2019
金融行业移动App安全观测报告

2019·10

CAICT 中国信通院

出品单位

中国信息通信研究院安全研究所

前　言

坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大会议精神，为促进金融科技安全发展，推动金融风控水平提高，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》等法律法规和《中国金融业信息技术“十三五”发展规划》《金融科技（FinTech） 发展规划（2019—2021 年）》《信息安全技术 个人信息安全规范》等标准规范与文件精神，中国信息通信研究院（以下简称：中国信通院）在有关领导部门的指导下，聚焦于金融行业 App，梳理金融行业 App 的安全现状，探究金融行业 App 的网络安全问题，总结形成本观测报告。

本次观测行动集中观测了金融行业中基于安卓系统的移动应用，共涉及 232 个应用市场收录的 133327 款金融行业 App。经过持续数月的观测，本报告研究团队综合运用大数据、漏洞扫描、病毒检测、抽样研究等技术和分析手段，全方位、多维度地梳理了金融行业 App 的网络安全现状。研究发现，金融行业 App 的安全风险集中体现在以下五个方面，**一是**高危漏洞普遍存在，**二是**恶意程序问题严峻，**三是**使用 SDK 引入风险，**四是**违规索权侵犯隐私，**五是**缺乏有效安全加固。

本报告旨在通过对金融行业的移动 App 进行安全观测与风险分析，提出金融行业 App 安全工作的思路与建议，通过各单位的协同联动，促进金融行业 App 的网络安全生态体系建立，支撑保障金融行业的安全发展。

目 录

一、金融行业 App 观测背景

（一）移动应用安全的政策背景

自十八大以来，党中央和国务院高度重视网络安全。习近平总书记指出，没有网络安全就没有国家安全，将网络安全提升到国家战略高度。随着移动互联网的快速发展，移动互联网安全在整体网络安全中的重要性愈加突出，而移动互联网安全的重中之重就是移动 App 的网络安全。

2019 年 1 月 25 日，中央网信办、工业和信息化部、公安部、市场监督总局四部门联合发布《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了《App 违法违规收集使用个人信息自评估指南》（以下简称《评估指南》），指导各相关单位进行自查整改。3 月 15 日，市场监管总局、中央网信办正式对外发布公告，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。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。8 月 8 日，为落实《中华人民共和国网络安全法》（以下简称《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颁布《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。

App 相关法律法规的密集颁布和出台，体现了政府对于保障 App 网络安全的重视和治理 App 网络安全的决心，也反映出当前移动 App 安全面临着严峻的形势。

（二）金融行业 App 的安全现状

近年来，随着智能手机和移动互联网的快速发展，移动 App 已经深入应用到大众生活的方方面面。用户通过金融行业进行投融资、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。然而，移动 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。移动 App 网络安全相关的法律法规和标准规范体系不完善，给不法分子带来可乘之机；安卓第三方应用商店繁多，App 上线审核不规范，管理不严格情况时有发生；部分金融行业 App 开发者安全意识淡薄，技术手段落后，开发流程不规范，更新修复不及时等问题严重；App 的用户缺乏安全意识，不良的 App 使用习惯带来安全隐患。据《2019 年上半年我国互联网网络安全态势》报告显示，CNCERT 对 105 款互联网金融 App 检测发现安全漏洞 505 个，其中高危漏洞 239 个。高危漏洞中，包括 59 个明文数据传输漏洞、58 个明文存储密码漏洞和 40 个源代码反编译漏洞。这些安全漏洞可能威

胁交易授权和数据保护，带来严重的安全风险。

为了进一步贯彻落实习近平总书记网络强国战略思想，促进金融行业安全发展，为金融行业管理部门、金融机构和信息安全厂商提供决策依据，中国信通院安全研究所行业安全团队对基于安卓系统的金融行业 App 网络安全现状进行观测，形成本观测报告。

二、金融行业 App 观测结果

（一）观测对象分布情况

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。

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 1 所示。

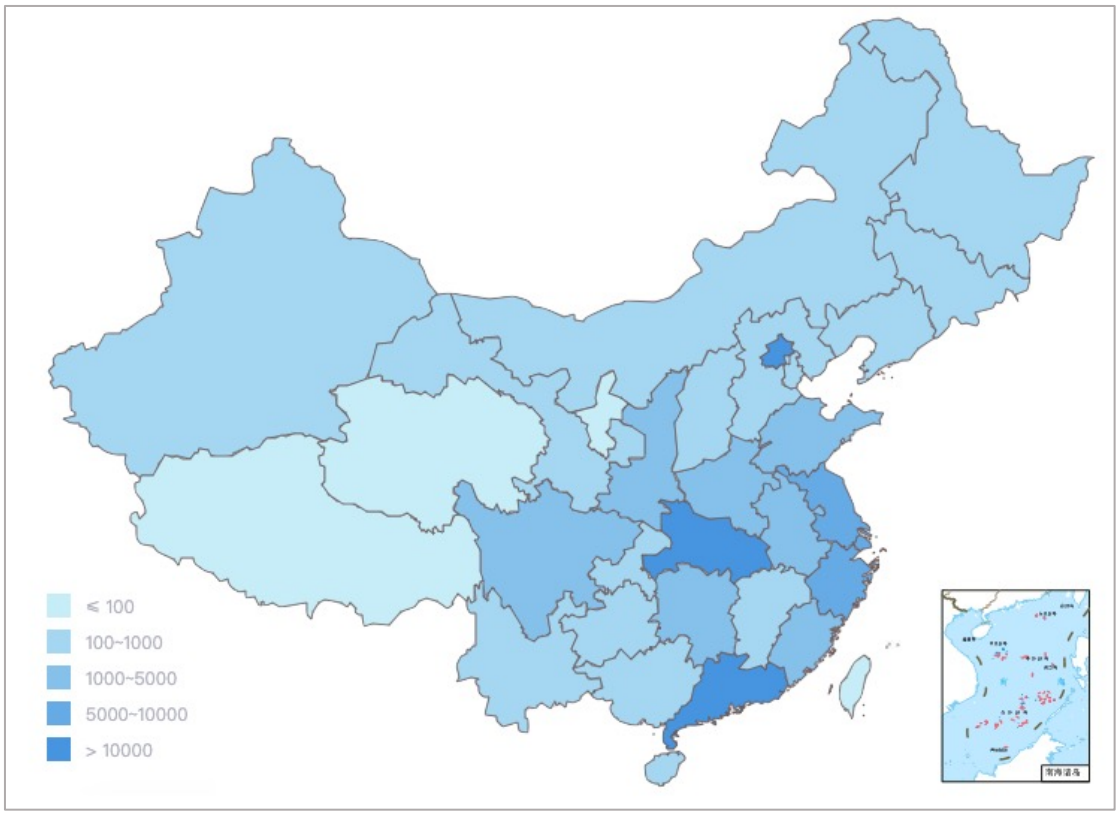


图 1　App 区域分布情况

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 2 所示：

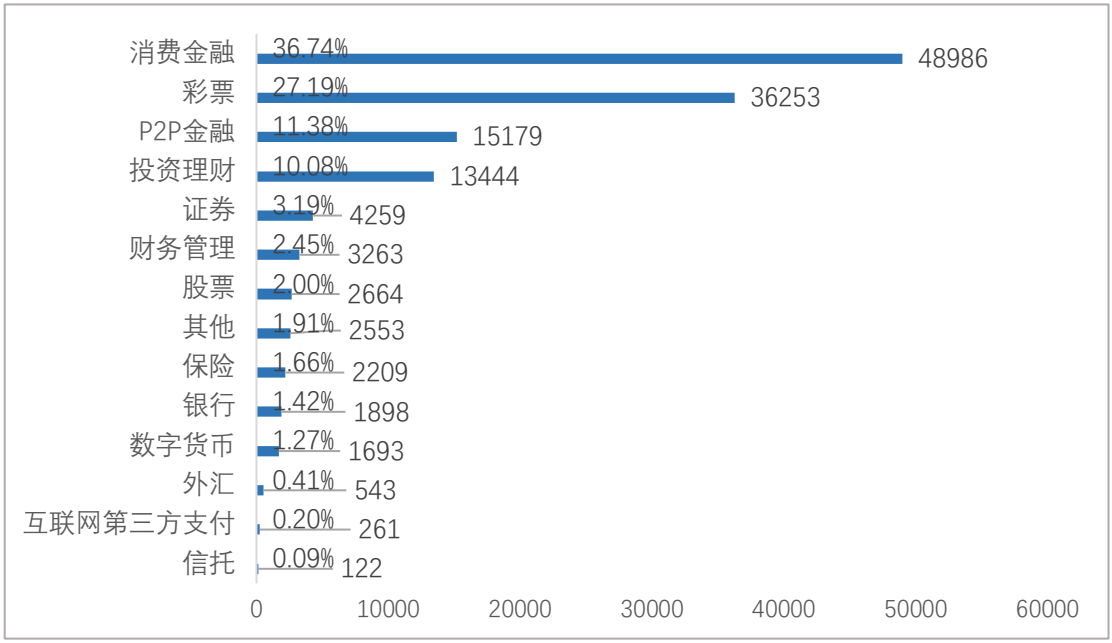


图 2　不同细分领域 App 数量及占比

（二）观测对象风险集中表现

1．以数据泄露为代表的高危漏洞风险

在本次观测中，发现有 70.22%的金融行业 App 存在高危漏洞，攻击者可利用这些漏洞窃取用户数据、进行 App 仿冒、植入恶意程序、攻击服务等，对 App 安全具有严重威胁。其中 Top3 的高危漏洞均存在导致 App 数据泄露的风险。

2．以流氓行为代表的恶意程序感染风险

本次观测发现，共有 8217 款金融行业 App 被检测出恶意程序，感染率为 6.16%，主要涉及的恶意行为包括流氓行为、信息窃取、恶意传播、资费消耗、远程控制等多种恶意行为，给 App 用户的个人隐私及财产安全带来危害。其中受到流氓行为恶意程序感染的 App 占比最多，约为 82.02%。

3．使用第三方 SDK 引入安全风险

本次观测发现，共有 20.48%的金融行业 App 被嵌入了第三方

SDK,嵌入的 SDK 数量共计高达 104005 个。在嵌入 SDK 的金融行业 App 中，有 45%的 App 嵌入了 5 个及以上的 SDK。由于第三方 SDK 存在隐蔽收集用户信息、自身安全漏洞易被不法分子利用等安全风险，使得金融行业 App 也面临一定的安全隐患。

4．违规索权带来的隐私泄露风险

本次观测中选取了具有典型代表性的 12 款下载量过亿的金融行业 App 进行抽样分析，经研究发现，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隐患。App 用户的个人隐私信息一旦泄露，将带来严重的后果，如骚扰电话、信息诈骗、恶意推销、网络情感诈骗等，会严重损害 App 用户的利益。

5．安全加固不足暴露安全风险

本次观测发现，仅有 17.08%的金融行业 App 进行了安全加固，超过 80%的金融行业 App 在应用市场“裸奔”，未进行任何的安全加固。然而，基于 Java 语言编写的安卓应用程序如不进行加固，则其打包的 APK 文件很容易被反编译工具进行逆向分析，进而暴露风险。

三、金融行业 App 的安全风险分析

（一）高危漏洞普遍存在

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 3 所示。

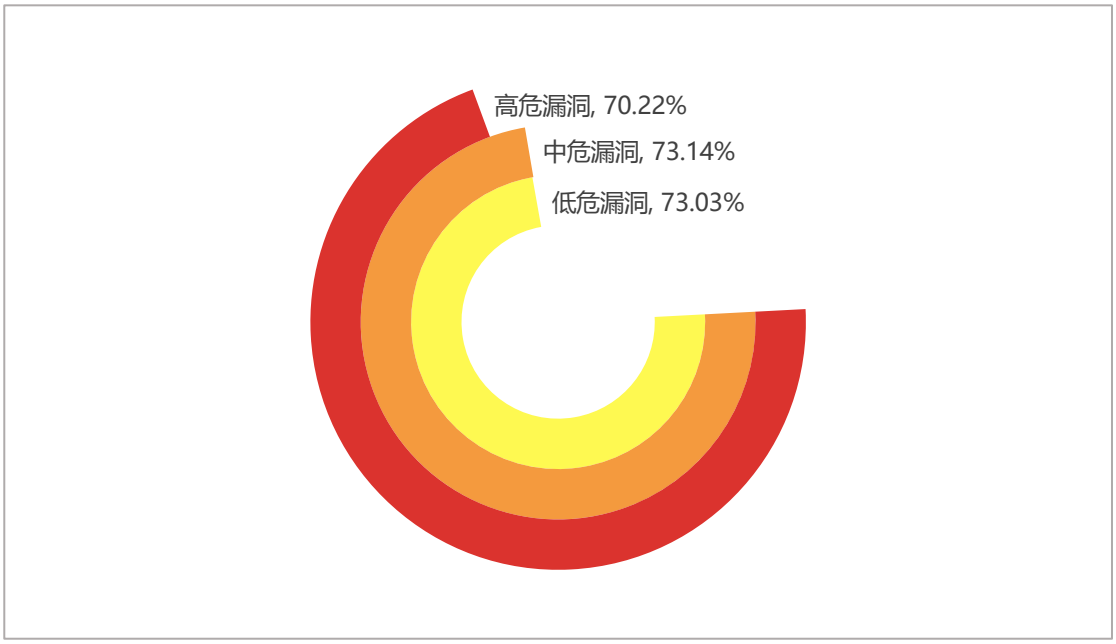


图 3 金融行业 App 各等级漏洞情况

从 App 分类角度来看，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 4 所示。

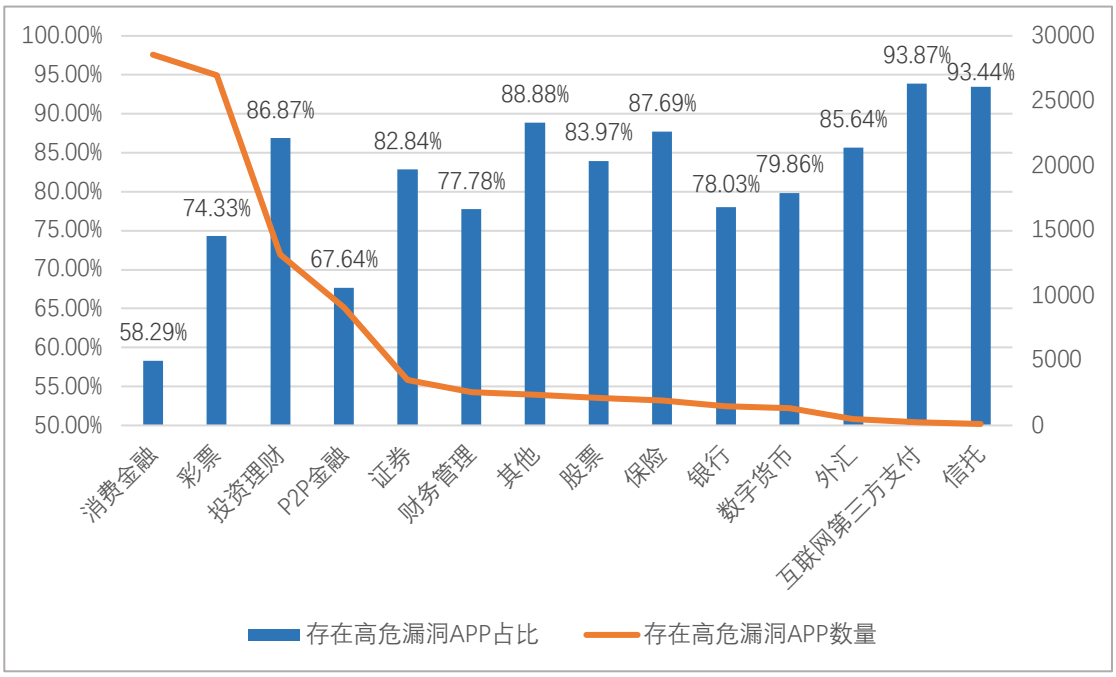


图 4 不同细分领域高危漏洞 App 数量及占比情况

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 5 所示。

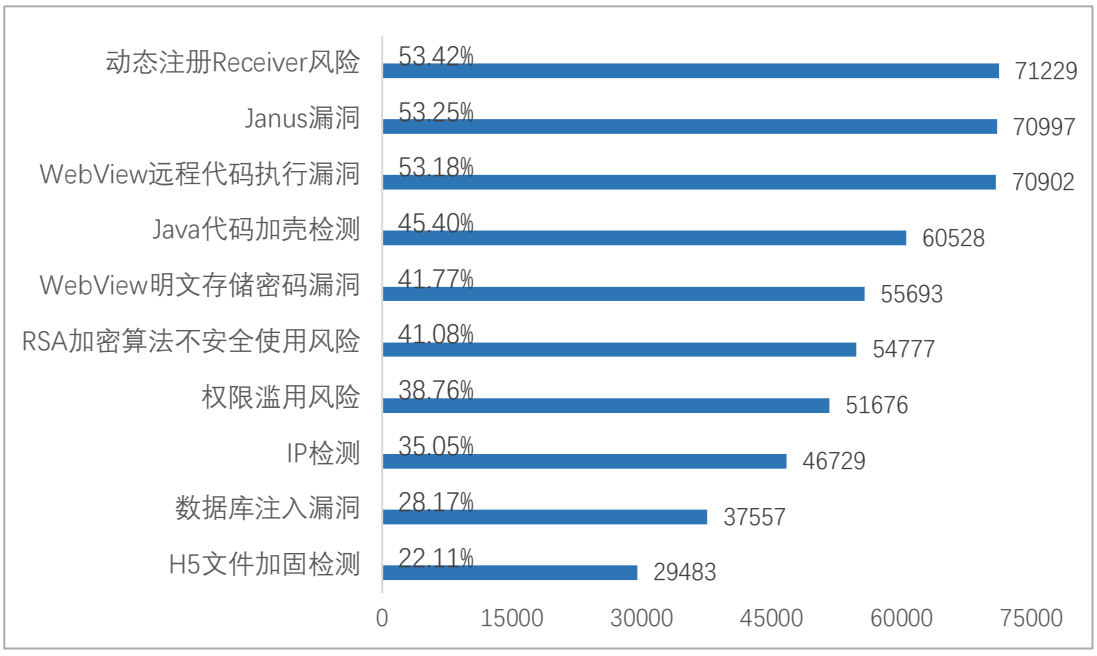


图 5 高危漏洞类型分布（Top10）

（二）恶意程序问题严峻

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 6 所示。

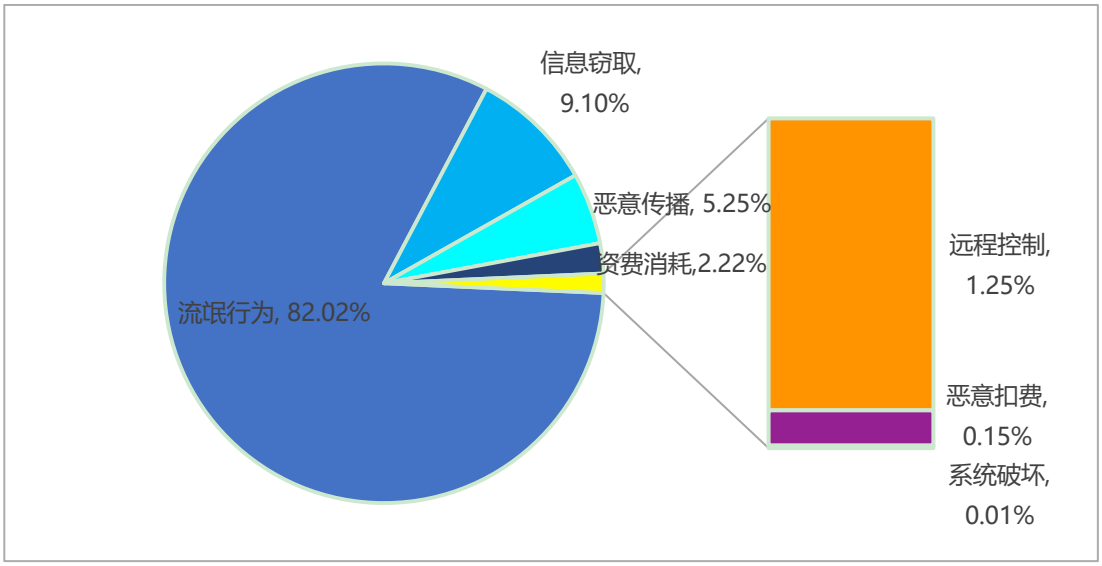


图 6　App 恶意程序类型分布情况（一款 App 可能存在多种病毒）

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 7 所示:

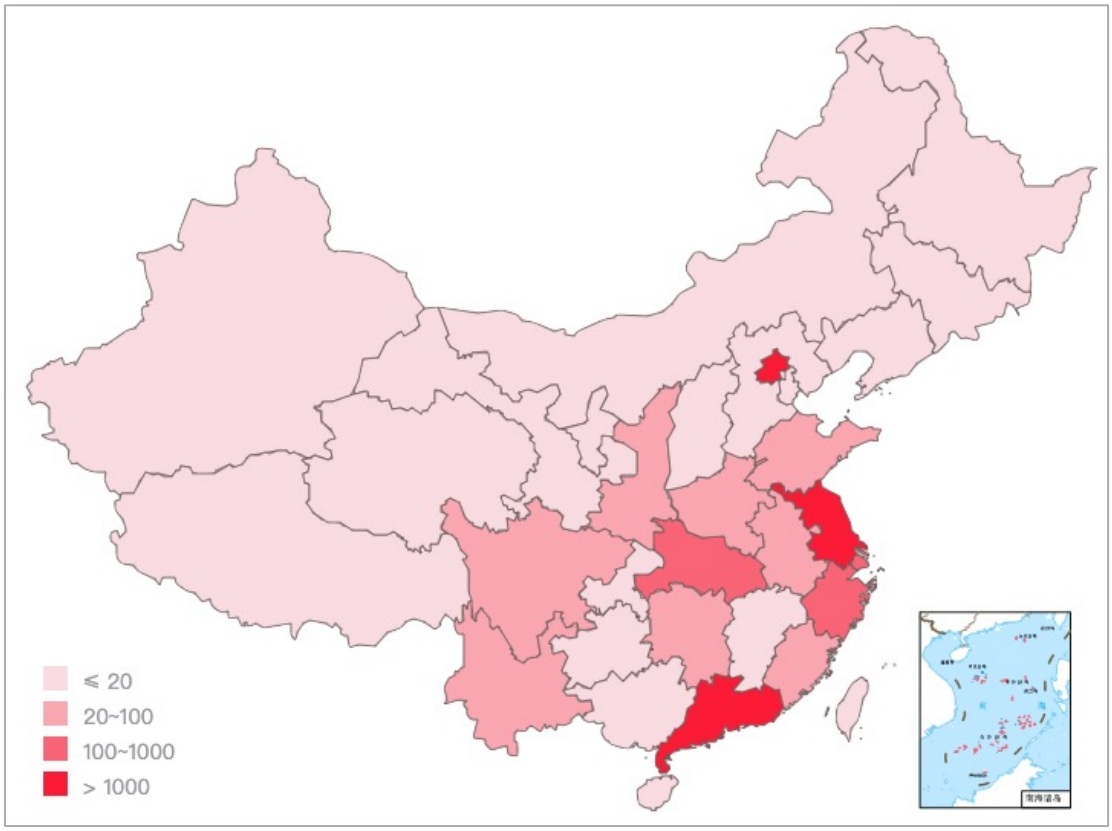


图 7 受到恶意程序感染的 App 区域分布情况

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 8 所示。

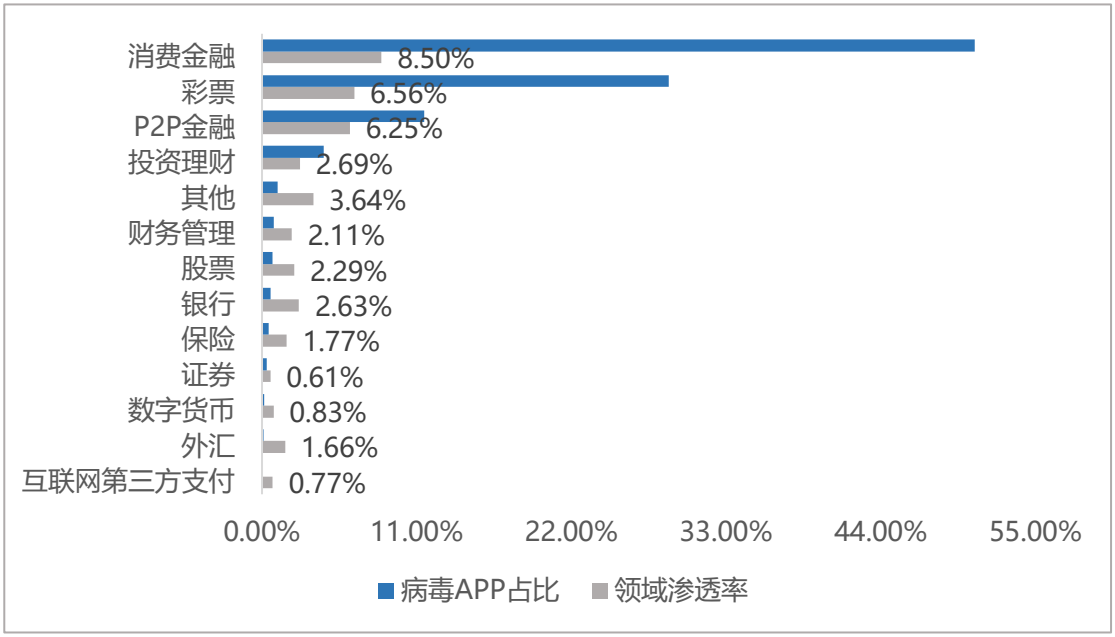


图 8 各细分领域受到恶意程序感染的 App 分布情况

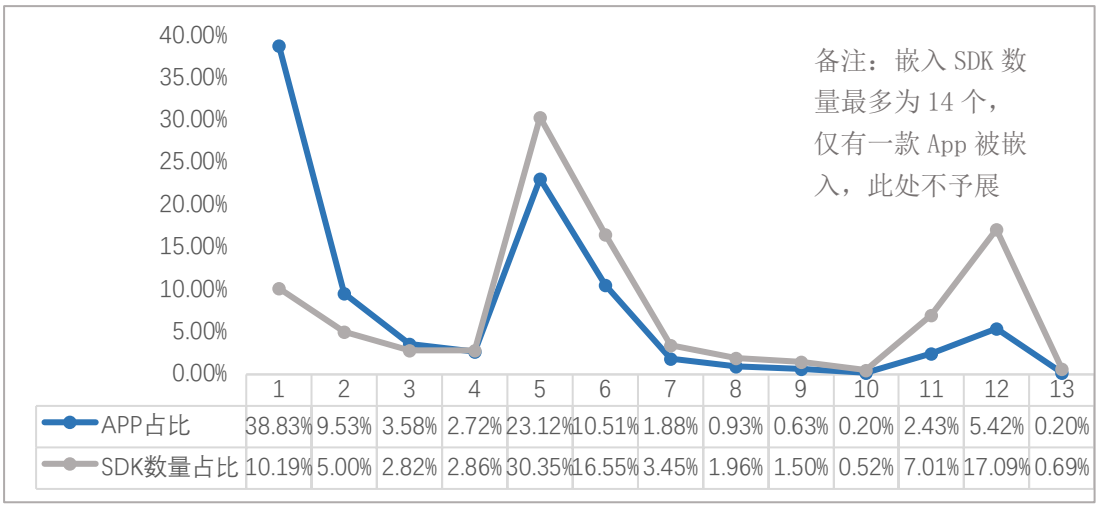
（三）使用 SDK 引入风险

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 9 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%

图 9 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 10 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。

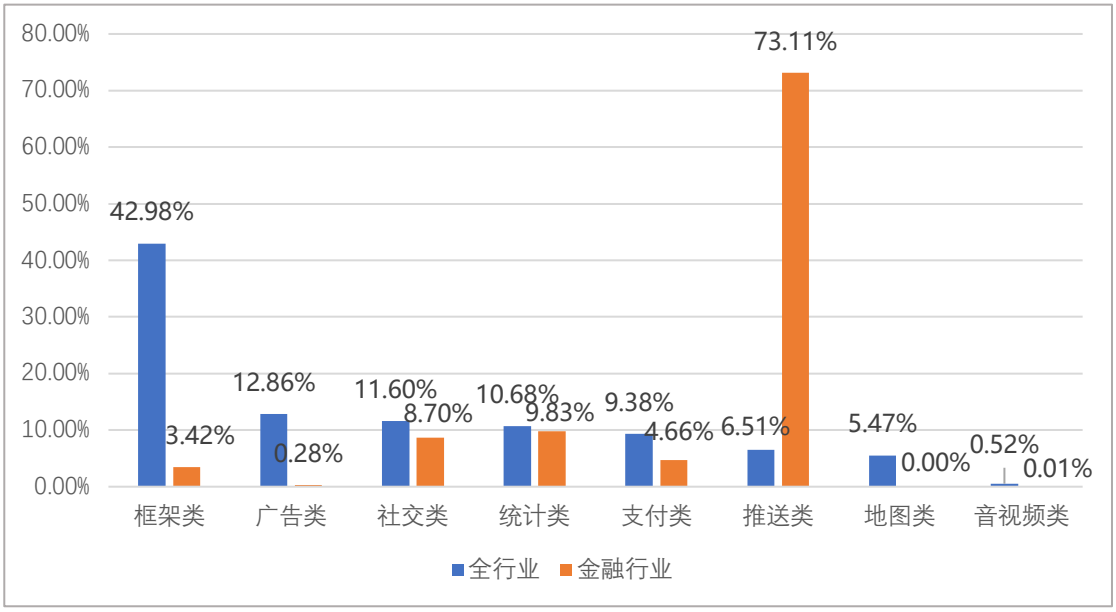


图 10 全行业和金融行业 App 使用的各类 SDK 分布对比

（四）违规索权侵犯隐私

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
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

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	访问大致位置信息	中敏感	ACCESS_COARSE_LOCATION	91.67%
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%

序号	权限类别	敏感度	权限名	获取权限 App 占比
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%
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%

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

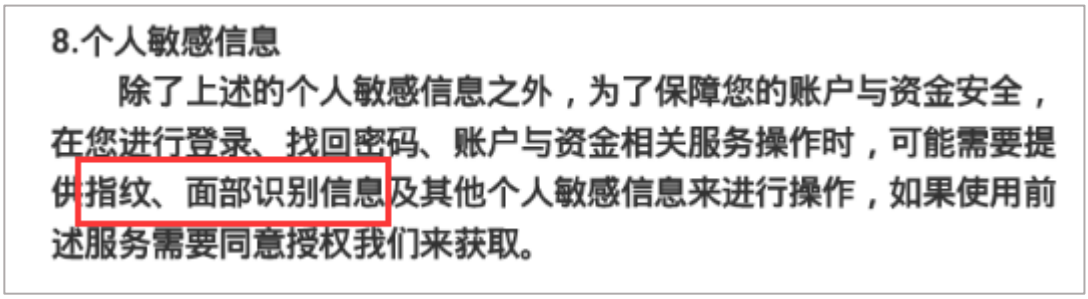
收集的必要信息包括：“手机号码”、“账号信息”、“身份信息”、“银行账户信息”、“个人征信信息”、“紧急联系人信息”以及“借贷交易记录”7 项内容。应用程序访问设备的手机功能及修改或删除存储卡中的内容涉嫌超范围获取权限。

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 11 某金融 App 隐私政策中收集用户指纹、面部等生物信息

如图 11 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。

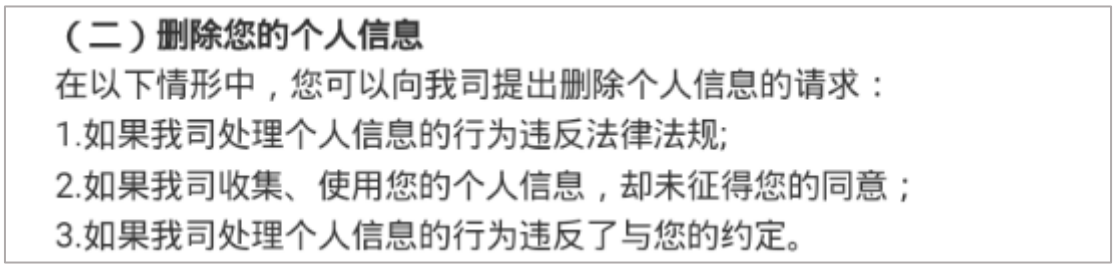


图 12 某金融 App 隐私政策中删除个人信息条款

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 12 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 13 某金融 App 未单独提供隐私政策

如图 13 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。

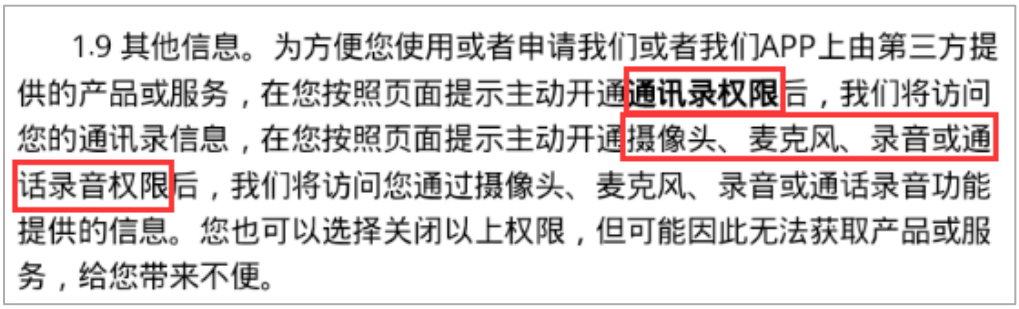
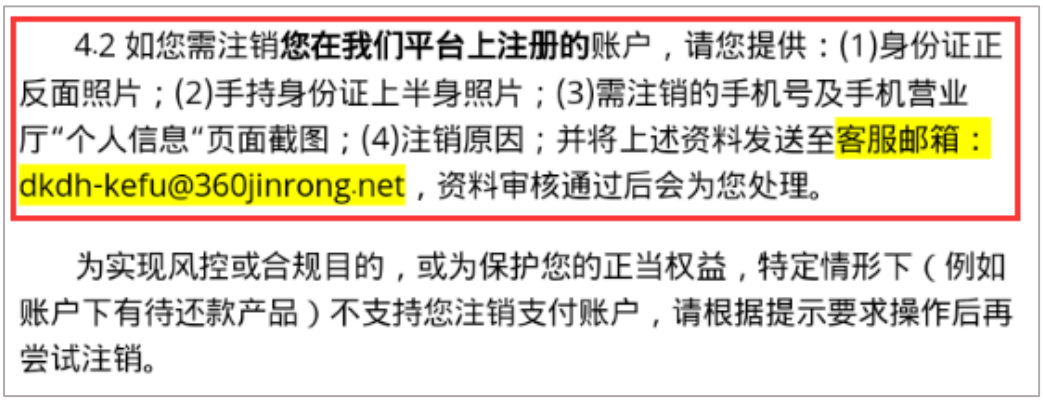

1.9 其他信息。为方便您使用或者申请我们或者我们APP上由第三方提供的产品或服务，在您按照页面提示主动开通**通讯录权限**后，我们将访问您的通讯录信息，在您按照页面提示主动开通摄像头、麦克风、录音或通话录音权限后，我们将访问您通过摄像头、麦克风、录音或通话录音功能提供的信息。您也可以选择关闭以上权限，但可能因此无法获取产品或服务，给您带来不便。

图 14 某金融 App 隐私政策中未说明收集信息的用途

如图 14 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。”

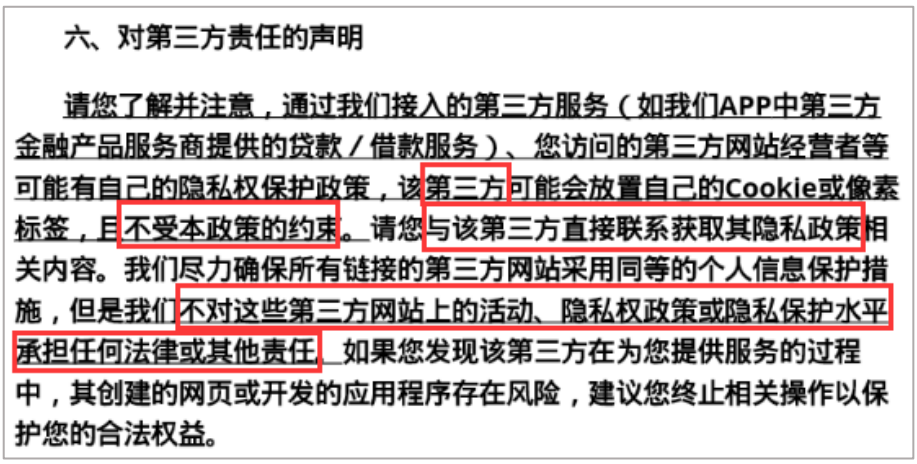

4.2 如您需注销**您在我们平台上注册的**账户，请您提供：(1)身份证正反面照片；(2)手持身份证上半身照片；(3)需注销的手机号及手机营业厅“个人信息”页面截图；(4)注销原因；并将上述资料发送至客服邮箱：dkdh-kefu@360jinrong.net，资料审核通过后会为您处理。

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 15 某金融 App 隐私政策中注销账号相关条款

如图 15 所示，某 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 16 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 16 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）缺乏有效安全加固

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 17 所示：

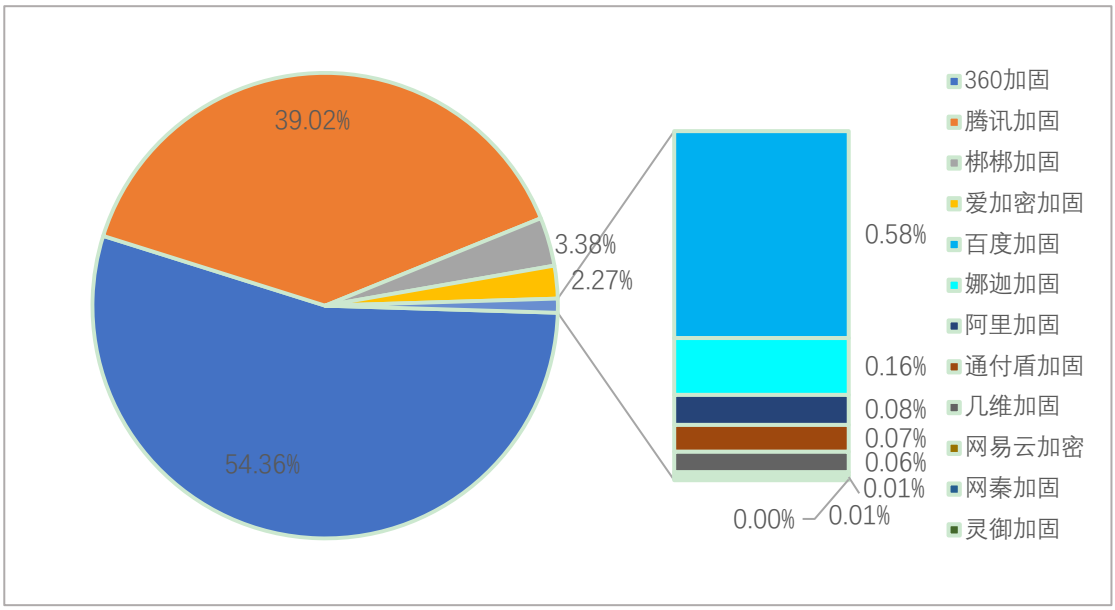


图 17 不同加固厂家服务的 App 占比

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，如图 18 所示。

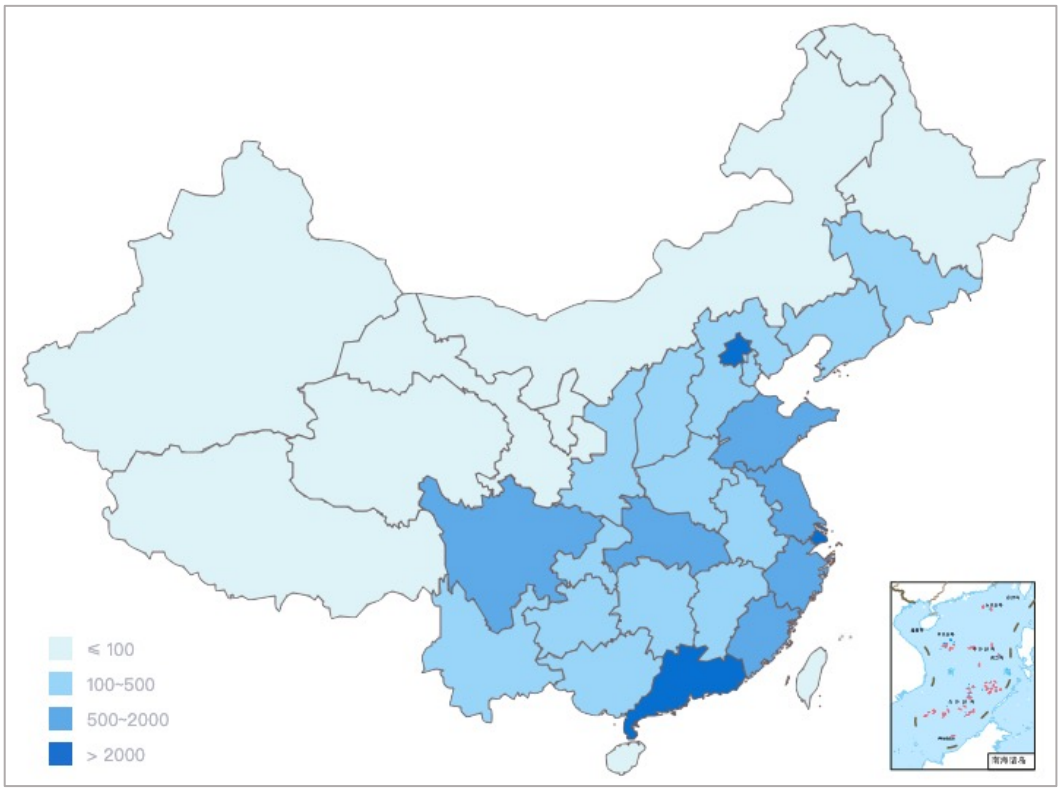
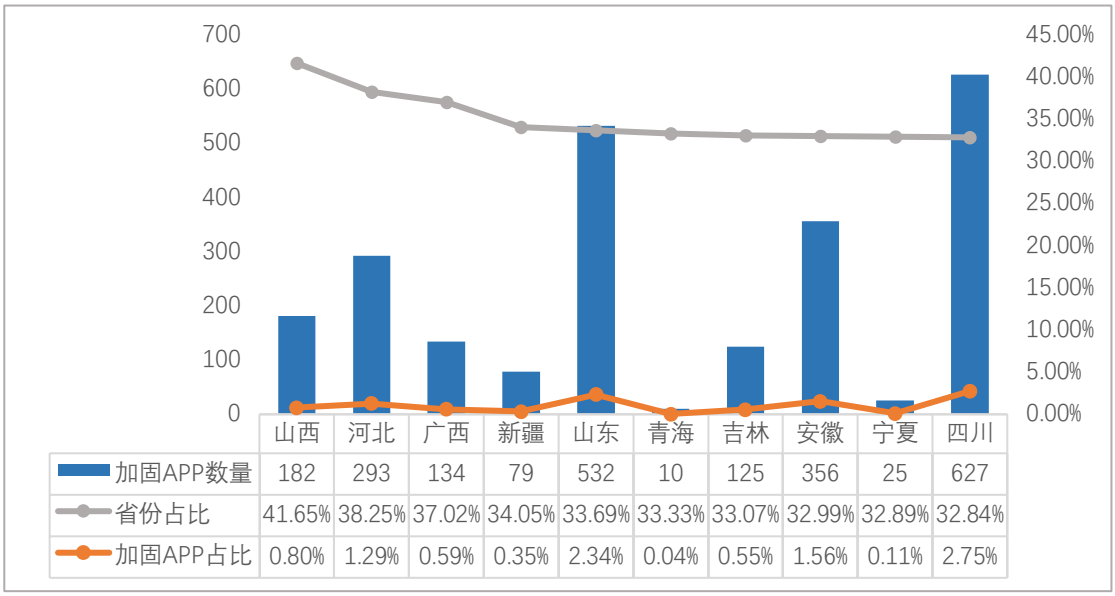


图 18 加固 App 地域分布

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%，如图 19 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%

图 19 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。如图 20 所示。

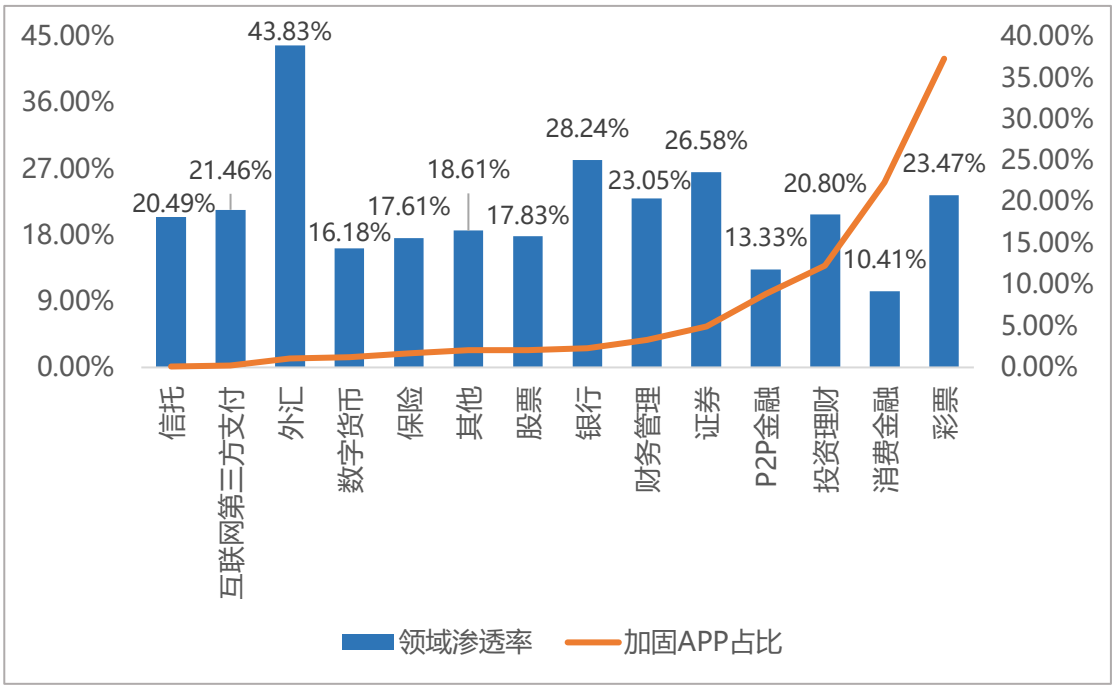


图 20 各金融细分领域 App 加固分布情况

四、金融行业 App 的安全工作思路

（一）相关行业主管部门

虽然近年来社会各界对金融行业网络安全的关注日益提升，但由于在 App 方面缺乏完整、配套的法律基础，使金融行业 App 安全无法得到充分的保护。相关行业主管部门应持续完善金融行业 App 安全法律法规和标准规范体系，一方面建立健全 App 安全等级保护测评制度，降低金融行业 App 遭受网络攻击风险；另一方面要加大 App 治理力度，持续规范金融行业 App 上的个人信息收集、使用和存储、共享等行为。

（二）应用商店运营者

应用商店是 App 与用户的桥梁，各应用商店运营者应严格贯彻落实《网络安全法》《个人信息安全规范》等法律法规和标准规范的要求，认真履行平台审核责任，保护好 App 开发者及用户权益。同时，协助行业主管部门开展 App 安全检测、认证等相关工作，引导用户下载通过安全认证的 App，降低因 App 安全问题给用户带来的损失。

（三）App 开发者

App 开发者是移动 App 安全的核心，其安全意识和安全防护能力对于 App 安全至关重要。针对金融行业 App 的开发者，首先，明确业务需求，详细界定 App 操作边界，不盲目开发，充分注重 App 开发后的维护和升级；其次，提高开发人员安全意识，建立 App 开发的安全理念和安全管理机制，合理合规使用第三方 SDK，避免过度收集

用户权限和隐私信息；最后，积极做好 App 安全防御措施，主动进行 App 安全检测和安全加固，及时修补安全漏洞，推动安全升级，防止 App 因漏洞问题被仿冒、攻击以及感染恶意程序等。

（四）App 的使用者

在网络安全方面，网民在绝大多数情况下是各类网络安全事件的直接受害者。从保护自身权益和规避网络安全事件角度，建议 App 的使用者，一是从正规应用市场下载 App，不随意点开不明下载链接；二是采用高强度口令，定期更换口令，避免口令重复；三是定期检测并及时使用安全软件修补漏洞，及时对系统和 App 进行更新升级；四是提高自身隐私安全意识，避免注册过多 App 和暴露过多个人隐私信息。

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%
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%

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、资产管理类应用	易收钱 App	1.0	https://www.zuiben.com/a_soft/36445.html
			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	龙里国丰村镇银行	1.4	http://www.xz7.com/downinfo/381780.html

序号	金融分类	分类逻辑	应用名称	版本号	网页链接
		开发的用于各类银行服务的应用	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/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。
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

序号	恶意程序	检测目的	类型说明
			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、

序号	恶意程序	检测目的	类型说明
			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%
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%

免责声明

本报告主要针对截止 2019 年 9 月 11 日安卓应用市场的金融行业 App 安全状况进行统计、研究和分析。本报告提供给媒体、公众和相关政府及行业机构作为金融行业 App 安全状况介绍和研究资料，请相关单位酌情使用。如若本报告阐述之状况、数据与其他机构研究结果有差异，请使用方自行辨别，中国信息通信研究院不承担与此相关的一切法律责任。