MoGua

69 3.8.01.APK 分析报告

APP名称: 69

包名:	orz.yemuwzlpxq.lgkqysvapy
域名线索:	2条
URL线索:	2条
邮箱线索:	0条
分析日期:	2024年10月30日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 69_225839652.apk
文件大小: 58.62MB
MD5值: 38bfcc4be023deeb46938ff0f06d63e3
SHA1值: 21430958f8544b4bdcfbcb902d6e83cdc87c14a4
SHA256值: ccdefc5a55225529d71863cb092c11a3f8fa9bd266bb7a760ca166503965831c

APP 信息

App名称: 69
包名: orz.yemuwzlpxq.lgkqysvapy
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
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
static.yximgs.com	**IP**: 101.73.101.239 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081

URL线索

URL信息	Url所在文件
https://static.yximgs.com/udata/pkg/kwai-client-image/gzone/wish_list_gift_effects_default_new.png	db7/b.java
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

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2024-10-29 14:53:13+00:00
有效期至: 2079-08-02 14:53:13+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x9b704d15dceee26e
哈希算法: sha256
md5值: b9056ca38a80673877e05297f89121ae
sha1值: 26b30169c2fac82aac80e46b76860d0a66c90fd6
sha256值: 31eda38d0858931a41886ebfd2d52d2a94c59eb5294bfef3de505af0d60ae9fa
sha512值: fceda5bc8b1dde69bbd53eb4e5765921c2fd36d50566cf21dc6a046a053225b557a54835608f7abfeda31a7b8055f1da730d70beb30117bcbc50ffde0525b068

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" : "输入支付密碼"
"ease_search_block_user" : "Search"
"expend_member_user" : "用户"
"forget_password_password" : "密码"
"get_auth_code" : "发送验证碼"
"google_api_key" : "AIzaSyCwlO0cLzfbWGjy9UBURWLsNWcoaYikz7s"
"google_crash_reporting_api_key" : "AIzaSyCwlO0cLzfbWGjy9UBURWLsNWcoaYikz7s"
"input_auth_code" : "请填写驗证碼"
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"live_player_private_status_msg1" : "您的礼物贡獻暂未能达到私信主播的要求！"
"live_player_private_status_msg2" : "请最低赠送價值%s的礼物才能開啓私信功能"
"login_account_forget_password" : "忘记密码？"
"login_account_password" : "密碼"

"login_account_remember_password" : "記住密碼"
"login_account_username" : "用户名"
"my_safety_certificate" : "安全认证"
"please_input_password" : "請輸入密碼"
"please_input_username" : "请输入賬號"
"register_password" : "密码"
"register_username" : "账号"
"system_payment_password" : "支付密碼"
"system_safety_certificate" : "安全认證"
"withdraw3_forget_pwd" : "忘记密码？"
"withdraw3_password" : "支付密碼"
"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.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
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.launcher.permission.READ_SETTINGS	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.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_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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
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_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.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
com.re.ng.uulive.permission.JPUSH_MESSAGE	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.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
	危		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

android.permission.CAMERA	险	拍照和录像	到的图像
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.OBSERVE_GRANT_REVOKE_PERMISSIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.DETECT_SCREEN_CAPTURE	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.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.asus.permission.READ_SDID_PROVIDER	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
freemme.permission.msa.SECURITY_ACCESS	未知	Unknown permission	Unknown permission from android reference
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.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_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
orz.yemuwzlpxq.lgkqysvapy.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

应用内通信