MoGua

奕丰 4.1.4.APK 分析报告

APP名称:	奕丰

包名:	cn.ifast.mobile.hybrid.ifa
域名线索:	15条
URL线索:	4条
邮箱线索:	0条
分析日期:	2025年6月21日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 奕丰.apk
文件大小: 137.59MB
MD5值: 05a7c5806e14d3766fff197a0ca986f9
SHA1值: 7a0b7894b376071318592f43fb8db463738104e9
SHA256值: 90641d7e29d4cc86f7ea46dc8c179726c7f3b16c77ead6b95b74007904dab093

APP 信息

App名称: 奕丰
包名: cn.ifast.mobile.hybrid.ifa
主活动Activity: cn.ifast.mobile.hybrid.ifa.MainActivity
安卓版本名称: 4.1.4
安卓版本: 250219

域名线索

域名	服务器信息
data-drcn.push.dbankcloud.com	**IP**: 121.36.117.8 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
grs.platform.dbankcloud.ru	没有服务器地理信息.
m.ifastps.com.cn	**IP**: 61.48.83.230 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 94.74.88.100

metrics-dra.dt.hicloud.com	**所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
data-dre.push.dbankcloud.com	IP: 80.158.49.244 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
data-drru.push.dbankcloud.com	IP: 159.138.202.31 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
metrics5.data.hicloud.com	IP: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
metrics1-drcn.dt.dbankcloud.cn	IP: 111.202.16.252 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
grs.dbankcloud.cn	IP: 49.4.35.251 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572

grs.dbankcloud.asia	**IP**: 49.4.35.251 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
metrics2.data.hicloud.com	**IP**: 80.158.2.190 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
metrics5.dt.dbankcloud.ru	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
grs.dbankcloud.eu	没有服务器地理信息.
data-dra.push.dbankcloud.com	**IP**: 119.8.163.189 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
grs.dbankcloud.com	**IP**: 60.28.200.159 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

URL线索

URL信息	Url所在文件
https://m.ifastps.com.cn/code-push-v1	摸瓜V1引擎
https://data-drcn.push.dbankcloud.com	摸瓜V2引擎
https://data-dra.push.dbankcloud.com	摸瓜V2引擎
https://data-dre.push.dbankcloud.com	摸瓜V2引擎
https://data-drru.push.dbankcloud.com	摸瓜V2引擎
https://metrics1-drcn.dt.dbankcloud.cn:443	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics2.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.dt.dbankcloud.ru:6447	摸瓜V2引擎
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://grs.platform.dbankcloud.ru	摸瓜V2引擎
https://grs.dbankcloud.eu	摸瓜V2引擎

https://gr3.ddunkcloud.cu	摸瓜V2引擎

邮箱线索

手机线索

手机号	所在文件
13530035980	摸瓜V1引擎

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=cn, ST=guangdong, L=shenzhen, O=ifast, OU=ifast, CN=soo cheng koh
签名算法: rsassa_pkcs1v15
有效期自: 2016-01-11 13:57:13+00:00
有效期至: 3015-05-14 13:57:13+00:00
发行人: C=cn, ST=guangdong, L=shenzhen, O=ifast, OU=ifast, CN=soo cheng koh
序列号: 0x7d57d562
哈希算法: sha256
md5值: 74c4ee4623decd9ab674ab780ac9c3e7
sha1值: e61cc65d12a1298cb43c1b3f58592b7d1856a39d
sha256值: 98a996692148e0137863901f78687a164c208c7a6469874b27394ac6d2b01178
sha512值: ccfff49f64cf9c47c44f707e419270f3d968ee5c0e0e6114ffc1222e4aa77f9a4e0a53fae4bd0c87d6dce81837f2ae6eb93987963429162ed35c06fc37822b96
公钥算法: rsa
密钥长度: 2048
指纹: 1a9ca4661079b6420790fc167535583658324201dbe778787b020570e85eedcb

硬编码敏感信息

可能的敏感信息
"ANDROID_CODE_PUSH_DEPLOYMENT_KEY" : "mXrN02ZKbQn5Mhq1qKJtv9pNIcSg4ksvOXqog"
"CodePushDeploymentKey" : ""
"IOS_CODE_PUSH_DEPLOYMENT_KEY" : "F9SRjbMMT6ZbpqichL28LxbTkObY4ksvOXqog"
"JPUSH_APPKEY" : "28a462fc2e5a59207f55601c"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
cn.ifast.mobile.hybrid.ifa.permission.JPUSH_MESSAGE	未	Unknown	Unknown permission from android reference

	知	permission	
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
com.hihonor.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.READ_CALENDAR	危险	读取日历事件	允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人
android.permission.WRITE_CALENDAR	危险	添加或修改日历事件并向客人发送电子邮件	允许应用程序添加或更改日历上的事件,这可能会向客人发送电子邮件。恶意应用程序可以使用它来删除或修改您的日历活动或向客人发送电子邮件
com.android.vending.CHECK_LICENSE	未知	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference

android.permission.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
com.fingerprints.service.ACCESS_FINGERPRINT_MANAGER	未知	Unknown permission	Unknown permission from android reference
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	未知	Unknown permission	Unknown permission from android reference
cn.ifast.mobile.hybrid.ifa.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
cn.ifast.mobile.hybrid.ifa.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
cn.ifast.mobile.hybrid.ifa.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)

cn.ifast.mobile.hybrid.ifa.MainActivity	Schemes: investor://, https://, Hosts: m.ifastps.com.cn, Path Prefixes: /investor,

---