MoGua

BiyAi 1.0.0.APK 分析报告

APP名称: BiyAi

包名:	quant.biy.bot
域名线索:	6条
URL线索:	7条
邮箱线索:	1条
分析日期:	2025年5月5日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 96bcddf2-c25b-412e-859a-d45721044d10.apk
文件大小: 17.5MB
MD5值: 0932c3c6fc2b5fe067e8641e7b8564a7
SHA1值: 10f197af2bbf297da3b0357d643b9787296efa11
SHA256值: 948bc8585f1b03f04112ee8635fbc5bd37d0b0481672f756855aaaacf140de0a

APP 信息

App名称: BiyAi
包名: quant.biy.bot
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.0
安卓版本: 100

域名线索

域名	服务器信息
upload.ffmpeg.org	**IP**: 213.36.253.119 **所属国家**: France **地区**: Ile-de-France **城市**: Paris **纬度**: 48.853409 **经度**: 2.348800
ask.dcloud.net.cn	**IP**: 124.236.20.231 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041389 **经度**: 114.478607
lame.sf.net	**IP**: 204.68.111.100 **所属国家**: United States of America **地区**: California

	城市: San Diego **纬度**: 32.799797 **经度**: -117.137047
ns.adobe.com	没有服务器地理信息.
crbug.com	**IP**: 216.239.32.29 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.openssl.org	**IP**: 23.64.183.254 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052231 **经度**: -118.243683

URL线索

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/36199	Android String Resource
ftp://upload.ffmpeg.org/incoming/	lib/armeabi-v7a/libijkplayer.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libstatic-webp.so
https://crbug.com/v8/8520	lib/armeabi-v7a/libweexjss.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libnative-imagetranscoder.so

http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so
http://lame.sf.net	lib/armeabi-v7a/liblamemp3.so

邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

手机线索

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=, L=, O=Android, OU=Android, CN=PXgD%2F11jJVKusUhbIp379A0l7qHtn21dVq4zX1q5r%2Fixg7iBZSTwsQggyEcaUX9LT1BMd8iXuvNIK%2FoN8ykAQA%3D%3D
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-05-01 19:44:06+00:00
Valid To: 2122-04-07 19:44:06+00:00
Issuer: C=CN, ST=, L=, O=Android, OU=Android, CN=PXgD%2F11jJVKusUhbIp379A0l7qHtn21dVq4zX1q5r%2Fixg7iBZSTwsQggyEcaUX9LT1BMd8iXuvNIK%2FoN8ykAQA%3D%3D
Serial Number: 0x788a3e58
Hash Algorithm: sha256
md5: ddec9ddd16aa8485a768870a51d60072
sha1: cac947fa266e9f9f274dbe6bd8a7cc820ecba2ea
sha256: d2c7ddb95fdcfe1bc11d6cde1bd0c2c1680b83724df3220fc3dd23f18545eaf3
sha512: b0d0a630ddd05d8c0a073e0041866f1ea03a5e4b5ef4df601a1fc8718f931f9e221bdd981d64689551c303b657011750d0eb5af12e98d3e52904ed56b5003ad8
PublicKey Algorithm: rsa
Bit Size: 2048

Fingerprint: c4d6caf774abd4a6dd31b8a828be9013cc0b31f1f40a77b3da89a5b121ce7be4

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.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.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.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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
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
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