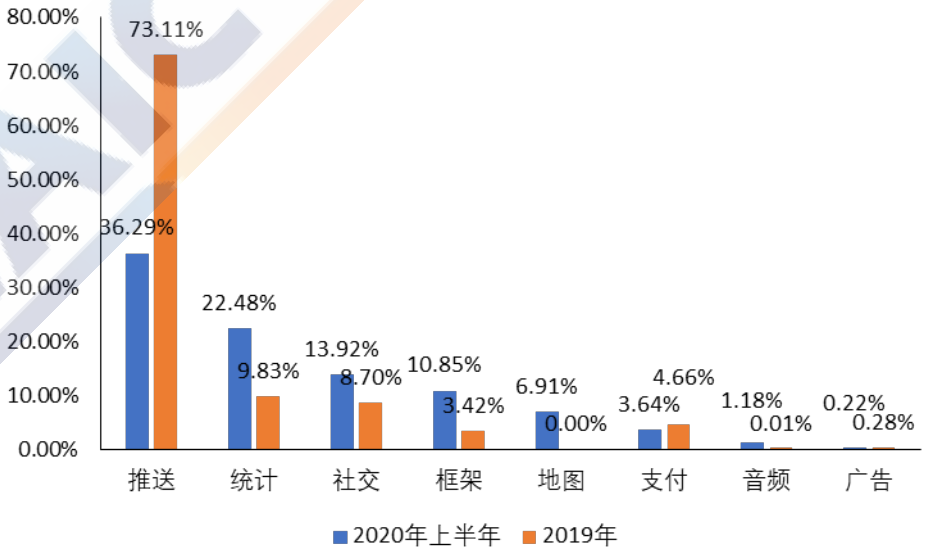


图 11　金融行业 App 使用的各类 SDK 占比情况

4. 安全加固对比分析

“安全加固”是维护 App 安全的重要防护手段，能够有效阻止对基于 Java 编写的安卓 App 的反汇编分析，进而降低 App 盗版、二次打包、注入等安全风险。经检测，共有 4580 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 15.75%。可见，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。

从 App 安全加固厂商的分布来看，金融行业 App 主要选择 360、腾讯、爱加密、梆梆、百度等 5 家安全服务商进行安全加固。其中，64.96%的金融行业 App 选择 360 加固平台进行安全加固；19.54%的金融行业 App 选择腾讯加固平台，其余约 15.50%的金融行业 App 选择其他厂商进行安全加固。加固厂家分布如图 12 所示。

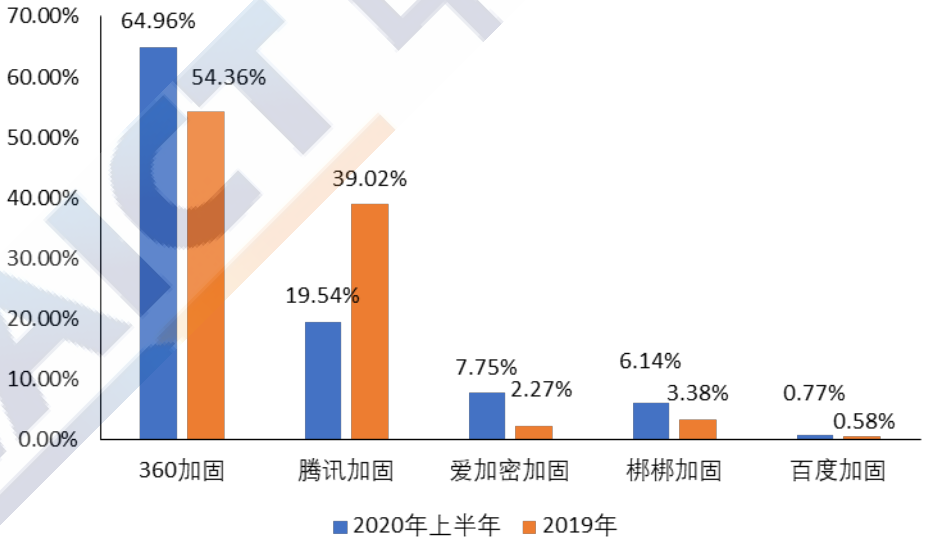


图 12　不同加固厂家服务的 App 分布

从加固 App 的地域分布来看，主要集中在广东省、北京市、上海市等经济发达地区，App 加固数量排名前十的省份占加固 App 总

数的 80%以上。分析各省份 App 加固比例可以发现，除台湾省、陕西省、湖南省、广东省、湖北省外，大部分省份的 App 加固比例均超过了行业整体加固比例 15.75%，其中河北省金融行业 App 加固比例最高，达到 50.22%。如图 13 所示。

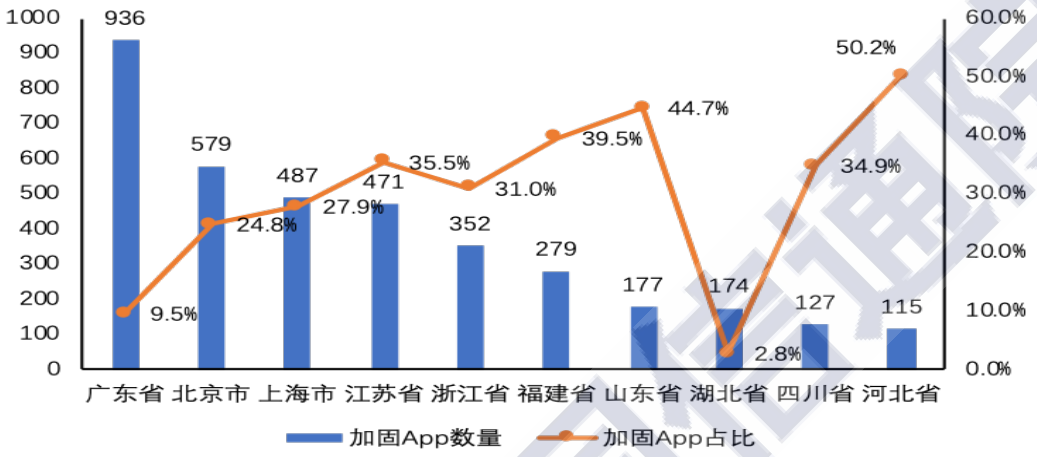


图 13　加固 App 地域分布 Top10

从加固 App 所属金融行业的主要细分领域分布来看，消费金融类、投资理财类和数字货币类 App 加固比例分别为 6.29%、10.44%和 13.92%，低于金融行业 App 平均加固比例。外汇类、银行类和黄金类 App 的开发者安全意识相对较强，加固比例位列前三，分别是 48.88%、37.59%和 33.41%。具体数据如图 14 所示。

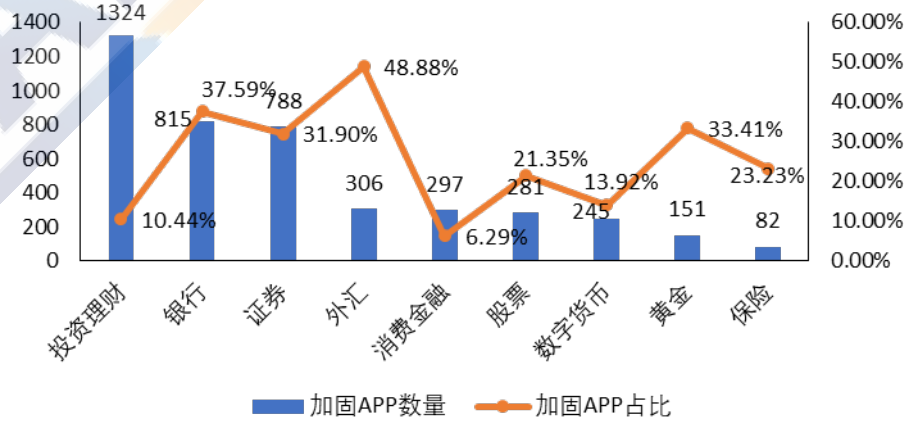


图 14　各金融细分领域 App 加固分布情况

三、数字金融 App 侵害用户权益专项检测结果

2020 年 7 月 22 日，工业和信息化部印发《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），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。

为此，报告团队在专项整治行动的文件精神指导下，针对数字金融 App 侵害用户权益的问题进行了专项检测。本次检测分别在多个应用分发平台上抽样选取了银行、保险、证券各 10 款 App，共计 30 款典型金融行业 App。检测发现，抽样 App 中存在“违规处理用户个人信息”“设置障碍、频繁骚扰用户”“应用分发平台责任落实不到位”等不同程度的问题，严重侵害了用户权益。其中，保险类 App 问题数量最多，占问题总数的 47.06%；银行类 App 问题数量占问题总数的 35.29%；证券类 App 问题数量最少，占问题总数的 17.65%。

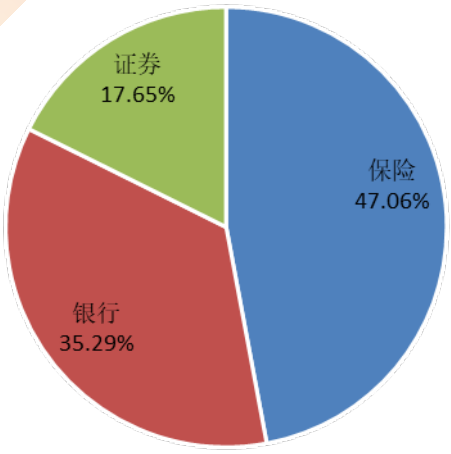


图 15　抽样 App 检测发现问题数量占比

（一）违规处理用户个人信息

根据专项整治行动要求，报告团队对抽取的 30 款典型金融行业 App 是否存在违规处理用户个人信息的行为进行了检测，发现有 18 款 App 存在不同程度的违规收集使用个人信息、超范围收集个人信息等问题，给用户的个人信息安全带来了隐患。

1．违规收集使用个人信息

违规收集使用个人信息，主要是指 App 或嵌入的 SDK 未向用户告知且未经用户同意，私自收集使用个人信息，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。检测发现，抽样 App 中有 16 款存在“违规收集使用个人信息”的问题，占存在“违规处理用户个人信息”问题的 App 总数的 88.89%。

以某证券类 App 为例，检测发现该应用嵌入的某第三方 SDK 在使用过程中收集了用户手机的唯一设备识别码，但并未通过隐私政策或其他显著方式向用户明示该 SDK 的个人信息收集使用行为，涉嫌违规收集使用个人信息。

2．超范围收集个人信息

超范围收集个人信息，主要是指 App 或嵌入的 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。检测发现，抽样 App 中有 3 款存在“超范围收集个人信息”的问题，占存在“违规处理用户个人信息”问题的 App 总数的 16.67%。

以某保险类 App 为例，检测发现该应用索取了通讯录的权限，但在其服务中并无合理应用场景，而在隐私政策中也未明示需要授权通讯录相关权限，涉嫌超范围收集个人信息。



图 16　某保险类 App 超范围收集个人信息

（二）设置障碍、频繁骚扰用户

根据专项整治行动要求，报告团队对抽取的 30 款典型金融行业 App 是否存在设置障碍、频繁骚扰用户方面的行为进行了检测，发现有 14 款 App 存在频繁、过度、强制索取权限的问题。

1．App 频繁索取权限

App 频繁索取权限，主要是指 App 在用户明确拒绝权限申请后，仍频繁弹窗、反复申请与当前服务场景无关权限的行为。检测发现，

抽样 App 中有 10 款存在“频繁索取权限”的问题，占存在“设置障碍、频繁骚扰用户”问题的 App 总数的 71.43%。

以某银行类 App 为例，检测发现该应用在用户拒绝提供位置信息及管理电话权限后，每次 App 重新启动，都会再次向用户索取这两个权限的授权，涉嫌频繁索取权限。



图 17　某银行类 App 频繁索取权限

2．App 过度索取权限

App 过度索取权限，主要是指 App 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所需权限的行为。检测发现，抽样 App 中有 3 款存在“过度索取权限”的问题，占存在“设置障碍、频繁骚扰用户”问题的 App 总数的 21.43%。

以某保险类 App 为例，检测发现该应用在启动时，无合理应用场景，也未明确告知用户索取权限的目的和用途，提前向用户申请获

取拍照、录制音视频以及位置权限，涉嫌过度索取权限。



图 18　某保险类 App 过度索取权限

3．App 强制索取权限

App 强制索取权限，主要是指 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。检测发现，抽样 App 中有 2 款存在“强制索取权限”的问题，占存在“设置障碍、频繁骚扰用户”问题的 App 总数的 14.29%。

以某银行类 App 为例，检测发现该应用在启动时，必须要授权使用拍摄照片和录制视频权限以及提供位置信息，否则无法使用 App。但实际上，这两项权限并非该 App 正常运行的必要权限，涉嫌强制索取权限。

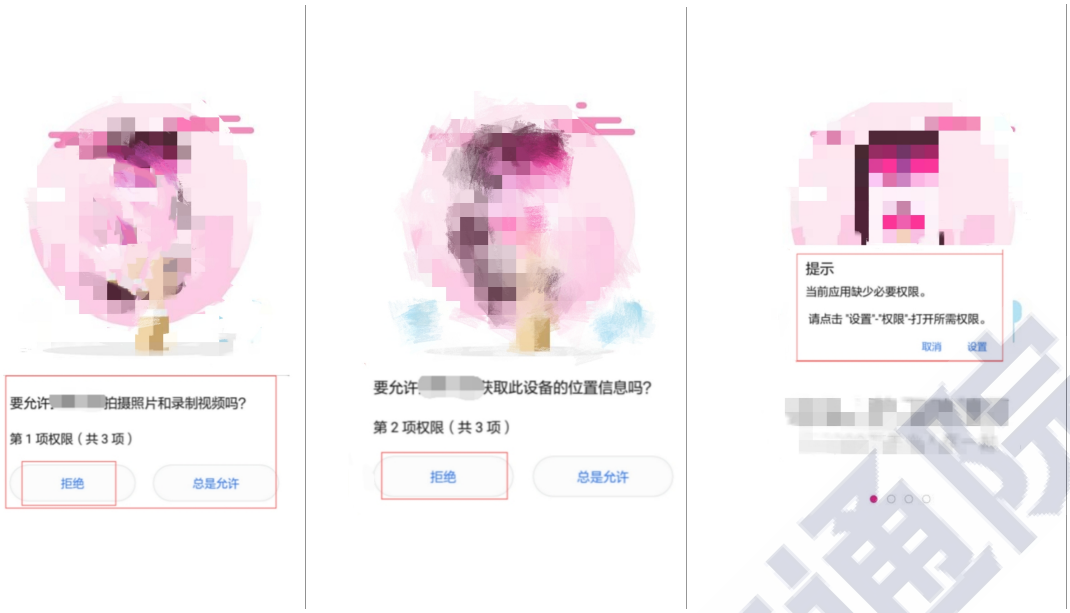


图 19　某银行类 App 强制索取权限

（三）应用分发平台责任落实不到位

在抽取 App 的过程中，报告团队根据专项整治行动要求，对应用分发平台的责任落实情况进行了检测，发现个别应用分发平台存在管理责任落实不到位的问题，缺乏完善的 App 上架审核机制，可能导致部分存在漏洞或者恶意程序的 App 被发布上线，存在侵害用户权益的风险。



图 20　某应用分发平台收录的某银行类 App 存在恶意程序

四、数字金融 App 的安全工作思路与建议

（一）App 相关监管部门

数字经济时代，伴随着移动互联网的高速发展，App 安全已成为多方关注的重点，各监管部门基于自身职能，以专项行动为牵引，着力开展 App 安全管理实践，对企业监督执法力度持续加强。近两年，中央网信办、工业和信息化部、公安部、国家市场监督管理总局等行业监管部门成立专项治理工作组联合开展 App 违法违规收集使用个人信息专项治理行动，人民银行也发文要求各地人民银行分支机构及相关监管机构开启金融科技风险专项摸排工作，把“移动金融客户端应用软件”作为主要摸排对象之一。监管部门的一系列举措表明，App 的监管整治正在提速。但从报告团队的安全观测结果可以看出，数字金融 App 的安全形势依然严峻。相关监管部门应持续完善以法律法规为准绳、制度指引为方向、监管机制为保障、技术手段为依托、标准评估为支撑的全方位 App 安全治理体系，同时，在前期 App 专项治理工作的基础上，强化跨部门安全联动管理，完善行业分管、协同联动的管理模式，多方协同、多管齐下，加大数字金融 App 的治理力度。

（二）App 开发运营者

作为责任主体，App 开发运营者的安全意识和安全防护能力对于 App 安全至关重要。在金融信息安全监管体系逐渐完善的趋势下，数字金融 App 的开发运营者应主动拥抱监管，严格履行法律法规规定

的责任义务，同时依照相关标准，对 App 安全与个人信息保护情况进行自评估，积极防范化解安全隐患。一方面，应结合实际的业务功能和场景所需，明确 App 所提供的服务类型和最小必要个人信息范围，仅申请 App 业务功能所必需的权限，不违规收集、使用、处理个人信息，不骚扰、欺骗、误导用户；另一方面，应建立 App 开发的安全管理机制，加强对嵌入使用的第三方 SDK 的安全检测，积极做好 App 安全防御措施，主动进行 App 安全加固，及时修补安全漏洞，推动安全升级，防止 App 感染恶意程序或因漏洞问题被仿冒、攻击等。

（三）App 应用分发平台

应用商店等分发平台应按照相关法律法规和标准规范的要求，落实平台管理责任，加强对金融行业 App 上架前的审核，将 App 安全与个人信息保护措施作为重点审核内容，对违法违规 App 不予上架。同时，应严格落实相关要求，向用户明示 App 运行所需权限列表，以及收集、使用用户个人信息的内容、目的、方式和范围等。此外，应用分发平台应做好自身的安全防护工作，定期开展网络安全评测，及时封堵脆弱性、安全漏洞及恶意程序等基础安全隐患和问题，不给外部攻击者可乘之机。

（四）App 用户

在网络安全方面，大部分 App 用户的安全意识和能力仍然不足。从保护自身权益和规避网络安全风险角度，建议金融行业的 App 用

户应做好 App 使用时的安全防护，重视自身个人信息保护。一是应从正规的应用分发平台下载 App，并及时对系统和 App 进行更新升级；二是提高自身隐私保护意识，安装 App 时认真阅读隐私政策和权限提醒，关注相关权限是否为使用该 App 所必需的权限，谨慎开启录音、读取通讯录、访问位置等较容易直接泄露个人敏感信息的权限；三是设置高强度密码并定期更换，谨慎使用“一键登录”“自动绑卡”“快捷支付”等弱验证的功能，切勿为贪图便利而牺牲安全性。

CAICT 中国信通院

附录 A　数字金融 App 地域分布表

序号	省份	App 数量	占比
1	广东省	9818	35.21%
2	湖北省	6109	21.91%
3	北京市	2334	8.37%
4	上海市	1748	6.27%
5	江苏省	1328	4.76%
6	浙江省	1136	4.07%
7	湖南省	838	3.01%
8	福建省	706	2.53%
9	河南省	615	2.21%
10	陕西省	434	1.56%
11	山东省	396	1.42%
12	四川省	364	1.31%
13	河北省	229	0.82%
14	辽宁省	180	0.65%
15	江西省	156	0.56%
16	安徽省	147	0.53%
17	重庆市	145	0.52%
18	天津市	141	0.51%
19	山西省	135	0.48%
20	吉林省	121	0.43%
21	广西壮族自治区	96	0.34%
22	黑龙江省	95	0.34%
23	海南省	95	0.34%
24	甘肃省	91	0.33%
25	贵州省	89	0.32%
26	内蒙古自治区	85	0.30%
27	云南省	85	0.30%
28	新疆维吾尔自治区	62	0.22%
29	西藏自治区	29	0.10%
30	宁夏回族自治区	27	0.10%
31	青海省	18	0.06%
32	台湾省	16	0.06%
33	香港特别行政区	9	0.03%
34	澳门特别行政区	6	0.02%

附录 B　Top10 高危漏洞说明

序号	恶意程序	检测目的	类型说明
1	系统键盘使用风险漏洞	检测应用在敏感数据输入时是否使用不安全的系统键盘。	用户在客户端的敏感界面（如登录、注册、支付界面等）输入敏感信息与显示（输出）时，如果未使用安全键盘，而使用第三方未知键盘或系统键盘，可能存在数据被拦截与监听的风险，导致账号、密码等敏感数据泄露。
2	ZipperDown 漏洞	检测应用程序中是否存在 ZipperDown 漏洞。	当前大量应用均会读取 zip 压缩包进行相关业务，最常见的场景就是从服务器下载压缩包，进行资源、代码热更新。如果攻击者用远程劫持或者本地替换等方式将 App 将要加载的正常 zip 包替换为带有路径前缀的恶意 zip 包，而 App 又未对解压文件的文件名称进行处理，则攻击者可以对应用资源、代码进行任意篡改、替换，从而实现远程代码劫持等。
3	H5 文件加固检测漏洞	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，植入钓鱼页面或者恶意代码，导致用户账号、登录密码、支付密码等敏感信息泄露。更有甚者，H5 代码可能暴露相关活动的业务逻辑，从而被黑产团队用来刷红包、薅羊毛等，造成经济损失。
4	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，主要用于在不同的应用程序之间实现数据共享的功能。当 Content Provider 的数据源是 SQLite 数据库并且 Provider 组件暴露时，如果使用拼接字符串形式构造的 SQL 语句去查询底层 SQLite 数据库，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泄露，例如用户名、密码等，或者产生查询异常导致应用崩溃。
5	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，用户在输入用户名和密码时，会被明文保存到应用数据目录中。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。

序号	恶意程序	检测目的	类型说明
6	SO 文件加固检测漏洞	检测应用程序中的 SO 文件是否进行加固。	SO 文件为 APK 中包含的动态链接库文件，Android 利用 NDK 技术将 C/C++语言实现的核心代码编译为 SO 库文件供 Java 层调用。SO 文件被破解可能导致应用的核心功能代码和算法泄露。攻击者利用核心功能与算法可轻易抓取到客户端的敏感数据，并对其解密，导致用户的隐私泄露或直接财产损失。
7	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 以及之前的版本存在该漏洞，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，给 WebView 加入一个 JavaScript 桥接接口，通过接口调用可以直接与本地的 Java 接口进行交互。这可能导致手机被安装木马程序、发送扣费短信、通讯录或者短信被窃取等。
8	Java 代码加壳检测漏洞	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。攻击者通过反编译工具可能得到应用程序的代码，导致代码逻辑泄露。
9	动态注册 Receiver 风险漏洞	检测应用是否存在动态注册 Receiver 风险。	动态注册的 BroadcastReceiver 是全局的并且默认可导出的，如果没有限制访问权限，可能被任意外部 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。
10	Janus 漏洞	检测应用是否存在 Janus 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，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。

附录 C　App 恶意程序类型说明

序号	恶意程序	类型说明
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，导致用户直接经济损失。
2	隐私窃取	在用户不知情或未授权的情况下，获取涉及用户隐私的信息，包括用户的手机号、通讯录、短信内容、通话记录、通话内容、地理位置、本机已安装软件等信息。
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；感染此类恶意程序的个人手机会成为控制者的肉鸡，完全被对方控制。
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代码进行扩散的恶意行为；感染此类恶意程序的用户，会蒙受数据流量损失和成为恶意程序的传播者。
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。
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。
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恶意行为。
8	流氓行为	对系统没有直接损害，但会严重影响用户体验，包括但不限于在用户不知情或未授权的情况下，自动捆绑安装的；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、卸载、删除的；执行用户未授权的其他操作等。

附录 D　受恶意程序感染的数字金融 App 地域分布表

序号	省份	病毒 App 数量	病毒感染率	病毒数量占比
1	广东省	2796	28.48%	45.21%
2	湖北省	1088	17.81%	17.59%
3	江苏省	787	59.26%	12.73%
4	河南省	365	59.35%	5.90%
5	北京市	294	12.60%	4.75%
6	上海市	195	11.16%	3.15%
7	浙江省	167	14.70%	2.70%
8	湖南省	111	13.25%	1.79%
9	陕西省	108	24.88%	1.75%
10	福建省	71	10.06%	1.15%
11	四川省	40	10.99%	0.65%
12	山东省	21	5.30%	0.34%
13	辽宁省	19	10.56%	0.31%
14	江西省	17	10.90%	0.27%
15	天津市	12	8.51%	0.19%
16	内蒙古自治区	11	12.94%	0.18%
17	甘肃省	10	10.99%	0.16%
18	河北省	9	3.93%	0.15%
19	吉林省	7	5.79%	0.11%
20	重庆市	7	4.83%	0.11%
21	云南省	7	8.24%	0.11%
22	山西省	6	4.44%	0.10%
23	安徽省	6	4.08%	0.10%
24	广西壮族自治区	6	6.25%	0.10%
25	新疆维吾尔自治区	5	8.06%	0.08%
26	贵州省	3	3.37%	0.05%
27	西藏自治区	3	10.34%	0.05%

序号	省份	病毒 App 数量	病毒感染率	病毒数量占比
28	青海省	3	16.67%	0.05%
29	台湾省	3	18.75%	0.05%
30	黑龙江省	2	2.11%	0.03%
31	海南省	2	2.11%	0.03%
32	香港特别行政区	2	22.22%	0.03%
33	澳门特别行政区	1	16.67%	0.02%

CAICT 中国信通院

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

电子邮箱：jiangding@caict.ac.cn

传真：010-62304364

网址：www.caict.ac.cn