



MoGua

蛋播星球 1.0.1.APK 分析报告



APP名称:

蛋播星球

包名:	com.danbo.danbo
域名线索:	34条
URL线索:	24条
邮箱线索:	3条
分析日期:	2025年5月9日
分析平台:	摸瓜APK反编译平台

文件名: danbo_android_1.0.1.apk

文件大小: 35.3MB

MD5值: 734addb07d4c662b3245bb66d85b0a1d

SHA1值: 2c3d2a6c791418a3107bc65dc6d3b2eb6cd0c97a

SHA256值: 0901cd373a32182c6be8bc772beb4895a7938de6421c3eb508b41a0a07fe4e40

i APP 信息

App名称: 蛋播星球

包名: com.danbo.danbo

主活动Activity: com.danbo.danbo.MainActivity

安卓版本名称: 1.0.1

安卓版本: 1

🔍 域名线索

域名	服务器信息
api.tiankongapi.com	IP: 154.13.7.54 所属国家: Canada 地区: Ontario 城市: Toronto 纬度: 43.653625 经度: -79.600632
dartbug.com	IP: 216.239.36.21 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
ns.adobe.com	没有服务器地理信息.
	IP: 127.0.0.1

aomedia.org	所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
issuetracker.google.com	IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
lyxx.sygjx.com	IP: 116.62.135.11 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
developer.android.com	IP: 142.251.33.110 所属国家: Canada 地区: Ontario 城市: Toronto 纬度: 43.653660 经度: -79.382927
api.vvhan.com	IP: 110.40.26.155 所属国家: China 地区: Sichuan 城市: Chengdu 纬度: 30.666670 经度: 104.066269
www.sec.co.kr	IP: 112.106.187.200 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul 纬度: 37.566311 经度: 126.977203

api.txqq.pro	IP: 101.72.224.113 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
dashif.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
jszyapi.com	IP: 8.218.111.47 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
schemas.android.com	没有服务器地理信息.
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
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
	IP: 34.111.97.67 所属国家: United States of America

developer.mozilla.org	地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
developer.apple.com	IP: 23.48.5.7 所属国家: Japan 地区: Osaka 城市: Ibaraki 纬度: 34.816425 经度: 135.568909
v2.api-m.com	IP: 118.123.202.11 所属国家: China 地区: Sichuan 城市: Chengdu 纬度: 30.666670 经度: 104.066269
collect.wolongzyw.com	IP: 194.147.100.83 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.620621 经度: -122.310959
api.deepseek.com	IP: 116.205.40.120 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
i2.wp.com	IP: 192.0.77.2 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.748425 经度: -122.413673

api.siliconflow.cn	IP: 47.102.37.23 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
cujfgm0g91hkparuaegg.baseapi.memfiredb.com	IP: 106.15.205.190 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
api.zxki.cn	IP: 123.60.159.147 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
movie.douban.com	IP: 81.70.124.99 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
g.co	IP: 142.251.33.110 所属国家: Canada 地区: Ontario 城市: Toronto

	纬度: 43.653660 经度: -79.382927
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.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
purl.org	IP: 207.241.225.157 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.781734 经度: -122.459435
dmpay.knowhub.vip	IP: 111.229.183.182 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
video.360kan.com	IP: 121.18.236.3 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
	IP: 31.13.94.10

www.youtube.com	所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires 纬度: -34.603600 经度: -58.381554
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

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	A/b.java
http://ns.adobe.com/xap/1.0/\u0000	W/g.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	R/C0107t.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	R/O.java
https://issuetracker.google.com/issues/241760537	R/c0.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	R/C0108u.java
https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted	f0/C0331u.java
http://g.co/dev/packagevisibility.	f0/C0336z.java
http://ns.adobe.com/xap/1.0/	N0/a.java

https://docs.flutter.dev/deployment/android	i2/b.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/n.java
https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md	n2/C0479j.java
https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread	h0/C0362G.java
http://dashif.org/guidelines/trickmode	k0/C0425b.java
http://dashif.org/guidelines/trickmode	l0/C0433e.java
http://dashif.org/guidelines/last-segment-number	l0/C0433e.java
https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md	y3/d.java
https://aomedia.org/emsg/ID3	Q0/a.java
https://developer.apple.com/streaming/emsg-id3	Q0/a.java
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://api.vhan.com/api/moyu?type=json	lib/arm64-v8a/libapp.so
http://www.unicode.org/copyright.html	lib/arm64-v8a/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	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

https://cujfgm0g91hkparuaegg.baseapi.memfiredb.com/rest/v1	lib/armeabi-v7a/libapp.so
https://api.zxki.cn/api/sjtx?type=text	lib/armeabi-v7a/libapp.so
https://api.siliconflow.cn/v1	lib/armeabi-v7a/libapp.so
https://i2.wp.com/web-static.4ce.cn/storage/bucket/v1/9f76dde36d21e1089ad2e0ef75c7280f.webp	lib/armeabi-v7a/libapp.so
https://cujfgm0g91hkparuaegg.baseapi.memfiredb.com	lib/armeabi-v7a/libapp.so
https://api.vvhan.com/api/avatar/rand?type=json	lib/armeabi-v7a/libapp.so
http://purl.org/dc/elements/1.1/	lib/armeabi-v7a/libapp.so
http://www.sec.co.kr/	lib/armeabi-v7a/libapp.so
https://movie.douban.com/j/search_subjects	lib/armeabi-v7a/libapp.so
https://cujfgm0g91hkparuaegg.baseapi.memfiredb.com/realtime/v1	lib/armeabi-v7a/libapp.so
https://movie.douban.com/j/new_search_subjects	lib/armeabi-v7a/libapp.so
https://www.youtube.com/	lib/armeabi-v7a/libapp.so
https://api.vvhan.com/api/avatar/dm?type=json	lib/armeabi-v7a/libapp.so
https://api.zxki.cn/api/lzy?url=	lib/armeabi-v7a/libapp.so
https://api.vvhan.com/api/avatar/niche?type=json	lib/armeabi-v7a/libapp.so
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status	lib/armeabi-v7a/libapp.so
https://api.txqq.pro/api/sjtx2.php	lib/armeabi-v7a/libapp.so
https://api.vvhan.com/api/moyu?type=json	lib/armeabi-v7a/libapp.so

https://api.vvhan.com/api/avatar/girl?type=json	lib/armeabi-v7a/libapp.so
https://dmply.knowhub.vip/d?url=	lib/armeabi-v7a/libapp.so
https://cujfgm0g91hkparuaegg.baseapi.memfiredb.com/storage/v1	lib/armeabi-v7a/libapp.so
https://api.zxki.cn/api/wyrg	lib/armeabi-v7a/libapp.so
https://cujfgm0g91hkparuaegg.baseapi.memfiredb.com/functions/v1	lib/armeabi-v7a/libapp.so
https://v2.api-m.com/api/head	lib/armeabi-v7a/libapp.so
https://collect.wolongzyw.com/api.php/provide/vod/	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://api.zxki.cn/api/wyy?type=url&id=	lib/armeabi-v7a/libapp.so
https://jszyapi.com/api.php/provide/vod/	lib/armeabi-v7a/libapp.so
https://api.vvhan.com/api/avatar/boy?type=json	lib/armeabi-v7a/libapp.so
https://api.deepseek.com/v1	lib/armeabi-v7a/libapp.so
http://lyxx.sygjx.com	lib/armeabi-v7a/libapp.so
https://cujfgm0g91hkparuaegg.baseapi.memfiredb.com/storage/v1/object/public/other/placeholder.png	lib/armeabi-v7a/libapp.so
http://video.360kan.com/suggest.php	lib/armeabi-v7a/libapp.so
https://api.zxki.cn/api/wyy?type=lrc&id=	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.	lib/armeabi-v7a/libapp.so

https://api.zxki.cn/api/mt60s	lib/armeabi-v7a/libapp.so
https://api.tiankongapi.com/api.php/provide/vod/	lib/armeabi-v7a/libapp.so
https://cujfgm0g91hkparuaegg.baseapi.memfiredb.com/auth/v1	lib/armeabi-v7a/libapp.so
http://www.unicode.org/copyright.html	lib/armeabi-v7a/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues	lib/armeabi-v7a/libflutter.so
https://dartbug.com/52121	lib/armeabi-v7a/libflutter.so
https://api.vvhan.com/api/moyu?type=json	lib/x86_64/libapp.so
http://www.unicode.org/copyright.html	lib/x86_64/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	lib/x86_64/libflutter.so
https://github.com/flutter/flutter/issues	lib/x86_64/libflutter.so
https://dartbug.com/52121	lib/x86_64/libflutter.so

邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libflutter.so
_fencematch@1195445617.frommatch _double@0150898.fromintege growablelist@0150898.literal	

_growablelist@0150898._internal
_growablelist@0150898.withcapaci
_growablelist@0150898._literal6
_receiveportimpl@1026248.fromrawrec
_list@0150898._ofarray
_timer@1026248.periodic
_nativesocket@16069316.datagram
_growablelist@0150898._literal2
_list@0150898.empty
_file@16069316.fromrawpat
_nativesocket@16069316.normal
_imagefilter@17065589.fromcolorf
_invocationmirror@0150898._withtype
_hashcollisionnode@43137193.fromcollis
storationinformation@288124995.fromserial
authenticationscheme@15463476.fromstring
_compressednode@43137193.single
_uri@0150898.file
_growablelist@0150898._literal1
_future@5048458.immediatee
_growablelist@0150898._literal4
_growablelist@0150898._ofgrowabl
_growablelist@0150898.of
_link@16069316.fromrawpat
_list@0150898.of
_list@0150898.generate
_colorfilter@17065589.mode
_future@5048458.zonevalue
_typeerror@0150898._create
_imagefilter@17065589.composed
_list@0150898._ofgrowabl
_list@0150898._ofefficie
_growablelist@0150898._ofarray
_growablelist@0150898._literal3
_growablelist@0150898._ofother
ngstreamssubscription@5048458.zoned
_timer@1026248._internal
_growablelist@0150898._literal5
_bytebuffer@8027147._new
_httpparser@15463476.responsepa
_list@0150898._ofother
_internetaddress@16069316.fixed
_future@5048458.immediate

lib/armeabi-v7a/libapp.so

_colorfilter@17065589.srgbtoline _future@5048458.value _assertionerror@0150898._create _directory@16069316.fromrawpat _colorfilter@17065589.lineartosr _uri@0150898.directory _imagefilter@17065589.blur _growablelist@0150898._literal8 _assetmanifestbin@51287047.fromstanda _growablelist@0150898.generate _uri@0150898.notsimple _growablelist@0150898._literal7 _growablelist@0150898._ofefficie	
appro@openssl.org	lib/x86_64/libflutter.so

手机线索

手机号	所在文件
17512775099	O1/a.java
19199999641	摸瓜V2引擎
19771752451	摸瓜V2引擎

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=86, ST=beijing, L=Unknown, O=danbo, OU=Unknown, CN=guoliangzhang

签名算法: rsassa_pkcs1v15

有效期自: 2020-05-14 00:37:56+00:00

有效期至: 2047-09-30 00:37:56+00:00

发行人: C=86, ST=beijing, L=Unknown, O=danbo, OU=Unknown, CN=guoliangzhang

序列号: 0x47c468ae

哈希算法: sha256

md5值: 1844358c82b5d1661b3b2bc7031280d7

sha1值: 322f0e91c24c3192a48ed408768ef9080b2f573b

sha256值: e614df834f1227f87cd7b1183d62224ace94ce1fb55841f0e8bdd3719e1a456c

sha512值: 3f3c6e7afb2a7426d6445e179304df6181023cde992093a41a8936a54ed44b3bf9c0275bf515c3d53e6192081dfeb7dd6d00ef0b9d79927eca514ed8ab6e33a1

公钥算法: rsa

密钥长度: 2048

指纹: d99e15bd16ed07b8eb0e64073322fb4aff6d61eccc3a126b7bf0efe49d9e7f37

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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.CAPTURE_AUDIO_OUTPUT	系统需要		允许应用程序捕获音频输出。
android.permission.CAPTURE_VIDEO_OUTPUT	正常		允许应用程序捕获视频输出
android.permission.CAPTURE_SECURE_VIDEO_OUTPUT	正常		允许应用程序捕获安全视频输出
android.permission.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
android.permission.USE_FINGERPRINT	正常	allow use of 指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
com.danbo.danbo.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.danbo.danbo.MainActivity	Schemes: io.supabase.flutterquickstart://, Hosts: login-callback,