



MoGua

51猎奇 1.3.0.APK 分析报告



APP名称:

51猎奇

包名: 51lieqi_1.3.0_230829_1.apk

域名线索: 21条

URL线索: 18条

邮箱线索: 2条

分析日期: 2025年10月12日

分析平台: [摸瓜APK反编译平台](#)

文件名: 51lieqi_1.3.0_230829_1.apk
文件大小: 17.97MB
MD5值: 05a97754ba95385269adbee0774120b1
SHA1值: 53bb22f111acfcc2edd6fc4da19b5ba71be414d0
SHA256值: 10add784d3a772c9ad04b9eceac5d61d40c4c02aa5068210cebcbff1f9868adf1

i APP 信息

App名称: 51猎奇
包名: 51lieqi_1.3.0_230829_1.apk
主活动Activity: []
安卓版本名称: 1.3.0
安卓版本: 1004

🔍 域名线索

域名	服务器信息
schemas.microsoft.com	IP: 13.107.213.74 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.jsdelivr.com	IP: 216.24.57.253 所属国家: United States of America 地区: California

	城市: San Francisco 纬度: 37.775700 经度: -122.395203
51lqapi.51lq.me	IP: 104.21.8.228 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
github.com	IP: 192.30.255.112 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
aomedia.org	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
51lqapi.mtaoapi006.org	IP: 104.21.65.51 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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

127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
www.ibm.com	IP: 23.51.45.93 所属国家: Malaysia 地区: Selangor 城市: Cyberjaya 纬度: 2.922500 经度: 101.654999
exoplayer.dev	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
ns.adobe.com	没有服务器地理信息.
data.flurry.com	IP: 69.147.88.8 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.731323 经度: -73.990089
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
	IP: 199.36.158.100 所属国家: United States of America

flutter.dev	地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
proton.flurry.com	没有服务器地理信息.
developer.apple.com	IP: 17.253.67.204 所属国家: Australia 地区: New South Wales 城市: Sydney 纬度: -33.867779 经度: 151.207047
raw.githubusercontent.com	IP: 185.199.109.133 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
51lqapi.mtaoapi006.info	IP: 104.21.80.65 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
staff.tea123.me	IP: 104.21.71.17 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
developer.android.com	IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View

纬度: 37.405991
经度: -122.078514

 URL线索

URL信息	Url所在文件
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/e.java
https://github.com/flutter/flutter/issues/2897).It	io/flutter/plugin/platform/l.java
https://developer.android.com/reference/javax/net/ssl/SSLSocket	io/flutter/plugins/d/t.java
https://proton.flurry.com/sdk/v1/config	c/d/b/s.java
https://data.flurry.com/aap.do	c/d/b/k0.java
http://data.flurry.com/aap.do	c/d/b/k0.java
https://data.flurry.com/pcr.do	c/d/b/a0.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	c/e/a/a/g2.java
http://www.w3.org/ns/ttml	c/e/a/a/v2/s/c.java
https://exoplayer.dev/issues/cleartext-not-permitted	c/e/a/a/x2/z.java
https://x</LA_URL>	c/e/a/a/p2/j0.java
https://x	c/e/a/a/p2/j0.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	c/e/a/a/p2/k0.java

http://ns.adobe.com/xap/1.0/	c/e/a/a/q2/h0/a.java
https://aomedia.org/emsg/ID3	c/e/a/a/s2/j/a.java
https://developer.apple.com/streaming/emsg-id3	c/e/a/a/s2/j/a.java
http://ns.adobe.com/xap/1.0/\u0000	b/c/a/a.java
https://www.jsdelivr.com/using-sri-with-dynamic-files	Mogua Engine V2
https://github.com/apvarun/toastify-js	Mogua Engine V2
https://github.com/richtr/NoSleep.js/issues/15	Mogua Engine V2
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released	Mogua Engine V2
http://www.w3.org/XML/1998/namespace	lib/armeabi-v7a/libflutter.so
http://www.w3.org/2000/xmlns/	lib/armeabi-v7a/libflutter.so
https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues.	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues/73620.	lib/armeabi-v7a/libflutter.so
http://www.w3.org/1998/Math/MathML	lib/armeabi-v7a/libapp.so
http://www.w3.org/2000/svg	lib/armeabi-v7a/libapp.so
http://www.w3.org/2000/xmlns/	lib/armeabi-v7a/libapp.so
https://51lqapi.mtaoapi006.info/api.php	lib/armeabi-v7a/libapp.so
http://127.0.0.1:	lib/armeabi-v7a/libapp.so

https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html	lib/armeabi-v7a/libapp.so
https://51lqapi.mtaoapi006.org/api.php	lib/armeabi-v7a/libapp.so
https://raw.githubusercontent.com/little-5/backup/master/51lq.txt	lib/armeabi-v7a/libapp.so
https://staff.tea123.me/e.jpg	lib/armeabi-v7a/libapp.so
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues/new	lib/armeabi-v7a/libapp.so
https://51lqapi.51lq.me/api.php	lib/armeabi-v7a/libapp.so

 邮箱线索

邮箱地址	所在文件
l@_dashoffsettype.percentage _growablelist@0150898._withdata n_typeerror@0150898._create _double@0150898.fromintege s_immutablelist@0150898._jbb _growablelist@0150898._literal _immutablemap@0150898._create eo_bytebuffer@7027147._new l@boxwidthstyle.tight _casterror@0150898._create _assertionerror@0150898._create	lib/armeabi-v7a/libapp.so

ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so
-------------------------	---------------------------------

📱 手机线索

手机号	所在文件
17512775099	c/e/b/c/a.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: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=.
签名算法: rsassa_pkcs1v15
有效期自: 2023-08-29 03:02:02+00:00
有效期至: 2024-08-28 03:02:02+00:00
发行人: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=.
序列号: 0x775226bf
哈希算法: sha256
md5值: de37536c482936e7e08f9f23f059be6f
sha1值: 373262badaec1702970545249d8de780e6be54f3
sha256值: cd9b10e8b5384588177002c857478c553eb0161f1c50d4f247bc0fc4f3c90b65
sha512值: 2202e5cbe9f215eeb10cce04d11e322f9dafd50bf704958387b683163b7c8adf8d7ecdf6e303799c6e8b1129c35afdd0bc68049ba46fb10ad931f791a3534fd0
公钥算法: rsa
密钥长度: 2048
指纹: 516e05a79a038347f2311f4a9af9c8dd90b1ae627a8b3f4e273a24db95f41812

🔑 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	允许应用程序写入外部存储

		外部存储内容	
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

应用内通信