MoGua

絮语 9.07.APK 分析报告

APP名称:	絮语

包名:	me.wI01qN3I.HY69t3wg
域名线索:	4条
URL线索:	8条
邮箱线索:	0条
分析日期:	2025年6月30日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: base.apk
文件大小: 31.14MB
MD5值: c341f8e6f9c75f545097acb1205765fe
SHA1值: 1ed35ff63aca27ea82cc13a171c1084319b8b5fc
SHA256值: c4eef64d6e0ee46062c8928c273736aa8638c96fa4771a124b7956f1db4bbd71

APP 信息

App名称: 絮语
包名: me.wl01qN3I.HY69t3wg
主活动Activity: .main
安卓版本名称: 9.07
安卓版本: 970

域名线索

域名	服务器信息
android.googlesource.com	**IP**: 74.125.20.82 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
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
img03.sogoucdn.com	**IP**: 123.125.244.83 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397102
schemas.android.com	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://github.com/kongzue/DialogX/wiki	com/kongzue/dialogx/DialogX.java
https://github.com/kongzue/DialogX	com/kongzue/dialogx/interfaces/BaseDialog.java
https://github.com/kongzue/DialogX	com/kongzue/dialogx/impl/ActivityLifecycleImpl.java
http://img03.sogoucdn.com/app/a/100520146/ad76ed07d7ea2e1628203d16af27320d	com/example/glidetest/MainActivity.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://schemas.android.com/aapt	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
https://github.com/kongzue/DialogX	摸瓜V3引擎
https://github.com/kongzue/DialogX/wiki	摸瓜V3引擎

https://android.googlesource.com/toolchain/llvm-project	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm	摸瓜V3引擎
http://img03.sogoucdn.com/app/a/100520146/ad76ed07d7ea2e1628203d16af27320d	摸瓜V3引擎
https://android.googlesource.com/toolchain/clang	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=WFrxOLYf7UaGPgth, ST=rgGcD5aFjIsI1p5B, L=y4ldNcNGKxRSoq0o, O=g9A1751068681364, OU=CXV1751068681364, CN=Q0nI61751068681364
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-27 23:58:01+00:00
有效期至: 2075-06-27 23:58:01+00:00
发行人: C=WFrxOLYf7UaGPgth, ST=rgGcD5aFjIsI1p5B, L=y4ldNcNGKxRSoq0o, O=g9A1751068681364, OU=CXV1751068681364, CN=Q0nI61751068681364
序列号: 0x48a842a978f6d3da
哈希算法: sha256
md5值: 1a2b9daea66a0fac2a0113d94a6ba775
sha1值: 0e739ed7791399ee05a279b629867e119fef8924
sha256值: e46d9477a42f954108a460f62e338db7ba5f680f991e800c2919061892ac6724
sha512值: a4653c421991128ee17ec6fb41a97f06ab775ce9e85f6b706d0acb88531f0059e502f4ba661833477ff1967d4087a9c4fe215f42a4a3abf5072f5f854e46e821
公钥算法: rsa
密钥长度: 2048
指纹: cf086688dbfb639af128c8633f558b96df15576813932f6052c461cb70d328ff

硬编码敏感信息

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_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.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_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_NOTIFICATION_POLICY	正常		希望访问通知策略的应用程序的标记权限。
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.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
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
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

应用内通信
