MoGua

UangKaya 3.0.APK 分析报告

APP名称:	UangKaya

包名:	com.UangKaya.hotpot
域名线索:	8条
URL线索:	7条
邮箱线索:	3条
分析日期:	2025年4月30日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: hivay20200825-47.apk
文件大小: 12.27MB
MD5值: 3dd12abc3f208b16e62d1ed7734ee73d
SHA1值: 5ce5f99fb05cf60d82cbfce3015e1aa3e5d2e73f
SHA256值: 45346e057e9ec1a49e93b779247f68998eac4853956feaaf7d47e036aa988f53

APP 信息

App名称: UangKaya
包名: com.UangKaya.hotpot
主活动Activity: com.UangKaya.hotpot.activity.StartActivity
安卓版本名称: 3.0
安卓版本: 1

域名线索

域名	服务器信息
uangkaya.firebaseio.com	**IP**: 34.120.160.131 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
api.bahagiasejahtera.com	**IP**: 147.139.196.140 **所属国家**: Indonesia **地区**: Jakarta Raya **城市**: Jakarta **纬度**: -6.214620 **经度**: 106.845131
10.1.10.31	**IP**: 10.1.10.31 **所属国家**: - **地区**: -

	城市: - **纬度**: 0.000000 **经度**: 0.000000
192.168.0.222	IP: 192.168.0.222 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
app.bahagiasejahtera.com	IP: 147.139.171.54 **所属国家**: Indonesia **地区**: Jakarta Raya **城市**: Jakarta **纬度**: -6.214620 **经度**: 106.845131
uangkaya.id	IP: 147.139.171.54 **所属国家**: Indonesia **地区**: Jakarta Raya **城市**: Jakarta **纬度**: -6.214620 **经度**: 106.845131
testapi.id.jiaozifin.com	没有服务器地理信息.
play.google.com	IP: 142.251.43.14 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514

URL线索

URL信息	Url所在文件
http://testapi.id.jiaozifin.com:88/	com/UangKaya/hotpot/FunApplication.java
https://api.bahagiasejahtera.com	com/UangKaya/hotpot/FunApplication.java
http://192.168.0.222:8000/	com/UangKaya/hotpot/FunApplication.java
https://app.bahagiasejahtera.com	com/UangKaya/hotpot/FunApplication.java
https://play.google.com/store/apps/details?id=	com/UangKaya/hotpot/FunApplication.java
http://uangkaya.id/app/uangkaya/PrivacyPolicy.html	com/UangKaya/hotpot/Constants.java
https://uangkaya.firebaseio.com	Mogua Engine V1
http://10.1.10.31:9825	lib/armeabi-v7a/libaailiveness_v1.2.0.so
http://%s	lib/armeabi-v7a/libaailiveness_v1.2.0.so
http://pre-staging-%s	lib/armeabi-v7a/libaailiveness_v1.2.0.so
http://%s-%s/%s	lib/armeabi-v7a/libaailiveness_v1.2.0.so
http://pre-staging-%s-%s/%s	lib/armeabi-v7a/libaailiveness_v1.2.0.so
http://10.1.10.31:9825	lib/arm64-v8a/libaailiveness_v1.2.0.so
http://%s	lib/arm64-v8a/libaailiveness_v1.2.0.so
http://pre-staging-%s	lib/arm64-v8a/libaailiveness_v1.2.0.so
http://%s-%s/%s	lib/arm64-v8a/libaailiveness_v1.2.0.so
http://pre-staging-%s-%s/%s	lib/arm64-v8a/libaailiveness_v1.2.0.so

http://10.1.10.31:9825	lib/armeabi/libaailiveness_v1.2.0.so
http://%s	lib/armeabi/libaailiveness_v1.2.0.so
http://pre-staging-%s	lib/armeabi/libaailiveness_v1.2.0.so
http://%s-%s/%s	lib/armeabi/libaailiveness_v1.2.0.so
http://pre-staging-%s-%s/%s	lib/armeabi/libaailiveness_v1.2.0.so

邮箱线索

邮箱地址	所在文件
ftp@example.com	lib/armeabi-v7a/libaailiveness_v1.2.0.so
ftp@example.com	lib/arm64-v8a/libaailiveness_v1.2.0.so
ftp@example.com	lib/armeabi/libaailiveness_v1.2.0.so

手机线索

手机号	所在文件
15552000000	com/UangKaya/hotpot/util/HistoryUtil.java
15552000000	com/UangKaya/hotpot/util/SMSUtil.java

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-05-03 07:45:34+00:00
Valid To: 2049-04-25 07:45:34+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: fafe9faeb43bf75255c60c888db53e85
sha1: 6b0ce0566791c74af4944fae0d81a927c0b3654e
sha256: 669f1401f5fcaac1c4dcc7a016768adfd9c64bf45618d94aff1da93b68ace9f2
sha512: 0b25cb73d6a55346a59e21f934500190b3f2d0f8bc21b50e19911313ecc528080cda149353e68aacdfe61b124b1d14630adadbeab3375fba0ba7d0f4140c03b0
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: f4f3ea875d25f9e0af59cdbadf8d12b8a9577ba7878eea336cd7ecd0b253d4ad

硬编码敏感信息

可能的敏感信息
"com_facebook_device_auth_instructions" : "Visit facebook.com/device and enter the code shown above."
"firebase_database_url" : "https://uangkaya.firebaseio.com"
"google_api_key" : "AIzaSyAccCSBCSMF1B0UGjjYXWeHawio2KzpBeY"
"google_crash_reporting_api_key" : "AIzaSyAccCSBCSMF1B0UGjjYXWeHawio2KzpBeY"
"liveness_auth_check" : "Please Wait"

"liveness_failed_reason_auth_failed" : "Authorization failed, please check network"

"liveness_auth_check" : "请稍候"

"liveness_failed_reason_auth_failed" : "授权失败，请检查网络"

"liveness_auth_check" : "Mohon Tunggu"

"liveness_failed_reason_auth_failed" : "Otorisasi gagal, mohon cek jaringan Anda"

"liveness_auth_check" : "โปรดรอสักครู่"

"liveness_failed_reason_auth_failed" : "การอนุญาติล้มเหลวกรุณาตรวจสอบเครือข่าย"

"liveness_auth_check" : "कृपया प्रतीक्षा करें"

"liveness_failed_reason_auth_failed" : "प्राधिकरण विफल रहा, कृपया नेटवर्क जांचें"

"liveness_auth_check" : "Xin vui lòng đợi"

"liveness_failed_reason_auth_failed" : "Ủy quyền không thành công, xin vui lòng kiểm tra kết nối mạng"

"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og indtast koden, som er vist ovenfor."

"com_facebook_device_auth_instructions" : "facebook.com/deviceにアクセスして、上のコードを入力してください。"

"com_facebook_device_auth_instructions" : "facebook.com/device 'ਤੇ ਵਿਜ਼ਿਟ ਕਰੋ ਅਤੇ ਉੱਪਰ ਦਿੱਤੇ ਕੋਡ ਨੂੰ ਦਾਖ਼ਲ ਕਰੋ।"

"com_facebook_device_auth_instructions" : "facebook.com/device ஐப் பார்வையிட்டு, மேலே காட்டப்பட்ட குறியீட்டை உள்ளிடவும்."

"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og skriv inn koden som vises over."

"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di atas."

"com_facebook_device_auth_instructions" : "Gehe zu facebook.com/device und gib den oben angezeigten Code ein."

"com_facebook_device_auth_instructions" : "Gehe zu facebook.com/device und gib den oben angezeigten Code ein."

"com_facebook_device_auth_instructions" : "facebook.com/deviceని సందర్శించి ఎగువన చూపిన కోడ్‌ను నమోదు చేయండి."

"com_facebook_device_auth_instructions" : "Besoek facebook.com/device en voer die kode wat hierbo gewys word, in."

"com_facebook_device_auth_instructions" : "ไปที่ facebook.com/device แล้วป้อนรหัสที่ปรากฏด้านล่าง"

"com_facebook_device_auth_instructions" : "Siirry osoitteeseen facebook.com/device ja anna oheinen koodi."

"com_facebook_device_auth_instructions" : "facebook.com/device पर विज़िट करें और ऊपर दिखाया गया कोड डालें."

"com_facebook_device_auth_instructions" : "Truy cập facebook.com/device và nhập mã được hiển thị bên trên."

"com_facebook_device_auth_instructions" : "Navštívte stránku facebook.com/device a zadajte kód zobrazený vyššie."

"com_facebook_device_auth_instructions" : "Πηγαίνετε στη διεύθυνση facebook.com/device και εισαγάγετε τον παραπάνω κωδικό."

"com_facebook_device_auth_instructions" : "facebook.com/device സന്ദർശിച്ച് മുകളിൽ കാണിച്ചിരിക്കുന്ന കോഡ് നൽകുക."

"com_facebook_device_auth_instructions" : "Ga naar facebook.com/device en voer de bovenstaande code in."

"com_facebook_device_auth_instructions" : "Odwiedź stronę facebook.com/device i wprowadź powyższy kod."

"com_facebook_device_auth_instructions" : "Puntahan ang facebook.com/device at ilagay ang code na ipinapakita sa itaas."

"com_facebook_device_auth_instructions" : "facebook.com/device দেখুন এবং উপরে দেখানো কোডটিকে প্রবেশ করান৷"

"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di bawah ini."

"com_facebook_device_auth_instructions" : "facebook.com/device ಗೆ ಭೇಟಿ ನೀಡಿ ಮತ್ತು ಮೇಲೆ ತೋರಿಸಿದ ಕೋಡ್ ಅನ್ನು ನಮೂದಿಸಿ."

"com_facebook_device_auth_instructions" : "facebook.com/device에 방문하여 위 코드를 입력하세요."

"com_facebook_device_auth_instructions" : "Vizitează facebook.com/device şi introdu codul de mai sus."

"com_facebook_device_auth_instructions" : "تفضل بزيارة facebook.com/device وإدخال الرمز الموضح أعلاه."
"com_facebook_device_auth_instructions" : "Consultez facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "Posjetitw facebook.com/device i unesite gore prikazani kôd."
"com_facebook_device_auth_instructions" : "facebook.com/device भेट द्या आणि वरील कोड प्रविष्ट करा."
"com_facebook_device_auth_instructions" : "facebook.com/device adresine git ve yukarıda gösterilen kodu gir."
"com_facebook_device_auth_instructions" : "Přejděte na facebook.com/device a zadejte nahoře uvedený kód."
"com_facebook_device_auth_instructions" : "Ve a facebook.com/device e ingresa el código que se muestra arriba."
"com_facebook_device_auth_instructions" : "Lawati facebook.com/device dan masukkan kod yang ditunjukkan di atas."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e inserisci il codice mostrato qui sotto."
"com_facebook_device_auth_instructions" : "Acesse facebook.com/device e insira o código mostrado acima."
"com_facebook_device_auth_instructions" : "facebook.com/device</b&gt ની મુલકાત લો; અને ઉપર આપેલો કોડ દાખલ કરો."
"com_facebook_device_auth_instructions" : "Keresd fel a facebook.com/device címet, és írd be a fent megjelenített kódot."
"com_facebook_device_auth_instructions" : "Откройте facebook.com/device и введите код, показанный выше."
"com_facebook_device_auth_instructions" : "Gå till facebook.com/device och skriv in koden som visas ovan."
"com_facebook_device_auth_instructions" : "יש לבקר בכתובת facebook.com/device</b&gt ולהזין את הקוד המוצג למעלה"
"com_facebook_device_auth_instructions" : "Accédez à facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "前往facebook.com/device</b&gt，並輸入上方顯示的代碼。"
"com_facebook_device_auth_instructions" : "请访问facebook.com/device并输入以上验证码。"

"com_facebook_device_auth_instructions" : "Visita facebook.com/device e introduce el código que se muestra más arriba."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e insere o código apresentado abaixo."
"com_facebook_device_auth_instructions" : "前往facebook.com/device</b&gt，並輸入上方顯示的代碼。"

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.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.hardware.camera.autofocus	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志

android.permission.WRITE_CALL_LOG	危险		允许应用程序写入（但不读取）用户号召日志数据。
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
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.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
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.UangKaya.hotpot.activity.StartActivity	Schemes: app://, Hosts: supplement.vn,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.UangKaya.hotpot,

---