



# MoGua

## 69 3.8.01.APK 分析报告



包名: com.XFvpCUERKcQ0aIAX.jeYEV0a1RsXTJybM

域名线索: 3条

URL线索: 3条

邮箱线索: 1条

分析日期: 2024年10月30日

分析平台: [摸瓜APK反编译平台](#)

文件名: 69zb-p8Yik-v1d8e32f4.apk

文件大小: 59.76MB

MD5值: 699412f2d0bcbf1bae31fedde83b963b

SHA1值: 89df0558922a8292016ad2b12dea535373a81e67

SHA256值: 28002664d213e740dd8b6facb3dd7ec1fece58c19a4f61b5724749144773c63e

## i APP 信息

App名称: 69

包名: com.XFvpCUERkCQ0alAX.jeYEV0a1RsXTJybM

主活动Activity: com.xx.live.ui.activity.SplashActivity

安卓版本名称: 3.8.01

安卓版本: 3801

## 🔍 域名线索

域名	服务器信息
www.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
www.w3.org	IP: 104.18.22.19 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
<a href="https://github.com/vinc3m1">https://github.com/vinc3m1</a>	摸瓜V1引擎
<a href="https://github.com/vinc3m1/RoundedImageView">https://github.com/vinc3m1/RoundedImageView</a>	摸瓜V1引擎
<a href="https://github.com/vinc3m1/RoundedImageView.git">https://github.com/vinc3m1/RoundedImageView.git</a>	摸瓜V1引擎
<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>	摸瓜V2引擎
<a href="https://github.com/ecomfe/zrender/blob/master/LICENSE.txt">https://github.com/ecomfe/zrender/blob/master/LICENSE.txt</a>	摸瓜V2引擎
<a href="http://schemas.android.com/aapt">http://schemas.android.com/aapt</a>	摸瓜V3引擎
<a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>	摸瓜V3引擎
<a href="http://schemas.android.com/apk/res-auto">http://schemas.android.com/apk/res-auto</a>	摸瓜V3引擎
<a href="http://schemas.android.com/apk/res-auto">www.googleapis.com</a>	摸瓜V3引擎
<a href="http://schemas.android.com/apk/res-auto">http://schemas.android.com/apk/res-auto</a>	摸瓜V3引擎

## 邮箱线索

邮箱地址	所在文件

## 手机线索

## 签名证书

无法读取代码签名证书.

## 硬编码敏感信息

可能的敏感信息
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"djw_input_fund_password" : "输入支付密码"
"ease_search_block_user" : "Search"
"expend_member_user" : "用户"
"forget_password_password" : "密码"
"get_auth_code" : "发送验证码"
"google_api_key" : "AlzaSyCwIO0cLzfbWGjy9UBURWLSNWcoaYikz7s"
"google_crash_reporting_api_key" : "AlzaSyCwIO0cLzfbWGjy9UBURWLSNWcoaYikz7s"
"input_auth_code" : "请填写验证码"

"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"live_player_private_status_msg1" : "您的礼物贡献暂未能达到私信主播的要求! "
"live_player_private_status_msg2" : "请最低赠送价值%s的礼物才能开启私信功能"
"login_account_forget_password" : "忘记密码? "
"login_account_password" : "密码"
"login_account_remember_password" : "记住密码"
"login_account_username" : "用户名"
"my_safety_certificate" : "安全认证"
"please_input_password" : "请输入密码"
"please_input_username" : "请输入账号"
"register_password" : "密码"
"register_username" : "账号"
"system_payment_password" : "支付密码"
"system_safety_certificate" : "安全认证"
"withdraw3_forget_pwd" : "忘记密码? "
"withdraw3_password" : "支付密码"

"ease\_search\_block\_user": "搜索"

## 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.READ_MEDIA_VISUAL_USER_SELECTED	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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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
com.android.launcher.permission.READ_SETTINGS	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
com.re.ng.uulive.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
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.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.google.android.gms.permission.AD_ID	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_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
com.asus.msa.SupplementaryDID.ACCESS	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
freemme.permission.msa.SECURITY_ACCESS	未知	Unknown permission	Unknown permission from android reference
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
com.asus.permission.READ_SDID_PROVIDER	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。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference

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.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
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
android.permission.READ_CLIPBOARD_IN_BACKGROUND	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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。
android.permission.OBSERVE_GRANT_REVOKE_PERMISSIONS	未知	Unknown permission	Unknown permission from android reference
com.XFvpCUERkCQ0alAX.jeYEV0a1RsXTJybM.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.BIND_REMOTEVIEWS	合法		RemoteViewsService 必须要求,以确保只有系统可以绑定到它
android.permission.DETECT_SCREEN_CAPTURE	未知	Unknown permission	Unknown permission from android reference

# 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。