



MoGua

360借条 2.0.12.APK 分析报告



APP名称:

360借条

包名:	com.qibu.qfqb
域名线索:	21条
URL线索:	7条
邮箱线索:	0条
分析日期:	2025年10月5日
分析平台:	摸瓜APK反编译平台

文件名: base.apk
文件大小: 69.97MB
MD5值: 4f3780cc99245f722b1110e721c2d6e2
SHA1值: 89367a608d0fb7bff2f033f8107c07fb11f3c2a7
SHA256值: 1fe7f234865fb862bcdaa5726cc5779def70f0a273b1cf466dcbf454d1c6fb6f

i APP 信息

App名称: 360借条
包名: com.qibu.qfqb
主活动Activity: com.qihoo.loan.LunchActivity
安卓版本名称: 2.0.12
安卓版本: 793

🔍 域名线索

域名	服务器信息
metrics-dre.dt.dbankcloud.cn	IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
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
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
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
httpdns.huaweicloud.com	IP: 122.112.208.149 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
grs.dbankcloud.eu	没有服务器地理信息.
connectivitycheck.cbg-app.huawei.com.cn	IP: 49.4.45.202 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572

connectivitycheck.platform.dbankcloud.com	IP: 121.22.232.151 所属国家: China 地区: Hebei 城市: Qinhuangdao 纬度: 39.932541 经度: 119.588226
grs.dbankcloud.com	IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
huashan-datahub-drcn.emui.dbankcloud.com	IP: 49.4.32.39 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
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
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
metrics-dra.dt.dbankcloud.cn	IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore

	纬度: 1.289987 经度: 103.850281
grs.dbankcloud.cn	IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
grs.dbankcloud.asia	IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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.platform.dbankcloud.ru	没有服务器地理信息.
data-drcn.push.dbankcloud.com	IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
render.alipay.com	IP: 221.207.101.97 所属国家: China 地区: Heilongjiang 城市: Jiamusi 纬度: 46.833328 经度: 130.350006

URL线索

URL信息	Url所在文件
https://render.alipay.com/p/yuyan/180020010001208736/alipayFacewelcome.html	摸瓜V1引擎
https://httpdns.huaweicloud.com	摸瓜V1引擎
https://metrics1-drcn.dt.dbankcloud.cn:443	摸瓜V2引擎
https://metrics-dra.dt.dbankcloud.cn:443	摸瓜V2引擎
https://metrics-dre.dt.dbankcloud.cn:443	摸瓜V2引擎
https://metrics5.dt.dbankcloud.ru:443	摸瓜V2引擎
https://huashan-datahub-drcn.emui.dbankcloud.com	摸瓜V2引擎
https://connectivitycheck.cbg-app.huawei.com.cn/	摸瓜V2引擎
https://connectivitycheck.platform.dbankcloud.com/	摸瓜V2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 bankcloud.com:6447	摸瓜V2引擎

https://metrics-grs.dbankcloud.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

 邮箱线索

 手机线索

手机号	所在文件
14534438610	摸瓜V2引擎
16057009010	摸瓜V2引擎
19318408234	摸瓜V2引擎
18138650888	摸瓜V2引擎

14534438610	摸瓜V2引擎
19298225107	摸瓜V2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: CN=loan
签名算法: rsassa_pkcs1v15
有效期自: 2016-04-11 07:22:03+00:00
有效期至: 2041-04-05 07:22:03+00:00
发行人: CN=loan
序列号: 0x2f72db56
哈希算法: sha256
md5值: f8837fc6c737023c70a4cf368923a6da
sha1值: 3a4582d530171a42137b7a2816935c239b4afdf9
sha256值: 7129f2e6e961ff2fd06cf34443998ae02ffcbe7dc2ebc3681ac7141d60c44870
sha512值: d4862c9c71e66cb7770a10f3861d04e2ca50003eb1de7fdd1890853e124f3b2d097555668ac5bc9f500b213a1a4856e744baf33bc6015b64ae1c264f026a6e51
公钥算法: rsa
密钥长度: 2048
指纹: 840f6159cddb0355c1ff6617566d4791126e48e871b03ad9002e2c2b9524622

🔑 硬编码敏感信息

可能的敏感信息
"loan_event_id_contact_no_auth" : "9000801"
"loan_event_id_pwd_dialog" : "9003601"

"loan_pwd_verify_forget_face" : "忘记交易密码，可通过刷脸完成借款申请，完成借款后可在APP→我的→账号设置→账户安全管理→重置交易密码，进行交易密码修改。"
"security_public_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8hzUojzHX8jDL+97pqr7CaLiKSsZ0aOES7FucX7vh9PoEDbCKNCTakRXdS5EiurPk3QpvsAGbfyls7JWKm4py9KcldJsZRh9onknVeAVIU++jnrGFGYfQb8iKzCIN059gYeejBs9mwi7RGU9tj0KHUG659v5sMBxv7zNse3fjQIDAQAB"

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.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由

android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
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.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.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。

android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
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
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
com.qibu.qfqb.permission.LDSDK_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.qibu.qfqb.permission.QDAS_MESSAGE	未知	Unknown permission	Unknown permission from android reference

com.android.permission.GET_INSTALLED_APPS	未知	Unknown permission	Unknown permission from android reference
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa.SECURITY_ACCESS	未知	Unknown permission	Unknown permission from android reference
oplus.permission.settings.LAUNCH_FOR_EXPORT	未知	Unknown permission	Unknown permission from android reference
com.vivo.identifier.permission.OAID_STATE_DIALOG	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.DETECT_SCREEN_CAPTURE	未知	Unknown permission	Unknown permission from android reference
com.qibu.qfqb.permission.JPUSH_MESSAGE	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。
	未	Unknown	

com.vivo.notification.permission.BADGE_ICON	知	permission	Unknown permission from android reference
com.hihonor.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
com.qibu.qfqb.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.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.qibu.qfqb.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.hihonor.push.permission.READ_PUSH_NOTIFICATION_INFO	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
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.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.qibu.qfqb.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.qibu.qfqb.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.qihoo.loan.LunchActivity	Schemes: qihooloanqb://, http://, https://, Hosts: 360.cn, qfqb.xjietiao.com, q.jrurl.cn,
com.qihoo.loan.SchemeLauncherActivity	Schemes: qfqbpanda://, http://, https://,
com.alipay.sdk.app.AlipayResultActivity	Schemes: qihooloanqb_alipay://,
com.tencent.tauth.AuthActivity	Schemes: tencent102005265://,

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。