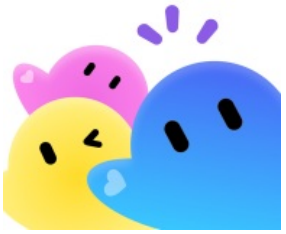
MoGua

酷友i 2.0.1.APK 分析报告



APP名称: 酷友i

包名:	com.malelive.zbsznew
域名线索:	9条
URL线索:	2条
邮箱线索:	0条
分析日期:	2025年6月15日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: ky201new.apk
文件大小: 61.95MB
MD5值: 875216c494a373ab316e3a1edc462197
SHA1值: c3ae2eb46d2564439ad174c2e4fa414719c3284f
SHA256值: 36864919bf091b2feb09ca099e9e52e873fda4f1aa76d5e4fbd8684e2132ac00

APP 信息

App名称: 酷友i
包名: com.malelive.zbsznew
主活动Activity: com.malelive.zbsznew.activity.LauncherActivity
安卓版本名称: 2.0.1
安卓版本: 9

域名线索

域名	服务器信息
c.appjiagu.com	**IP**: 106.63.25.12 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
sharesdk.cn	**IP**: 115.227.43.65 **所属国家**: China **地区**: Zhejiang **城市**: Jiaxing **纬度**: 30.752199 **经度**: 120.750000
www.mob.com	**IP**: 180.188.26.28 **所属国家**: China **地区**: Zhejiang

	城市: Taizhou **纬度**: 28.666668 **经度**: 121.349998
mob.com	**IP**: 116.62.130.46 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
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
android.googlesource.com	**IP**: 173.194.202.82 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
dev.yinxiang.com	**IP**: 140.143.50.251 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
streams.videolan.org	**IP**: 213.36.253.119 **所属国家**: France **地区**: Ile-de-France **城市**: Paris **纬度**: 48.859077 **经度**: 2.293486

www.sharesdk.cn	**IP**: 115.227.43.65 **所属国家**: China **地区**: Zhejiang **城市**: Jiaxing **纬度**: 30.752199 **经度**: 120.750000

URL线索

URL信息	Url所在文件
https://github.com/vinc3m1	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView.git	摸瓜V1引擎
http://www.mob.com/about/policy>http://www.mob.com/about/policy	摸瓜V1引擎
http://www.mob.com	摸瓜V1引擎
http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en.If	摸瓜V1引擎
https://streams.videolan.org/upload/	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎
http://dev.yinxiang.com/support/	摸瓜V3引擎
http://schemas.android.com/apk/res/android11net.lucode.hackware.magicindicator.MagicIndicator	摸瓜V3引擎
http://www.sharesdk.cn/	摸瓜V3引擎

https://android.googlesource.com/toolchain/clang	摸瓜V3引擎
https://github.com/opencv/opencv/issues/6293	摸瓜V3引擎
https://www.sharesdk.cn	摸瓜V3引擎
http://www.sharesdk.cn	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm	摸瓜V3引擎
http://sharesdk.cn	摸瓜V3引擎
http://c.appjiagu.com/apk/cr.html	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
http://mob.com	摸瓜V3引擎

邮箱线索

手机线索

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

签名算法: rsassa_pkcs1v15
有效期自: 2022-11-08 04:25:32+00:00
有效期至: 2047-11-02 04:25:32+00:00
发行人: C=CN
序列号: 0x6134ebe9
哈希算法: sha256
md5值: d373572d4fbd1063dec7be488e051fbf
sha1值: b24285c57d15b2434054805508dc55c88ca19dda
sha256值: 8994456aac99283dd66b6421b9baa265306ea3058c1760b00ba0950e2fbaced8
sha512值: 37b09bb665933e93ee0310f19fb168217a9ec68a0fe3afebea08e0c8115786a8efe1ce6a6a5c85a1e17f717f76e2c85d9e6ba2eb47da282d13d74caca9e77507
公钥算法: rsa
密钥长度: 2048
指纹: d4873710485d3a7837d0225974186f253e473ff7a9b30ef8d8ac6adfca5c8336

硬编码敏感信息

可能的敏感信息
"cash_input_bank_user_name" : "请输入持卡人姓名"
"find_pwd_find" : "立即找回"
"find_pwd_forget" : "忘记密码"
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"live_input_password" : "请输入房间密码"
"live_room_type_pwd" : "本房间为密码房间，请输入密码"
"live_set_pwd" : "请设置房间密码"
"login_auth_cancle" : "授权取消"

"login_auth_failure" : "授权失败"

"login_auth_ing" : "正在授权登录"

"login_auth_success" : "登录成功"

"login_forget_pwd" : "忘记密码"

"login_input_pwd" : "请输入密码"

"main_live_type_pwd" : "密码房间"

"mobdemo_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见http://www.mob.com/about/policy。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"

"mobdemo_authorize_dialog_title" : "服务授权"

"modify_pwd" : "重置密码"

"reg_input_pwd_1" : "请填写密码"

"reg_input_pwd_2" : "请确认密码"

"ssdk_cmcc_auth" : "手机认证服务由中国移动提供"

"ssdk_cmcc_login_one_key" : "本机号码一键登录"

"ssdk_instapaper_pwd" : "密码"

"ssdk_weibo_oauth_regiseter" : "应用授权"

"mobdemo_authorize_dialog_content" : "In order to provide you with Mobservice related products and services, please check our privacy policy in detail, see detailshttp://www.mob.com/about/policy/en.If you agree with our privacy policy, please click accept. If you disagree with our privacy policy, please click reject."

ncy, please click reject.
"mobdemo_authorize_dialog_title" : "service authority"
"ssdk_cmcc_auth" : "Provided by China Mobile"
"ssdk_cmcc_login_one_key" : "PhoneNum Login"
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"

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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.NETWORK_PROVIDER	未知	Unknown permission	Unknown permission from android reference
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

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.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.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.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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
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.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。
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作
android.permission.RECEIVE_USER_PRESENT	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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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

com.malelive.zxbhdandroid.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.braintreepayments.api.BraintreeBrowserSwitchActivity	Schemes: com.yunbao.phonelive.braintree://,
cn.sharesdk.tencent.qq.ReceiveActivity	Schemes: tencent101551222://,
com.tencent.tauth.AuthActivity	Schemes: tencent101555598://,
cn.sharesdk.onekeyshare.LineAuthenticationCallbackActivity	Schemes: lineauth://,