MoGua

瓜子影视 1.9.2.APK 分析报告

APP名称:	瓜子影视

包名:	com.secondhand.money
域名线索:	8条
URL线索:	4条
邮箱线索:	1条
分析日期:	2025年5月28日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: gzys.apk
文件大小: 39.81MB
MD5值: 53174d7628937c8824e0825317cfce9b
SHA1值: bf773a4eb212937d4e6c3b03d969f7124bfedc39
SHA256值: eb8ffda1f3d6680f598ee81eafbf89dc1a27eb2192be1f9ee4e7eaedaef90453

APP 信息

App名称: 瓜子影视
包名: com.secondhand.money
主活动Activity: com.movie.firstIn.activity.splash.SplashActivity
安卓版本名称: 1.9.2
安卓版本: 2406025

域名线索

域名	服务器信息
gcc.gnu.org	**IP**: 8.43.85.97 **所属国家**: United States of America **地区**: North Carolina **城市**: Raleigh **纬度**: 35.773994 **经度**: -78.632759
www.openssl.org	**IP**: 34.49.79.89 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
android.googlesource.com	**IP**: 172.253.117.82 **所属国家**: United States of America **地区**: California

	城市: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.hpplay.com.cn	**IP**: 123.6.82.136 **所属国家**: China **地区**: Henan **城市**: Zhengzhou **纬度**: 34.757778 **经度**: 113.648613
tvapp-openclient.yiboapp.tv	没有服务器地理信息.
errlogos.umeng.com	**IP**: 47.246.110.18 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
www.gstatic.com	**IP**: 203.208.43.66 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
errlog.umeng.com	**IP**: 223.109.148.143 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992

URL线索

URL信息	Url所在文件
http://www.hpplay.com.cn/	摸瓜V1引擎
https://tvapp-openclient.yiboapp.tv	摸瓜V1引擎
https://android.googlesource.com/toolchain/llvm	摸瓜V3引擎
infinitedata-pa.googleapis.com	摸瓜V3引擎
https://android.googlesource.com/toolchain/clang	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎
firebaseinstallations.googleapis.com	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
instantmessaging-pa.googleapis.com	摸瓜V3引擎
www.googleapis.com	摸瓜V3引擎
gmscompliance-pa.googleapis.com	摸瓜V3引擎
clientservices.googleapis.com	摸瓜V3引擎
www.gstatic.com	摸瓜V3引擎
http://gcc.gnu.org/bugs.html):	摸瓜V3引擎
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so

https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so

邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

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: OU=sdfsa, CN=asdf
签名算法: rsassa_pkcs1v15
有效期自: 2020-11-09 07:23:09+00:00
有效期至: 2045-11-03 07:23:09+00:00
发行人: OU=sdfsa, CN=asdf
序列号: 0x3d5b3b4
哈希算法: sha256
md5值: c23806ba4be69398a7b44012e2f51159
sha1值: 2f5e572e64b4ed3082e9e80cc8035c7115cd67fb

sha256值: 2daa94115dc5c48038693654ffcc3aa095cbd093165b47bd7f15c8f83ca1bc9b
sha512值: f621288c5e699a5ac4e194ed9d69ab3f5c8bfee87d68617e48b9491d7afecf6722c5eecbbf067cd587422b70dc071a39b92a25ecd6db12ca722a443cab64ddc9
公钥算法: rsa
密钥长度: 2048
指纹: 3fbc293e16e09bb71de852db54edc480858c60ff956b0b851bdc53781612950f

硬编码敏感信息

可能的敏感信息
"comment_reply_user_name" : "回复@%s:"
"google_api_key" : "AIzaSyBuIOzfKN-XAI1UJ5HisclnXI1WH0Y2F7M"
"google_crash_reporting_api_key" : "AIzaSyBuIOzfKN-XAI1UJ5HisclnXI1WH0Y2F7M"
"login_forger_password" : "忘记密码"
"login_input_password" : "请输入您的密码"
"setEmail_input_password" : "请输入您的密码"

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
com.secondhand.money.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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.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_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率

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.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
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
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
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_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.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.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.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.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.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.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.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.GET_PACKAGE_SIZE	正常	测量应用程序存储空间	允许应用程序找出任何包使用的空间
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_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.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.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.secondhand.money.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.secondhand.money.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	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
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
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.movie.firstIn.activity.homepage.HomepageActivity	Schemes: puvideo://, Hosts: video,
com.movie.firstIn.activity.splash.SplashActivity	Schemes: ay56to://, sa13f27bec://,

---