



MoGua

泡芙短视频 4.7.9.APK 分析报告



APP名称:

泡芙短视频

包名:	com.lot0y.ZelgK
域名线索:	8条
URL线索:	6条
邮箱线索:	1条
分析日期:	2025年6月18日
分析平台:	摸瓜APK反编译平台

文件名: dsp4.7.9.apk
文件大小: 46.28MB
MD5值: c09e25757e5c51f115e39ecc51fa9f91
SHA1值: 6fbac5a38868b01bca718589f81fe823ea79b11a
SHA256值: adcd3b0239226cc0a4cbfe605c5a1620b75053f5175b9105d80677ee18805ab0

i APP 信息

App名称: 泡芙短视频
包名: com.lotOy.ZelgK
主活动Activity: com.example.pf.MainActivity
安卓版本名称: 4.7.9
安卓版本: 700

🔍 域名线索

域名	服务器信息
dnlq8umwclsn5.cloudfront.net	IP: 3.166.216.96 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
journeyapps.com	IP: 18.65.168.3 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
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
dartbug.com	IP: 216.239.34.21 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
api.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
www.jsdelivr.com	IP: 172.67.208.113 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
developer.mozilla.org	IP: 34.111.97.67 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://journeyapps.com/	摸瓜V1引擎
https://github.com/journeyapps/zxing-android-embedded	摸瓜V1引擎
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V2引擎
https://github.com/apvarun/toastify-js	摸瓜V2引擎
https://github.com/nodeca/pica	摸瓜V2引擎
https://github.com/richtr/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
https://github.com/flutter/flutter/issues	lib/arm64-v8a/libflutter.so
https://dartbug.com/52121	lib/arm64-v8a/libflutter.so
https://dnlq8umwclsn5.cloudfront.net	lib/arm64-v8a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so

邮箱线索

邮箱地址	所在文件
android@openjdk.org	lib/arm64-v8a/libflutter.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: C='中国', ST='北京', L='北京', O='北京', OU='北京', CN='中国'

签名算法: rsassa_pkcs1v15

有效期自: 2024-12-03 09:40:03+00:00

有效期至: 2034-12-01 09:40:03+00:00

发行人: C='中国', ST='北京', L='北京', O='北京', OU='北京', CN='中国'

序列号: 0x32f82a6a

哈希算法: sha256

md5值: f323e04187cef7ffea7f53ee14948209

sha1值: 030205ea55e0d6a1a803cb4cd8658510cd9052d2

sha256值: a51596c4e1f9ddb86f881985c65bf234c202c602304fad6c5cd57c79a1edfd29

sha512值: 83d72dc7458f2a4eecb5d1a8c2c4aa774bbbd7d1c8f70a7b0e8aa7f4f3a1a118ead987d2ae6a66da154945edc2a209eaae1e384b234293fe5356e31854e2980

公钥算法: rsa

密钥长度: 2048

指纹: 110b0151e71634f70c9bf435d7f1c38ffee9ca2322c2ab56713926ed5f0868bf

硬编码敏感信息

可能的敏感信息
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

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
android.permission.KILL_BACKGROUND_PROCESSES	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.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_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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
com.lotOy.ZelgK.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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。