



MoGua

AI色色 1.9.0.APK 分析报告



APP名称:

AI色色

包名:	cn.kyewy.lpgiet
域名线索:	9条
URL线索:	6条
邮箱线索:	1条
分析日期:	2025年7月6日
分析平台:	摸瓜APK反编译平台

文件名: aisese_1.9.0_250701_6.apk
文件大小: 30.68MB
MD5值: 23c9ccd42c58fc0832d6b92b184aebdd
SHA1值: 25f8d590d40fdc906c950d1b49904b18810c941c
SHA256值: 100d029f0f1fbf7155412b126d66f553a40bff009e0524b78d11f7f93f0b9b17

i APP 信息

App名称: AI色色
包名: cn.kyewy.lpgiet
主活动Activity: com.views.mai.MainActivity
安卓版本名称: 1.9.0
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
www.unicode.org	IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204
developer.android.com	IP: 142.251.33.78 所属国家: Canada 地区: Ontario

	城市: Toronto 纬度: 43.653660 经度: -79.382927
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
docs.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
aomedia.org	IP: 192.133.77.197 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
www.google.cn	IP: 114.250.69.34 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
dartbug.com	IP: 216.239.32.21 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
	IP: 34.111.97.67

developer.mozilla.org	所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
-----------------------	--

URL线索

URL信息	Url所在文件
https://docs.flutter.dev/deployment/android	io/flutter/embedding/engine/loader/FlutterLoader.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/PlatformPlugin.java
https://www.google.cn/intl/zh-CN/chrome	摸瓜V2引擎
https://aomedia.org/emsg/ID3	摸瓜V2引擎
https://github.com/richttr/NoSleep.js/issues/15	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)	摸瓜V2引擎
http://www.unicode.org/copyright.html	lib/arm64-v8a/libflutter.so
https://github.com/flutter/flutter/issues.	lib/arm64-v8a/libflutter.so
https://dartbug.com/52121.	lib/arm64-v8a/libflutter.so

邮箱线索

--	--

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libflutter.so

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

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: CN=Android Debug, O=Android, C=US
签名算法: rsassa_pkcs1v15
有效期自: 2022-11-03 10:16:02+00:00
有效期至: 2052-10-26 10:16:02+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha1
md5值: 7d8a2c0d2493e5d6d85c3865d0918482
sha1值: 7682ef35f017d1b3d352557971c295a6885fae4c
sha256值: 7b86e6199d7c910d075153a0fe61cf241a4b390dd5f4dd0a74381dab7cf42b6f
sha512值: 5d1a8d09f651ee318f3411e559df66a5439dfea5538839f3bc527c6fa3a0671d1326e28949e56f2766e9f716b69ff5ecb1298370c4bb59b7701a43ef4744178b
公钥算法: rsa
密钥长度: 2048
指纹: a715c81d7c87ff29afca669875aed119aeed1a6f489b5d567f6e4c3922f04e1f

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.DOWNLOAD_WITHOUT_NOTIFICATION	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
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.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
cn.kyewy.lpgiet.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

