



MoGua

夹米 0.0.3.APK 分析报告



APP名称:

夹米

包名: com.jiamiappprovip.app

域名线索: 6条

URL线索: 2条

邮箱线索: 1条

分析日期: 2025年8月10日

分析平台: [摸瓜APK反编译平台](#)

文件名: 2_jiami_v0.apk
文件大小: 114.49MB
MD5值: 4ae90d4746bbd94b26373d5840494e9a
SHA1值: 1a9623e6ce6e9ed88502a41d3239d9d2515ab30e
SHA256值: 7ff326db3bf838b488a1e3a50f67e85168887a72f27ffd9e0d2253d929cd5e1c

i APP 信息

App名称: 夹米
包名: com.jiamiappprovip.app
主活动Activity: com.jiamiappprovip.app.ui.activity.SplashActivity
安卓版本名称: 0.0.3
安卓版本: 3

🔍 域名线索

域名	服务器信息
grs.dbankcloud.eu	没有服务器地理信息.
github.com	IP: 20.205.243.166 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

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
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
www.jsdelivr.com	IP: 104.21.23.24 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

 URL线索

URL信息	Url所在文件
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.eu	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V2引擎

✉ 邮箱线索

邮箱地址	所在文件
sw@jiamivip.com kf@jiamivip.com media@jiamivip.com	摸瓜V1引擎

☰ 手机线索

✿ 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=JiaMi, OU=JiaMi, O=JiaMi, L=WuHan, ST=HuBei, C=cn
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-03 15:02:46+00:00
有效期至: 2050-05-28 15:02:46+00:00
发行人: CN=JiaMi, OU=JiaMi, O=JiaMi, L=WuHan, ST=HuBei, C=cn
序列号: 0x1
哈希算法: sha256
md5值: 31e59900b6b1a9355087cebae1594145
sha1值: dc27dcdb70b5242c73f1f432c8b5e09d1f3001c0
sha256值: c3c7ded23a76aa7a5f2c64efac0111fa594c5339894683dde2b5aff05a57d9f4
sha512值: bb6d6caa8eba85f20817a6da5f3c11a8ed904f7bf2e28d7f1b79925b997c4472514ebf42240db57de5619ec8868a102737a5d4cc0db6a8afc74c59cb64659ed6
公钥算法: rsa
密钥长度: 2048

硬编码敏感信息

可能的敏感信息
"account_security_alipay_auth": "支付宝授权"
"account_security_alipay_auth_tip": "确定绑定支付宝吗? "
"account_security_forget_pay_password": "忘记支付密码"
"account_security_password": "登录密码"
"account_security_set_teen_mode_password": "设置独立密码"
"account_security_wx_auth": "微信授权"
"account_security_wx_auth_btn": "去绑定"
"account_security_wx_auth_tip": "确定绑定微信吗? "
"authorization_for_use_personal_information": "《个人信息使用授权书》"
"contact_no_such_user": "该用户不存在"
"http_token_refresh": "Refresh"
"http_token_refresh1": "令牌过期, 将自动申请令牌"
"invite_code_authentication": "邀请码认证"
"invite_code_authentication_inviter": "邀请人: "

"invite_code_authentication_inviter_info" : "邀请人信息"
"invite_code_authentication_inviter_info_back" : "返回"
"invite_code_authentication_inviter_info_tips" : "一旦绑定，无法更改，请谨慎操作"
"invite_code_authentication_is_invalid" : "邀请码错误，请重新输入"
"invite_code_authentication_phone" : "手机号： "
"invite_code_authentication_tips" : "填写邀请码，享更多权益"
"ksad_ad_default_author" : "@可爱的广告君创造的原声"
"ksad_ad_default_username" : "@可爱的广告君"
"loading_go_auth" : "Go to Alipay for authorization"
"make_sure_payment_pwd_title" : "确认支付密码"
"modify_login_password_origin_pwd" : "原密码"
"password" : "密码"
"private_group" : "讨论组"
"real_authentication_agree" : "同意认证后，将同意您的个人信息用于认证"
"real_authentication_go_balance" : "去兑换余额"
"real_authentication_go_setup" : "去设置"
"real_authentication_id_card" : "身份证"

"real_authentication_id_card_tips" : "请输入正确的身份证号"
"real_authentication_name" : "姓名"
"real_authentication_pay" : "支付 ¥ 1.1 进行认证"
"real_authentication_pay_btn" : "确认支付"
"real_authentication_pay_failed" : "支付失败"
"real_authentication_pay_success" : "支付成功"
"real_authentication_pay_tips" : "需支付费用"
"real_authentication_pay_tips_1" : "认证信息错误导致失败，费用概不退回"
"real_authentication_pay_title" : "实名认证支付"
"real_authentication_phone" : "手机号"
"real_authentication_setup_success_tips" : "设置成功"
"real_authentication_submit" : "提交认证"
"real_authentication_tips" : "请进行实名认证，保护您的账号安全"
"real_authentication_tips_0" : "您尚未进行实名认证"
"real_authentication_tips_1" : "为了您的账号安全，请先进行实名认证"
"real_authentication_tips_2" : "夹米 信息安全保护中"
"real_authentication_title" : "实名认证"

"real_authentication_unset_pay_pwd_tips": "暂未设置支付密码，无法进行支付！ 请先设置支付密码再进行操作"
"setting_password": "修改密码"
"setting_payment_pwd_title": "设置支付密码"
"teenager_mode_make_sure_pwd_title": "确认支付密码"
"teenager_mode_pwd_title": "设置独立密码"
"loading_go_auth": "去支付宝授权"

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

	是		
--	---	--	--

向手机申请的权限	否 危 险	类型	详细情况
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.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.INTERNET	正 常	互联网接入	允许应用程序创建网络套接字
android.permission.MANAGE_EXTERNAL_STORAGE	危 险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.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
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.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.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.ACCESS_FINE_LOCATION	危	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

android.permission.ACCESS_FINE_LOCATION	危险	精细定位 (GPS)	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_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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.jiamiappprovip.app.permission.RECEIVE_MSG	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.jiamiappprovip.app.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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
com.jiamiappprovip.app.permission.KW_SDK_BROADCAST	未知	Unknown permission	Unknown permission from android reference
android.permission.SET_WALLPAPER	正常	设置壁纸	允许应用程序设置系统壁纸
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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
com.android.launcher.permission.INSTALL_SHORTCUT	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.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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
com.jiamiappprovip.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent102794740://,