



波币 1.1.6.APK 分析报告



APP名称:

波币

包名:

bbb.gjhqanrlq.dmvlpklhua

域名线索:

17条

URL线索:	15条
邮箱线索:	5条
分析日期:	2025年6月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: bp_175659343_sign.apk
文件大小: 41.05MB
MD5值: 77e401d285245021c62f36b74019aa7c
SHA1值: 16aac7853095fbd1ea7e99c9148fb8484e919798
SHA256值: caead86c12c24ea84bc20d0739e1fefcc4b6a77cc9eed98235034c323c8f10cd

APP 信息

App名称: 波币
包名: bbb.gjhqanqrlq.dmvlpklhua
主活动Activity: bbb.gjhqanqrlq.dmvlpklhua.MainActivity
安卓版本名称: 1.1.6
安卓版本: 1

🔍 域名线索

域名	服务器信息
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
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
10.0.2.2	IP: 10.0.2.2 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
www.example.com	IP: 92.122.244.34 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
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
payapp.weixin.qq.com	IP: 220.194.111.104 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102

wx.tenpay.com	IP: 220.196.148.65 所属国家: China 地区: Jiangsu 城市: Yancheng 纬度: 33.385559 经度: 120.125282
developer.android.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
plus.google.com	IP: 162.125.83.1 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.ibm.com	IP: 23.42.126.170 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
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
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
o4506995606880256.ingest.us.sentry.io	IP: 34.120.195.249 所属国家: United States of America 地区: Missouri 城市: Kansas City

	纬度: 39.099731 经度: -94.578568
www.tensorflow.org	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
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
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
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

 URL线索

URL信息	Url所在文件
http://www.example.com	com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java
https://plus.google.com/	i2/m1.java
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

http://10.0.2.2:8969/stream	io/sentry/SpotlightIntegration.java
https://github.com/Baseflow/flutter-permission-handler/issues	l/q.java
https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md	a9/q.java
https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md	z8/d.java
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.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
https://1e73b36f708c39bcba60a317ea4b6c6@o4506995606880256.ingest.us.sentry.io/4508869640192000	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
http://kiwi_bbpay	lib/armeabi-v7a/libapp.so
https://payapp.weixin.qq.com/	lib/armeabi-v7a/libapp.so
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status	lib/armeabi-v7a/libapp.so
https://wx.tenpay.com/	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.	lib/armeabi-v7a/libapp.so
http://kiwi_install	lib/armeabi-v7a/libapp.so
https://www.tensorflow.org/lite/guide/ops_select	lib/armeabi-v7a/libbarhopper_v3.so
http://http	lib/armeabi-v7a/libbarhopper_v3.so
https://www.tensorflow.org/lite/guide/ops_custom	lib/armeabi-v7a/libbarhopper_v3.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.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so
https://www.tensorflow.org/lite/guide/ops_select	lib/arm64-v8a/libbarhopper_v3.so
http://http	lib/arm64-v8a/libbarhopper_v3.so
https://www.tensorflow.org/lite/guide/ops_custom	lib/arm64-v8a/libbarhopper_v3.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

 邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	f2/r.java
_hashcollisionnode@48137193.fromcollis _growablelist@0150898._literal _growablelist@0150898.withcapaci _receiveportimpl@1026248.fromrawrec _growablelist@0150898._literal2 _bigintimpl@0150898.from _nativesocket@15069316.pipe _list@0150898.empty _imagefilter@17065589.fromcolorf _httpparser@16463476.responsepa _future@5048458.immediatee _axissize@1957299587.fromsize _growablelist@0150898._literal4 _growablelist@0150898.of _link@15069316.fromrawpat _list@0150898.of _list@0150898.generate	

_colorfilter@17065589.mode _typeerror@0150898._create _list@0150898._ofgrowabl _list@0150898._ofefficie _growablelist@0150898._ofarray _socket@15069316._readpipe 39bcbca60a317ea4b6c6@o4506995606880256.ingest _list@0150898._ofother _colorfilter@17065589.srgbtoline _colorfilter@17065589.lineartosr _rawsocket@15069316._readpipe _imagefilter@17065589.blur _growablelist@0150898._literal8 _assetmanifestbin@56287047.fromstanda channelcontroller@30156646.implementa _capture@2355136370.create _double@0150898.fromintege _growablelist@0150898._literal6 _list@0150898._ofarray _timer@1026248.periodic _invocationmirror@0150898._withtype _growablelist@0150898._literal1 _uri@0150898.file _growablelist@0150898._ofgrowabl _future@5048458.zonevalue _file@15069316.fromrawpat _imagefilter@17065589.composed _growablelist@0150898._literal3 _growablelist@0150898._ofother ngstreamssubscription@5048458.zoned _timer@1026248._internal _growablelist@0150898._literal5 authenticationscheme@16463476.fromstring _bytebuffer@8027147._new _future@5048458.immediate _future@5048458.value _assertionerror@0150898._create _pointerpanzoomdata@441213599.fromupdate _directory@15069316.fromrawpat _filestream@15069316.forstdin _nativesocket@15069316.normal _uri@0150898.directory androidstorage@34339836.implementa _growablelist@0150898.generate _uri@0150898.notsimple _compressednode@48137193.single _growablelist@0150898._literal7 _growablelist@0150898._ofefficie	lib/armeabi-v7a/libapp.so
android-sdk-releaser@oqei5.prod	lib/armeabi-v7a/libbarhopper_v3.so

android-sdk-releaser@oqei5.prod	lib/arm64-v8a/libbarhopper_v3.so
appro@openssl.org	lib/arm64-v8a/libflutter.so

手机线索

手机号	所在文件
17512775099	c4/a.java

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-16 09:39:27+00:00
有效期至: 2080-03-19 09:39:27+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0xba3d8ea402a34c1b
哈希算法: sha256
md5值: 5095eddd04ed1911d24a6637128980cc
sha1值: 254c859b6a846bf8e5032e402f8de4fa45355bf2
sha256值: 019c70df58df922e6abd73a510834f3a34f24495fd12e89a927aebdf27d42616
sha512值: 814a21a171ac3a4adb761fbd6c3c9f6aed5266abf1b83fa53206460336633f4575a4bb20cc63c61d99e8de89b676dc3f262bd3031bac4f4e38025b31e5af0835
公钥算法: rsa
密钥长度: 2048
指纹: a6b7ac51a0c5684c5325eea062c0e4e81f6aef10c467ae3b705594da06bc2a90

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.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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
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_VIDEO	未知	Unknown permission	Unknown permission from android reference
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
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.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由

android.permission.VIDEO_CAPTURE	未知	Unknown permission	Unknown permission from android reference
android.permission.AUDIO_CAPTURE	未知	Unknown permission	Unknown permission from android reference
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
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.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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
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
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.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
bbb.gjhqanqrlq.dmvlpklhua.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
bbb.gjhqanqrlq.dmvlpklhua.MainActivity	Schemes: lpjup1fs://,

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。