



# MoGua

## CIFHK 1.0.0.APK 分析报告



APP名称:

CIFHK

包名:	bidbxb.yduzgnq.ukcnqn
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年10月2日
分析平台:	<a href="#">摸瓜APK反编译平台</a>

文件名: CIFHK.apk

文件大小: 15.97MB

MD5值: 577f0377f6b0b840b0a14326e23804b8

SHA1值: 45d8e9de0048cee5fcf6256cf1c0056e3fae3b29

SHA256值: a6e3ba3cdcb49ddd6a1ff485583824b00b19f8fc467acb9994150b9e23cf70b7

## APP 信息

App名称: CIFHK

包名: bidbxb.yduzgnq.ukcnqn

主活动Activity: qpgd.kzxn.nvbr.hofht

安卓版本名称: 1.0.0

安卓版本: 10000

## 域名线索

## URL线索

## 邮箱线索

## 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=Ci, ST=JH14, L=ZbeE3, O=RjkLyz.35wM, OU=vDz.dzF0h8, CN=O8GSjt4HINOO8k

签名算法: rsassa\_pkcs1v15

有效期自: 2022-11-28 06:32:23+00:00

有效期至: 2050-04-15 06:32:23+00:00

发行人: C=Ci, ST=JH14, L=ZbeE3, O=RjkLyz.35wM, OU=vDz.dzF0h8, CN=O8GSjt4HINOO8k

序列号: 0x15eb096e

哈希算法: sha256

md5值: 22d659a2913b2606f54b3096dbc87907

sha1值: 1373dc92581e5e8d8ac55645738e18432c25310c

sha256值: 75a36fdc23c97f93c77243c23cdf8eb278a90605be1985cc2d2b74748118b034

sha512值: 08d03cd6197180d96fb3d733a31fef31d9e2c756ea06702ded373f476f2420a3b5c7c4b270a35dc6305c69ffc7d00e41f4b282977b03da33bea8cf772ca047f1

公钥算法: rsa

密钥长度: 2048

指纹: ce099456351fab0954edf20aa9a357898247530123cb8aa45ae6ca37a4810b96

## 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.ACCESS_GPS	未知	Unknown permission	Unknown permission from android reference
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.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.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.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_LOCATION	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.ACCESS_ASSISTED_GPS	未知	Unknown permission	Unknown permission from android reference
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

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。