



MoGua

闲赚侠 1.0.8.APK 分析报告



APP名称:

闲赚侠

包名:	com.ouqi.xianzhuanxia
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年6月29日
分析平台:	摸瓜APK反编译平台

文件名: com.ouqi.xianzhuanxia_1.0.8_9.apk
文件大小: 35.58MB
MD5值: f1baf0e5e10f669699eb32436e4f4268
SHA1值: 0d489c19945b34837f6573312b6b8e70c7b2cad6
SHA256值: 7b0477cd46688b85034af0208bc415e3c9962da11a57936ca65833ca89ab327e

i APP 信息

App名称: 闲赚侠
包名: com.ouqi.xianzhuanxia
主活动Activity: com.sifou.wanhe.login.activity.WelcomeActivity
安卓版本名称: 1.0.8
安卓版本: 9

🔍 域名线索

域名	服务器信息
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

🌐 URL线索

URL信息	Url所在文件
https://github.com/vinc3m1	Mogua Engine V1

https://github.com/vinc3m1/RoundedImageView	Mogua Engine V1
https://github.com/vinc3m1/RoundedImageView.git	Mogua Engine V1

 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: False
找到 1 个唯一证书
主题: C=86, ST=广州, L=广州, O=速狐科技, OU=速狐科技, CN=速狐科技
签名算法: rsassa_pkcs1v15
有效期自: 2021-07-14 06:50:37+00:00
有效期至: 2046-07-08 06:50:37+00:00
发行人: C=86, ST=广州, L=广州, O=速狐科技, OU=速狐科技, CN=速狐科技
序列号: 0x13c9c1f4
哈希算法: sha256
md5值: cb7d1b648d769f73d0e380c23fede15e
sha1值: 3586af62aec0602eb8beb35e17df8ce247b49027
sha256值: 06d46228a0ebdc8a7ae23e35a1d0e41eef9b4eeb3a9309fb2741903bedf72a60
sha512值: 93a54020e23052fefc524dbcc8b98682e2bb3325d7e385c8dab73d092e287922053a5181227f1143809406817a507fa1ce54afa92db62517956360ed52da0c61
公钥算法: rsa
密钥长度: 2048
指纹: d057adba2f0f36b35a0230ec7c92967279cfbd6ddfa9fb95424d429968a4926f

 硬编码敏感信息

--

可能的敏感信息
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"mq_auth_code" : "验证码"
"private_agree" : "点击同意,即表示您已阅读并同意"
"private_content" : " 亲,感谢您信任以及使用本应用。 我们依据最新的监管要求更新了闲赚侠的《隐私协议》,特向您进行如下说明: 1、为向您提供使用、交易相关基本功能,我们会收集、使用必要的信息; 2、基于您的明示授权,不限于启动、应用运行时,我们可能会获取您的位置(为您提供附近的商品、交易信息、优惠资讯等)、设备号信息(为保障您的账号与交易安全)、软件列表(分享商品和邀请好友的支持)等信息,使用MAC地址、IMEI、IMSI来标记用户,您有权拒绝或取消授权; 3、我们会采取相关的安全措施保护您的信息安全; 4、未经您的同意,我们不会从第三方处获取、共享或向其提供您的信息。 "
"mq_auth_code" : "CAPTCHA"
"mq_auth_code" : "Kode verifikaso"
"mq_auth_code" : "Kod pengesahan"
"mq_auth_code" : "驗證碼"

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.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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.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.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。
getui.permission.GetuiService.com.ouqi.xianzhuanxia	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.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.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.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
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

android.permission.INSTALL_SHORTCUT	正常		允许应用程序在启动器中安装快捷方式
android.permission.UNINSTALL_SHORTCUT	正常		不要在您的应用中使用此权限。不再支持此权限
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher2.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher3.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher3.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adw.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adw.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference

com.qihoo360.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.qihoo360.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.lge.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.lge.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
net.qihoo.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
net.qihoo.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adwfreak.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adwfreak.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adw.launcher_donut.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adw.launcher_donut.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher3.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher3.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.fede.launcher.permission.READ_SETTINGS	未	Unknown	Unknown permission from android reference

	知	permission	
com.fede.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.sec.android.app.twlauncher.settings.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.sec.android.app.twlauncher.settings.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.anddoes.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.anddoes.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.tencent.qqlauncher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.tencent.qqlauncher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher2.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.mylauncher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.mylauncher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.ebproductions.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference

com.ebproductions.android.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	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.huawei.android.launcher.permission.WRITE_SETTINGS	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
telecom.mdesk.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
telecom.mdesk.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
dianxin.permission.ACCESS_LAUNCHER_DATA	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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.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
com.ouqi.xianzhuanxia.openadsdk.permission.TT_PANGOLIN	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
org.simalliance.openmobileapi.SMARTCARD	未知	Unknown permission	Unknown permission from android reference
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
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
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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
android.permission.READ_PRIVILEGED_PHONE_STATE	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: tencent102039722://, tencent101962629://,
com.sifou.wanhe.wxapi.AliEntryActivity	Schemes: umpay://,
com.sifou.wanhe.login.activity.WelcomeActivity	Schemes: sifoupay://, sifouwanhe://, mtj6f0459e003://, Path Prefixes: /order,
com.sifou.wanhe.web.AliCommonWebActivity	Schemes: esign://, Hosts: facesdk,
com.sifou.wanhe.web.CommonWebActivity	Schemes: esign://, Hosts: facesdk,