



MoGua

片多多 2.0.1.APK 分析报告



APP名称:

片多多

包名:	com.app.pdd
域名线索:	22条
URL线索:	18条
邮箱线索:	3条
分析日期:	2025年6月21日
分析平台:	摸瓜APK反编译平台

文件名: 片多多.apk
文件大小: 62.97MB
MD5值: ac386f2968acc7564f5a5d8e942ee942
SHA1值: c8b9d727c5dbd8304dc93d7c37f1e38fbfb16e52
SHA256值: 3a5ae0668c63516b6fa822dfeca08181ef0f152023ff6bfac80ed96c320e0097

i APP 信息

App名称: 片多多
包名: com.app.pdd
主活动Activity: com.app.pdd.MainActivity
安卓版本名称: 2.0.1
安卓版本: 1

🔍 域名线索

域名	服务器信息
d1r1vw8zvbqvut.cloudfront.net	IP: 18.238.189.178 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958
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.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
journeyapps.com	IP: 18.65.168.85 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
grs.dbankcloud.cn	IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
developer.android.com	IP: 192.178.163.139 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
jhfkdnov21vfd.yuonqyfnyk.work	IP: 65.8.161.6 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418
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
	IP: 139.162.91.46

jhfkdnov21vfd.knykthqoax.work	所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
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.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
grs.dbankcloud.com	IP: 60.28.200.159 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
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
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

jhfkdnov21vfd.azjnsjtulf.work	IP: 65.8.161.31 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418
aomedia.org	IP: 108.160.166.148 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
dmfог846fakfh.cloudfront.net	IP: 3.165.84.56 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
dashif.org	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
dpcwvq4v975l1.cloudfront.net	IP: 18.238.189.116 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958
grs.dbankcloud.asia	IP: 49.4.40.185 所属国家: China 地区: Guangdong

	城市: Guangzhou 纬度: 23.127361 经度: 113.264572
grs.dbankcloud.eu	没有服务器地理信息.
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

 URL线索

URL信息	Url所在文件
https://)([\\s\\S]+)	com/huawei/hms/scankit/p/C0110bd.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/d.java
https://docs.flutter.dev/deployment/android	q3/c.java
https://github.com/Baseflow/flutter-permission-handler/issues	m1/d.java
https://journeyapps.com/	摸瓜V1引擎
https://github.com/journeyapps/zxing-android-embedded	摸瓜V1引擎
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎

https://grs.dbankcloud.eu	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://aomedia.org/emsg/ID3	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://api.flutter.dev/flutter/material/Scaffold/of.html	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
http://%.*s	lib/arm64-v8a/libmpv.so
https://%.*s	lib/arm64-v8a/libmpv.so
http://dashif.org/guidelines/last-segment-number	lib/arm64-v8a/libmpv.so
https://dpcwvq4v975l1.cloudfront.net/xmt_ldy.json	lib/armeabi-v7a/libapp.so
https://jhfkdnov21vfd.yuonqyfnyk.work	lib/armeabi-v7a/libapp.so
https://jhfkdnov21vfd.azinsjtulf.work	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://d1r1vw8zvbqvut.cloudfront.net/xmt.json	lib/armeabi-v7a/libapp.so

https://developer.mozilla.org/en-US/docs/Web/HTTP/Status	lib/armeabi-v7a/libapp.so
https://jhfkdnov21vfd.knykthqoax.work:51999	lib/armeabi-v7a/libapp.so
https://dmfog846fakfh.cloudfront.net/xmt.json	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android	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
http://%.*s	lib/armeabi-v7a/libmpv.so
https://%.*s	lib/armeabi-v7a/libmpv.so
http://dashif.org/guidelines/last-segment-number	lib/armeabi-v7a/libmpv.so
http://%.*s	lib/x86/libmpv.so
https://%.*s	lib/x86/libmpv.so
http://dashif.org/guidelines/last-segment-number	lib/x86/libmpv.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	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
http://%.*s	lib/x86_64/libmpv.so
https://%.*s	lib/x86_64/libmpv.so
http://dashif.org/guidelines/last-segment-number	lib/x86_64/libmpv.so

 邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libflutter.so
signinprizemodelimpl@1364457718.fromjson dyjm2016@gmail.com _compressednode@44137193.single _growablelist@0150898._literal _growablelist@0150898.withcapaci _receiveportimpl@1026248.fromrawrec _growablelist@0150898._literal2 _bigintimpl@0150898.from _list@0150898.empty _imagefilter@17065589.fromcolorf signininfomodelimpl@1361318755.fromjson weeksigninlogimpl@1362023555.fromjson _future@5048458.immediatee _growablelist@0150898._literal4 _growablelist@0150898.of _nativesocket@16069316.listen _list@0150898.of _list@0150898.generate tgamedetailmodelimpl@1319448735.fromjson	

_colorfilter@17065589.mode
_typeid@0150898._create
_list@0150898._ofgrowabl
_list@0150898._ofefficie
_growablelist@0150898._ofarray
_list@0150898._ofother
_colorfilter@17065589.srgbtoline
_colorfilter@17065589.lineartosr
adultgamemodelimpl@1122453901.fromjson
storationinformation@243124995.fromserial
_imagefilter@17065589.blur
_growablelist@0150898._literal8
_hashcollisionnode@44137193.fromcollis
picturecellmodelimpl@1218303248.fromjson
_double@0150898.fromintege
_growablelist@0150898._literal6
_list@0150898._ofarray
_timer@1026248.periodic
_nativesocket@16069316.normal
_invocationmirror@0150898._withtype
authenticationscheme@15463476.fromstring
syspartnermodelimpl@1366355620.fromjson
_growablelist@0150898._literal1
_uri@0150898.file
_growablelist@0150898._ofgrowabl
_link@16069316.fromrawpat
_httpparser@15463476.requestpar
_future@5048458.zonevalue
_imagefilter@17065589.composed
ecollectionmodelimpl@1318124904.fromjson
_growablelist@0150898._literal3
_growablelist@0150898._ofother
ngstreamsubscription@5048458.zoned
_timer@1026248._internal
_growablelist@0150898._literal5
_bytebuffer@8027147._new
_pointerpanzoomdata@383213599.fromupdate
_httpparser@15463476.responsepa

_future@5048458.immediate
_future@5048458.value
nerclassifymodelimpl@1365375200.fromjson
_assertionerror@0150898._create

lib/armeabi-v7a/libapp.so

_directory@16069316.fromrawpat _uri@0150898.directory _growablelist@0150898.generate _uri@0150898.notsimple _growablelist@0150898._literal7 _assetmanifestbin@389287047.fromstanda _growablelist@0150898._ofefficie	
appro@openssl.org	lib/x86_64/libflutter.so

手机线索

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=Your Country, ST=Your State, L=Your City, O=Your Company, OU=Your Org, CN=Your Name

签名算法: rsassa_pkcs1v15

有效期自: 2025-04-30 09:27:30+00:00

有效期至: 2050-04-24 09:27:30+00:00

发行人: C=Your Country, ST=Your State, L=Your City, O=Your Company, OU=Your Org, CN=Your Name

序列号: 0xb5236034e77d86fc

哈希算法: sha384

md5值: fbb88959cdfeb46545c958553004bbda

sha1值: 000a8bd2fed62be191a51e60edd534773372247c

sha256值: 49ed1be25e7bae5796bd56a58eb4fedf8dd6761d65daae412cec3c6fdb24bd84

sha512值: 912fb3478646820710e7ff40d7e9830b864a0ff6772407629c3d46d2c1730982c99bc5a4ca6348d83e3265ece9b26ae694904423c2a916afe60a9b33e96f7740

公钥算法: rsa

密钥长度: 2048

指纹: 13b6b1f69f89ff1f360f5fe7f34c836a5db674ef2aaa9477bb64ef3e4c653b00

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.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.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_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
com.app.pdd.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信