MoGua

小花钱包 1.0.APK 分析报告

APP名称:	小花钱包

包名:	
域名线索:	14条
URL线索:	3条
邮箱线索:	0条
分析日期:	2025年6月26日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.xhqb.app_6.27.1_20250618155445_signed_UMENG_CHANNEL_xhqb01.apk

文件大小: 72.93MB
MD5值: 35aa0aaec4c1b456595390e791db667a
SHA1值: 6c73742cbcef35fdd83001cdfc4339d2f250a096
SHA256值: 2657f031b0247a15e0d92af946896c21309a1bbff5f95c6e13c8826ba135f288

APP 信息

App名称: 小花钱包
包名:
主活动Activity: []
安卓版本名称: 1.0
安卓版本: []

域名线索

域名	服务器信息
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
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
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
grs.dbankcloud.cn	**IP**: 124.70.116.153 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
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
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
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
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
	IP: 49.4.35.251

grs.dbankcloud.asia	**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.
grs.platform.dbankcloud.ru	没有服务器地理信息.
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

URL线索

URL**信息**	Url**所在文件**

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

邮箱线索

手机线索

手机号	所在文件
17748595453	摸瓜V1引擎

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: CN=XiaoHuaQianBao
签名算法: rsassa_pkcs1v15
有效期自: 2015-12-04 06:21:15+00:00
有效期至: 3015-04-06 06:21:15+00:00
发行人: CN=XiaoHuaQianBao
序列号: 0x5f46e7da
哈希算法: sha256
md5值: 10a3730e538af07d24819b1fd5494b22
sha1值: d406ecf5cbb7868e9054afe14cd2529a02b1e9b3
sha256值: 60ee78c9f68590ec3ab73f5ead36046483f91e034681906591f2ef7aa714ffc1
sha512值: 9e0f7cffaf6d962db6c4cf988623eaee8b9746ab954df1e574cbe0356c176750b1e644b01c7457aa6238699b862ff63e1cc78592da879e75956c46824f5b46e6
公钥算法: rsa
密钥长度: 2048
指纹: 03cbb4d8c8acceb8c54528f1e584ae5d6cf37bf42158be3b9460a1a10bd97321

硬编码敏感信息

可能的敏感信息
"account_number_pwd_safety_signs" : "为了您的账号安全，请设置交易密码"
"again_input_pay_pwd" : "再次输入交易密码"

"exami_car_authentication" : "车辆认证，可获%s"

"forget_pay_pwd" : "忘记交易密码"

"forget_pwd" : "忘记密码"

"fotget_gesture_pwd" : "忘记手势密码?"

"gain_sms_auth_code" : "获取短信验证码"

"gt_one_login_auth_btn" : "一键登录"

"input_original_gesture_pwd" : "请输入原手势密码"

"input_pay_pwd" : "输入交易密码"

"input_pay_pwd_verify_id" : "请输入交易密码，以验证身份"

"input_sms_auth_code" : "请输入短信验证码"

"pay_pwd" : "交易密码"

"reset_gesture_pwd" : "重新设置手势密码"

"reset_pay_pwd" : "重新设置交易密码"

"security_public_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8hzUojzHX8jDL+97pqr7CaLiKSsZ0aOES7FUcX7vh9PoEDbCKNCTakRXdS5EiurPk3QpvsAGbfyIs7JWKm4py9KcIdJsZRh9onknVeAVlU++jnrGFGEYfQb8iKzClN059gYeeJBs9mwi7RGU9tj0KHUG659v5sMBxv7zNse3fJQIDAQAB"

"setting_gesture_pwd" : "重新设置手势密码"

"sms_auth_code_send_way" : "验证码将发送到您的新手机号,请注意查看"

"sms_auth_phone" : "验证码已发送至"

"sms_auth_resend" : "重新发送"
"sms_auth_title" : "请输入短信验证码"
"store_affirm_deal_pwd" : "确认交易密码"
"store_setting_deal_pwd" : "请设置交易密码"
"verify_gesture_pwd" : "验证手势密码"
"gt_one_login_auth_btn" : "一鍵登錄"
"gt_one_login_auth_btn" : "one-click login"

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

应用内通信

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。