Evaluation Warning: The document was created with Spire.Doc for Python.

**U8.com（ 1.3.34版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | U8.com |
| 版本 | 1.3.34 |
| 包名 | com.example.kkguoji |
| 域名线索 | 43条 |
| URL线索 | 26条 |
| APP图标 |  |
| 分析日期 | 2025年6月18日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | CJqxZghsueFDavMz.apk |
| 文件大小 | 68.73MB |
| MD5值 | 3d8a54dadd1d9aa58777f32f5e75981a |
| SHA1值 | dc2c08745e58afa7b6deab07b42e0bd1a15ddbe7 |
| SHA256值 | 9886483cba4a5d8e3122bc824fbcbba7fa8cfeb1c20d26de9c3fb31353be9178 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | U8.com |
| 包名 | com.example.kkguoji |
| 主活动Activity | com.example.kkguoji.MainActivity |
| 安卓版本名称 | 1.3.34 |
| 安卓版本 | 92 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| gfdhg.com | IP: 104.18.21.162  所属国家: United States of America  地区: California  城市: San Francisco |
| default.url | 没有服务器地理信息. |
| play.google.com | IP: 93.46.8.90  所属国家: Italy  地区: Lombardia  城市: Milan |
| anti-block.gfdhg.com | IP: 104.18.21.162  所属国家: United States of America  地区: California  城市: San Francisco |
| www.youtube.com | IP: 31.13.112.9  所属国家: Ireland  地区: Dublin  城市: Dublin |
| pagead2.googlesyndication.com | IP: 114.250.64.38  所属国家: China  地区: Beijing  城市: Beijing |
| dfklssd.com | IP: 104.18.9.62  所属国家: United States of America  地区: California  城市: San Francisco |
| kk-hongkong-hall-new.dbq9.com | IP: 104.18.24.242  所属国家: United States of America  地区: California  城市: San Francisco |
| wa.me | IP: 157.240.11.53  所属国家: United States of America  地区: California  城市: Los Angeles |
| www.ibm.com | IP: 23.42.126.170  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| sldgjsdm.com | IP: 104.18.18.136  所属国家: United States of America  地区: California  城市: San Francisco |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.example.com | IP: 92.122.244.34  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| oauth.telegram.org | IP: 157.240.17.36  所属国家: Switzerland  地区: Zurich  城市: Zurich |
| www.jsdelivr.com | IP: 104.21.23.24  所属国家: United States of America  地区: California  城市: San Francisco |
| anti-block.sldgjsdm.com | IP: 104.18.18.136  所属国家: United States of America  地区: California  城市: San Francisco |
| dashif.org | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| developer.apple.com | IP: 17.253.87.206  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| developer.mozilla.org | IP: 34.111.97.67  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| help.branch.io | IP: 104.18.21.218  所属国家: United States of America  地区: California  城市: San Francisco |
| bnc.lt | IP: 108.157.254.91  所属国家: United States of America  地区: Washington  城市: Seattle |
| t.me | IP: 149.154.167.99  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Warrington |
| schemas.microsoft.com | IP: 13.107.246.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| kk.net | IP: 104.18.9.72  所属国家: United States of America  地区: California  城市: San Francisco |
| dsklgllas.com | IP: 104.18.19.124  所属国家: United States of America  地区: California  城市: San Francisco |
| yourapp.app.link | IP: 3.173.197.27  所属国家: United States of America  地区: Washington  城市: Seattle |
| new-api.meiqia.com | IP: 114.117.133.42  所属国家: China  地区: Beijing  城市: Beijing |
| www.facebook.com | IP: 211.104.160.39  所属国家: Korea (Republic of)  地区: Gyeonggi-do  城市: Seongnam |
| edge-api2.meiqia.com | IP: 114.117.133.42  所属国家: China  地区: Beijing  城市: Beijing |
| api2.branch.io | IP: 13.35.37.118  所属国家: Taiwan (Province of China)  地区: Taipei  城市: Taipei |
| www.unicode.org | IP: 64.182.27.164  所属国家: United States of America  地区: Texas  城市: Dallas |
| flutter.dev | IP: 199.36.158.100  所属国家: United States of America  地区: California  城市: Mountain View |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| api.flutter.dev | IP: 199.36.158.100  所属国家: United States of America  地区: California  城市: Mountain View |
| cdn.livechatinc.com | IP: 2.22.54.90  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| branch.app.link | IP: 3.173.197.23  所属国家: United States of America  地区: Washington  城市: Seattle |
| developer.android.com | IP: 173.194.202.138  所属国家: United States of America  地区: California  城市: Mountain View |
| dartbug.com | IP: 216.239.32.21  所属国家: United States of America  地区: California  城市: Mountain View |
| cdn.branch.io | IP: 13.35.37.124  所属国家: Taiwan (Province of China)  地区: Taipei  城市: Taipei |
| ns.adobe.com | 没有服务器地理信息. |
| aomedia.org | IP: 128.242.240.244  所属国家: United States of America  地区: Washington  城市: Redmond |
| anti-block.dfklssd.com | IP: 104.18.9.62  所属国家: United States of America  地区: California  城市: San Francisco |
| anti-block.dsklgllas.com | IP: 104.18.18.124  所属国家: United States of America  地区: California  城市: San Francisco |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://new-api.meiqia.com/captchas | com/meiqia/meiqiasdk/util/HttpUtils.java |
| https://new-api.meiqia.com | com/meiqia/meiqiasdk/util/HttpUtils.java |
| https://new-api.meiqia.com/ | com/meiqia/core/v6.java |
| https://edge-api2.meiqia.com/summer/sdk/ | com/meiqia/core/v6.java |
| http://www.example.com | com/pichillilorenzo/flutter\_inappwebview\_android/chrome\_custom\_tabs/CustomTabsHelper.java |
| https://cdn.livechatinc.com/app/mobile/urls.json | com/livechatinc/inappchat/h.java |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted | d5/x.java |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread | h3/b1.java |
| https://developer.android.com/guide/topics/permissions/overview | io/flutter/plugin/platform/g.java |
| https://cdn.branch.io/ | j9/b0.java |
| https://api2.branch.io/ | j9/b0.java |
| https://bnc.lt/a/ | j9/e0.java |
| http://dashif.org/guidelines/last-segment-number | n4/d.java |
| http://dashif.org/guidelines/trickmode | n4/d.java |
| http://dashif.org/thumbnail\_tile | n4/d.java |
| http://dashif.org/guidelines/thumbnail\_tile | n4/d.java |
| https://github.com/Baseflow/flutter-permission-handler/issues | s0/q.java |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | l3/i0.java |
| https://x</LA\_URL> | l3/h0.java |
| https://default.url | l3/h0.java |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps | i5/b.java |
| http://ns.adobe.com/xap/1.0/ | r3/a.java |
| https://aomedia.org/emsg/ID3 | b4/a.java |
| https://developer.apple.com/streaming/emsg-id3 | b4/a.java |
| https://help.branch.io/developers-hub/docs/android-basic-integration | n9/c.java |
| https://help.branch.io/using-branch/docs/android-app-links | n9/c.java |
| https://<yourapp>.app.link/NdJ6nFzRbK\n | n9/c.java |
| https://<yourapp>.app.link/NdJ6nFzRbK?bnc\_validate=true | n9/c.java |
| https://branch.app.link/link-settings-page | n9/c.java |
| http://', | 摸瓜V2引擎 |
| https://'; | 摸瓜V2引擎 |
| https://github.com/nodeca/pica | 摸瓜V2引擎 |
| https://www.jsdelivr.com/using-sri-with-dynamic-files | 摸瓜V2引擎 |
| https://github.com/apvarun/toastify-js | 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://github.com/flutter/flutter/issues. | lib/arm64-v8a/libflutter.so |
| https://dartbug.com/52121. | lib/arm64-v8a/libflutter.so |
| https://anti-block.dsklgllas.com/xyw\_base.txt | lib/armeabi-v7a/libapp.so |
| https://dsklgllas.com/xyw\_base.txt | lib/armeabi-v7a/libapp.so |
| https://dfklssd.com/hwjb\_base.txt | lib/armeabi-v7a/libapp.so |
| https://sldgjsdm.com/uu6\_base.txt | lib/armeabi-v7a/libapp.so |
| https://wa.me/ | lib/armeabi-v7a/libapp.so |
| https://www.youtube.com/ | lib/armeabi-v7a/libapp.so |
| https://t.me/u8u8 | lib/armeabi-v7a/libapp.so |
| https://oauth.telegram.org/auth?bot\_id= | lib/armeabi-v7a/libapp.so |
| https://sldgjsdm.com/hwjb\_base.txt | lib/armeabi-v7a/libapp.so |
| https://anti-block.dfklssd.com/uu6\_base.txt | lib/armeabi-v7a/libapp.so |
| https://gfdhg.com/uu6\_base.txt | lib/armeabi-v7a/libapp.so |
| https://t.me/U8hdkefu8 | lib/armeabi-v7a/libapp.so |
| https://anti-block.gfdhg.com/hwjb\_base.txt | lib/armeabi-v7a/libapp.so |
| https://gfdhg.com/u8\_base.txt | lib/armeabi-v7a/libapp.so |
| https://anti-block.sldgjsdm.com/u8\_base.txt | lib/armeabi-v7a/libapp.so |
| https://dsklgllas.com/hwjb\_base.txt | lib/armeabi-v7a/libapp.so |
| http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd | lib/armeabi-v7a/libapp.so |
| https://dfklssd.com/xyw\_base.txt | lib/armeabi-v7a/libapp.so |
| https://anti-block.dfklssd.com/u8\_base.txt | lib/armeabi-v7a/libapp.so |
| https://www.facebook.com | lib/armeabi-v7a/libapp.so |
| https://github.com/dart-lang/language/issues/3488 | lib/armeabi-v7a/libapp.so |
| https://gfdhg.com/xyw\_base.txt | lib/armeabi-v7a/libapp.so |
| https://anti-block.dsklgllas.com/uu6\_base.txt | lib/armeabi-v7a/libapp.so |
| https://anti-block.gfdhg.com/u8\_base.txt | lib/armeabi-v7a/libapp.so |
| https://anti-block.sldgjsdm.com/hwjb\_base.txt | lib/armeabi-v7a/libapp.so |
| https://gfdhg.com/hwjb\_base.txt | lib/armeabi-v7a/libapp.so |
| https://anti-block.gfdhg.com/uu6\_base.txt | lib/armeabi-v7a/libapp.so |
| https://kk-hongkong-hall-new.dbq9.com/temps/images/2024/04/17/vgDzmACCpDIruPA8.jpg | lib/armeabi-v7a/libapp.so |
| https://kk.net/kk\_base.txt | lib/armeabi-v7a/libapp.so |
| https://sldgjsdm.com/xyw\_base.txt | lib/armeabi-v7a/libapp.so |
| https://dfklssd.com/u8\_base.txt | lib/armeabi-v7a/libapp.so |
| https://api.flutter.dev/flutter/material/Scaffold/of.html | lib/armeabi-v7a/libapp.so |
| https://anti-block.dfklssd.com/xyw\_base.txt | lib/armeabi-v7a/libapp.so |
| https://sldgjsdm.com/u8\_base.txt | lib/armeabi-v7a/libapp.so |
| https://t.me/ | lib/armeabi-v7a/libapp.so |
| https://dsklgllas.com/uu6\_base.txt | lib/armeabi-v7a/libapp.so |
| https://play.google.com/store/apps/details?id=com.azure.authenticator | lib/armeabi-v7a/libapp.so |
| https://anti-block.dsklgllas.com/hwjb\_base.txt | lib/armeabi-v7a/libapp.so |
| https://dsklgllas.com/u8\_base.txt | lib/armeabi-v7a/libapp.so |
| https://dfklssd.com/uu6\_base.txt | lib/armeabi-v7a/libapp.so |
| https://t.me/U8com\_cn | lib/armeabi-v7a/libapp.so |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android. | lib/armeabi-v7a/libapp.so |
| https://anti-block.gfdhg.com/xyw\_base.txt | lib/armeabi-v7a/libapp.so |
| https://github.com/flutter/flutter/issues/new. | lib/armeabi-v7a/libapp.so |
| http://www.unicode.org/copyright.html | 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 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0  u0013android@android.com | m5/u.java |
| appro@openssl.org | lib/arm64-v8a/libflutter.so |
| \_nativesocket@14069316.listen  \_httpparser@13463476.responsepa  channelcontroller@29092078.implementa  \_internetaddress@14069316.fixed  \_double@0150898.fromintege  \_future@4048458.immediate  \_growablelist@0150898.\_literal  \_link@14069316.fromrawpat  \_growablelist@0150898.withcapaci  \_growablelist@0150898.\_literal6  \_receiveportimpl@1026248.fromrawrec  \_colorfilter@15065589.mode  \_imagefilter@15065589.composed  \_list@0150898.\_ofarray  \_timer@1026248.periodic  \_growablelist@0150898.\_literal2  \_bigintimpl@0150898.from  \_list@0150898.empty  \_directory@14069316.fromrawpat  \_invocationmirror@0150898.\_withtype  \_colorfilter@15065589.lineartosr  \_growablelist@0150898.\_literal1  \_uri@0150898.file  \_imagefilter@15065589.blur  \_compressednode@45137193.single  \_growablelist@0150898.\_literal4  \_assetmanifestbin@53287047.fromstanda  \_growablelist@0150898.\_ofgrowabl  \_growablelist@0150898.of  authenticationscheme@13463476.fromstring  \_list@0150898.of  \_list@0150898.generate  \_typeerror@0150898.\_create  \_list@0150898.\_ofgrowabl  \_list@0150898.\_ofefficie  \_growablelist@0150898.\_ofarray  \_growablelist@0150898.\_literal3  \_growablelist@0150898.\_ofother  \_hashcollisionnode@45137193.fromcollis  \_future@4048458.value  \_timer@1026248.\_internal  androidstorage@31339836.implementa  \_growablelist@0150898.\_literal5  \_list@0150898.\_ofother  \_bytebuffer@7027147.\_new  \_routedata@1176504625.ofroute  ngstreamsubscription@4048458.zoned  \_assertionerror@0150898.\_create  \_nativesocket@14069316.normal  \_pointerpanzoomdata@424213599.fromupdate  channelcontroller@27156646.implementa  \_imagefilter@15065589.fromcolorf  \_colorfilter@15065589.srgbtoline  \_uri@0150898.directory  \_httpparser@13463476.requestpar  \_growablelist@0150898.\_literal8  \_file@14069316.fromrawpat  \_growablelist@0150898.generate  \_uri@0150898.notsimple  \_growablelist@0150898.\_literal7  \_future@4048458.zonevalue  \_growablelist@0150898.\_ofefficie  \_future@4048458.immediatee | lib/armeabi-v7a/libapp.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099 | j6/a.java |
| 18222222222 | s3/e.java |

## **5. 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: CN=Android Debug, O=Android, C=US 签名算法: rsassa\_pkcs1v15 有效期自: 2024-05-11 05:50:55+00:00 有效期至: 2054-05-04 05:50:55+00:00 发行人: CN=Android Debug, O=Android, C=US 序列号: 0x1 哈希算法: sha1 md5值: 21bd64fc6cee67f7c792676e6b6ad397 sha1值: 33dafd2513e2edebf5ff340e9bf6138d2b3c9f2e sha256值: 4a7faf79cabdfbfe4963d639c04a7e6c21bdf53556b07aeca41dbe7bea0707f3 sha512值: 71d4619957617ff88b3f0fe7953ce9e5221aea36d7fb2f91253ea53a4e584bc5d91f6f726a8e613ce284186dff7950ed82651ee1835c31400d1f23c6eb206313 公钥算法: rsa 密钥长度: 2048 指纹: 76972747edf601c7c807e36656fc68c86a517001bc0a2b042b132f85ab2f33dd**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "google\_api\_key" : "AIzaSyDQzCiTNgRWH6CUFVfSXm\_lh68tLK0tEhA" |
| "google\_crash\_reporting\_api\_key" : "AIzaSyDQzCiTNgRWH6CUFVfSXm\_lh68tLK0tEhA" |
| "mq\_auth\_code" : "验证码" |
| "mq\_auth\_code" : "認証コード" |
| "mq\_auth\_code" : "Kode verifikaso" |
| "mq\_auth\_code" : "รหัสยืนยัน" |
| "mq\_auth\_code" : "ओटीपी" |
| "mq\_auth\_code" : "Mã xác thực" |
| "mq\_auth\_code" : "CAPTCHA" |
| "mq\_auth\_code" : "Kode verifikaso" |
| "mq\_auth\_code" : "인증 코드" |
| "mq\_auth\_code" : "Código de Autenticação" |
| "mq\_auth\_code" : "Kod pengesahan" |
| "mq\_auth\_code" : "Código de autenticación" |
| "mq\_auth\_code" : "Код подтверждения" |
| "mq\_auth\_code" : "驗證碼" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.example.kkguoji.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.example.kkguoji.MainActivity | **Schemes**: huionetokkgj://, beard18://, https://,  **Hosts:** open, bu48l.app.link, bu48l-alternate.app.link, example.test-app.link, example-alternate.test-app.link, |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**