



MoGua

bitpie 1.1.0.APK 分析报告



APP名称:

bitpie

包名:	uni.UNI2652E16
域名线索:	20条
URL线索:	21条
邮箱线索:	0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: bitpie-1.apk
文件大小: 73.37MB
MD5值: 0c3e88c59b63c90ba90687f7297b3188
SHA1值: 8f791bbef27e0287d0ee99b975e5577c70c59f74
SHA256值: 8b0e1543e2e45ddc252409a03447966dbc753c059137ac25614ad0903a015bd4

i APP 信息

App名称: bitpie
包名: uni.UNI2652E16
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.1.0
安卓版本: 101

🔍 域名线索

域名	服务器信息
s6s7smdxyzbsd7d7nsrx.icu	IP: 47.243.165.24 所属国家: United States of America 地区: California 城市: San Mateo 纬度: 37.547424 经度: -122.330589
schemas.android.com	没有服务器地理信息.
quilljs.com	IP: 172.66.40.163 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

www.google.com	IP: 199.59.148.229 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
bitpie.com	IP: 172.67.73.74 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.trongrid.io	IP: 54.169.127.80 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
feross.org	IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont 纬度: 37.548271 经度: -121.988571
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
apis.map.qq.com	IP: 116.130.224.140 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501

	经度: 116.397102
ns.adobe.com	没有服务器地理信息.
service.dcloud.net.cn	IP: 110.40.169.99 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
developer.yahoo.com	IP: 69.147.80.15 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
ask.dcloud.net.cn	IP: 123.12.235.54 所属国家: China 地区: Henan 城市: Hebi 纬度: 35.899170 经度: 114.192497
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
bit.ly	IP: 67.199.248.10 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.750134 经度: -73.997009

m3w.cn	IP: 221.204.15.62 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
er.dcloud.io	没有服务器地理信息.
er.dcloud.net.cn	IP: 127.0.0.1 所属国家:- 地区:- 城市:- 纬度: 0.000000 经度: 0.000000
api.blockcypher.com	IP: 172.66.134.253 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
sxsfcc.com	IP: 129.226.110.198 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java

http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/e/b/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/e/b/a.java
https://er.dcloud.io/rv	io/dcloud/e/c/h/b.java
https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/b.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://sxsfcc.com/api/open/postByTokenpocket	摸瓜V2引擎
https://api.blockcypher.com/v1/btc/main/addrs/	摸瓜V2引擎
https://api.trongrid.io	摸瓜V2引擎

https://api.trongrid.io/	摸瓜V2引擎
https://bitpie.com/	摸瓜V2引擎
https://s6s7smdxyzbsd7d7nsrx.icu/api/cb/getxxx?t=bt10008	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://feross.org/opensource >	摸瓜V2引擎
https://bitpie.com	摸瓜V2引擎
https://bit.ly/2Zqjzkip	摸瓜V2引擎
http://feross.org >	摸瓜V2引擎
http://developer.yahoo.com/yui/license.html	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	摸瓜V2引擎
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	摸瓜V2引擎
https://www.google.com/maps/?daddr=	摸瓜V2引擎
https://www.google.com/maps/	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎

☰ 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=CN, ST=, L=, O=Android, OU=Android, CN=7SQIF%2FhAVEJ4VJ5BumotL3KzPXhcZ4XrG%2FvFjm8cBozgtYHm384qQJS0cWoPoxd
签名算法: rsassa_pkcs1v15
有效期自: 2024-02-27 02:02:07+00:00
有效期至: 2124-02-03 02:02:07+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=7SQIF%2FhAVEJ4VJ5BumotL3KzPXhcZ4XrG%2FvFjm8cBozgtYHm384qQJS0cWoPoxd
序列号: 0x6ed4e56d
哈希算法: sha256
md5值: 58010f0ffaac2ee4df14f0bd64ae25b4
sha1值: af91ce34437c491d78ac6155a6aa9a3a872143d6
sha256值: 64b670badce8ed2a454dc2e53a8d1aafb577a5b55f72bb67ea00c7cf9958d75c
sha512值: 8053591f1352c7095f7a499d44453dfea819531bb007b94f382700f577002d59081ce42e5ca23c2d19d7fe079834c1ace09b9a8bcef16792524773029b410cf9
公钥算法: rsa
密钥长度: 2048
指纹: 3be0f6a32432efb0d01fb87617c491b74f3547f112eff81b58d54f63b5e55d53

🔑 硬编码敏感信息

可能的敏感信息
"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"

"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"
"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"
"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"

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.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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
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.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.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
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.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.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.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference

应用内通信