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

**Hola Cash（ 1.1.7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 | Hola Cash |
| 版本 | 1.1.7 |
| 包名 | com.indiaholacash.holacash |
| 域名线索 | 40条 |
| URL线索 | 26条 |
| APP图标 |  |
| 分析日期 | 2024年12月23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 | Hola+Cash.apk |
| 文件大小 | 13.95MB |
| MD5值 | b97305edcd72c707e0b35a687293ba85 |
| SHA1值 | 3ae40d44647706aeed7795d46f66980bf277e9b3 |
| SHA256值 | 03a87f3df4035318f172900e93be834dbc656504c7aa7f0c67f435cf6b00a64b |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Hola Cash |
| 包名 | com.indiaholacash.holacash |
| 主活动Activity | com.mexico.inloancash.activity.IndiaLaunchActivity |
| 安卓版本名称 | 1.1.7 |
| 安卓版本 | 11 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| subscription.us.adjust.com | IP: 185.151.204.70  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| adminmxwj.cashbeemuch.com | 没有服务器地理信息. |
| gdpr.tr.adjust.com | IP: 195.244.54.7  所属国家: Turkey  地区: Izmir  城市: Izmir |
| sonelink.s | 没有服务器地理信息. |
| sconversions.s | 没有服务器地理信息. |
| pv.sohu.com | IP: 140.249.84.135  所属国家: China  地区: Shandong  城市: Jinan |
| app.adjust.world | IP: 185.151.204.40  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| sattr.s | 没有服务器地理信息. |
| gdpr.eu.adjust.com | IP: 185.151.204.60  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| sinapps.s | 没有服务器地理信息. |
| app.adjust.net.in | IP: 185.151.204.30  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| sgcdsdk.s | 没有服务器地理信息. |
| subscription.adjust.com | IP: 185.151.204.52  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| gdpr.adjust.world | IP: 185.151.204.40  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| app.tr.adjust.com | IP: 195.244.54.6  所属国家: Turkey  地区: Izmir  城市: Izmir |
| simpression.s | 没有服务器地理信息. |
| gdpr.adjust.com | IP: 185.151.204.51  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| svalidate.s | 没有服务器地理信息. |
| gdpr.us.adjust.com | IP: 185.151.204.70  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| in-api.advance.ai | 没有服务器地理信息. |
| github.com | IP: 20.205.243.166  所属国家: United States of America  地区: Washington  城市: Redmond |
| sapp.s | 没有服务器地理信息. |
| slaunches.s | 没有服务器地理信息. |
| app.eu.adjust.com | IP: 185.151.204.60  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| sregister.s | 没有服务器地理信息. |
| uc.qbox.me | IP: 42.202.211.103  所属国家: China  地区: Liaoning  城市: Chaoyang |
| subscription.adjust.net.in | IP: 185.151.204.34  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| www.facebook.com | IP: 128.121.146.109  所属国家: United States of America  地区: California  城市: Milpitas |
| sstats.s | 没有服务器地理信息. |
| ssdk-services.s | 没有服务器地理信息. |
| app.us.adjust.com | IP: 185.151.204.70  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| uplog.qbox.me | IP: 42.202.211.91  所属国家: China  地区: Liaoning  城市: Chaoyang |
| app.adjust.com | IP: 185.151.204.7  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| gdpr.adjust.net.in | IP: 185.151.204.51  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| subscription.adjust.world | IP: 185.151.204.44  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| admininwb.holymondy.com | IP: 172.67.214.2  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| www.instagram.com | IP: 108.160.165.139  所属国家: United States of America  地区: California  城市: San Francisco |
| subscription.tr.adjust.com | IP: 195.244.54.6  所属国家: Turkey  地区: Izmir  城市: Izmir |
| subscription.eu.adjust.com | IP: 185.151.204.60  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| adminyna.easycasher.club | IP: 172.67.157.150  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://admininwb.holymondy.com/appapi/login/agreement | ඓ/ඓ/K/䁗/C0730.java |
| http://adminyna.easycasher.club/adminappapi/ | ඓ/ඓ/K/㿎/C0701.java |
| http://pv.sohu.com/cityjson?ie=utf-8 | ඓ/ඓ/K/ῲ/RunnableC0646.java |
| https://uplog.qbox.me/log/3 | ඓ/ⁱ/K/K/C1260.java |
| https://uplog.qbox.me/log/3 | ඓ/ⁱ/K/ʬ/C1248.java |
| https://uc.qbox.me | ඓ/ⁱ/K/ῲ/C1255.java |
| http://%s | ඓ/ⁱ/K/ῲ/AbstractC1258.java |
| https://adminmxwj.cashbeemuch.com/appapi/login/prestamos\_privacy\_agreement.html | com/mexico/inloancash/activity/IndiaCodeActivity.java |
| https://adminmxwj.cashbeemuch.com/appapi/login/prestamos\_privacy\_agreement.html | com/mexico/inloancash/activity/IndiaLoginActivity.java |
| https://adminmxwj.cashbeemuch.com/appapi/login/prestamos\_privacy\_agreement.html | com/mexico/inloancash/activity/IndiaConfirm\_LoanActivity.java |
| https://in-api.advance.ai/in/openapi/face-identity/v1/id-card-ocr | com/mexico/inloancash/fragment/IndiaStepOneAuthFragment.java |
| https://in-api.advance.ai/in/openapi/face-identity/v1/face-comparison | com/mexico/inloancash/fragment/IndiaStepOneAuthFragment.java |
| https://www.facebook.com/ | com/mexico/inloancash/fragment/IndiaPersonalFragment.java |
| https://www.instagram.com/ | com/mexico/inloancash/fragment/IndiaPersonalFragment.java |
| https://app.adjust.com | com/adjust/sdk/Constants.java |
| https://gdpr.adjust.com | com/adjust/sdk/Constants.java |
| https://subscription.adjust.com | com/adjust/sdk/Constants.java |
| https://github.com/adjust/android\_sdk | com/adjust/sdk/ActivityHandler.java |
| https://app.adjust.world | com/adjust/sdk/network/UrlStrategy.java |
| https://app.eu.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://app.adjust.net.in | com/adjust/sdk/network/UrlStrategy.java |
| https://app.tr.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://app.us.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://gdpr.adjust.world | com/adjust/sdk/network/UrlStrategy.java |
| https://gdpr.eu.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://gdpr.adjust.net.in | com/adjust/sdk/network/UrlStrategy.java |
| https://gdpr.tr.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://gdpr.us.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://subscription.adjust.world | com/adjust/sdk/network/UrlStrategy.java |
| https://subscription.eu.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://subscription.adjust.net.in | com/adjust/sdk/network/UrlStrategy.java |
| https://subscription.tr.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://subscription.us.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| http://%s | lib/arm64-v8a/libaailiveness\_v1.2.9.so |
| http://pre-staging-%s | lib/arm64-v8a/libaailiveness\_v1.2.9.so |
| http://%s-%s/%s | lib/arm64-v8a/libaailiveness\_v1.2.9.so |
| http://pre-staging-%s-%s/%s | lib/arm64-v8a/libaailiveness\_v1.2.9.so |
| http://%s | lib/armeabi-v7a/libaailiveness\_v1.2.9.so |
| http://pre-staging-%s | lib/armeabi-v7a/libaailiveness\_v1.2.9.so |
| http://%s-%s/%s | lib/armeabi-v7a/libaailiveness\_v1.2.9.so |
| http://pre-staging-%s-%s/%s | lib/armeabi-v7a/libaailiveness\_v1.2.9.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ftp@example.com | lib/arm64-v8a/libaailiveness\_v1.2.9.so |
| ftp@example.com | lib/armeabi-v7a/libaailiveness\_v1.2.9.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17222222222 | com/appsflyer/AppsFlyerLibCore.java |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=CN, ST=heimei, L=heimei, O=heimei, OU=heimei, CN=heimei 签名算法: rsassa\_pkcs1v15 有效期自: 2021-09-30 10:01:10+00:00 有效期至: 2046-09-24 10:01:10+00:00 发行人: C=CN, ST=heimei, L=heimei, O=heimei, OU=heimei, CN=heimei 序列号: 0x6732cfdf 哈希算法: sha256 md5值: 4dcbf738523dda5c1e1396ceb9fce247 sha1值: 747670844b22f9af04094645e64a5b568e89d314 sha256值: 2517ea7b36af342abc6cc785a95028903a63518c21d1d90374c9a2c5a3500cc0 sha512值: 6142206f4f6fe69b46c66efe781f7e6a211c7f1fb6566e83a1753e91f9ce4a86508d4c663eebef5de3a73ce81e23a81d605a8718e9a71491f36525663eabe280 公钥算法: rsa 密钥长度: 2048 指纹: f02a9174ec5a5d5a42b9e3677605277d8551733603241eb272c8ef2371b1787d**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "com\_facebook\_device\_auth\_instructions" : "Visit <b>facebook.com/device</b> and enter the code shown above." |
| "complete\_data\_authentication" : "Por favor, complete la autentificación de datos" |
| "data\_authentication" : "Autenticación de datos" |
| "india\_auths\_completes" : "Completa" |
| "india\_titles\_auths" : "Certificación" |
| "liveness\_auth\_check" : "Please Wait" |
| "liveness\_failed\_reason\_auth\_failed" : "Authorization failed, please check network" |
| "login\_pwd" : "Dapatkan Kode" |
| "com\_facebook\_device\_auth\_instructions" : "Gå til <b>facebook.com/device</b> og indtast koden, som er vist ovenfor." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>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" : "<b>facebook.com/device</b> 'ਤੇ ਵਿਜਿਟ ਕਰੋ ਅਤੇ ਉੱਪਰ ਦਿੱਤੇ ਕੋਡ ਨੂੰ ਦਾਖ਼ਲ ਕਰੋ।" |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> ஐப் பார்வையிட்டு, மேலே காட்டப்பட்ட குறியீட்டை உள்ளிடவும்." |
| "com\_facebook\_device\_auth\_instructions" : "Gå til <b>facebook.com/device</b> og skriv inn koden som vises over." |
| "com\_facebook\_device\_auth\_instructions" : "Gehe zu <b>facebook.com/device</b> und gib den oben angezeigten Code ein." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>ని సందర్శించి ఎగువన చూపిన కోడ్‌ను నమోదు చేయండి." |
| "com\_facebook\_device\_auth\_instructions" : "Besoek <b>facebook.com/device</b> en voer die kode wat hierbo gewys word, in." |
| "com\_facebook\_device\_auth\_instructions" : "ไปที่ <b>facebook.com/device</b> แล้วป้อนรหัสที่ปรากฏด้านล่าง" |
| "com\_facebook\_device\_auth\_instructions" : "Siirry osoitteeseen <b>facebook.com/device</b> ja anna oheinen koodi." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> पर विज़िट करें और ऊपर दिखाया गया कोड डालें." |
| "com\_facebook\_device\_auth\_instructions" : "Truy cập <b>facebook.com/device</b> và nhập mã được hiển thị bên trên." |
| "com\_facebook\_device\_auth\_instructions" : "Navštívte stránku <b>facebook.com/device</b> a zadajte kód zobrazený vyššie." |
| "com\_facebook\_device\_auth\_instructions" : "Πηγαίνετε στη διεύθυνση <b>facebook.com/device</b> και εισαγάγετε τον παραπάνω κωδικό." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> സന്ദർശിച്ച് മുകളിൽ കാണിച്ചിരിക്കുന്ന കോഡ് നൽകുക." |
| "com\_facebook\_device\_auth\_instructions" : "Ga naar <b>facebook.com/device</b> en voer de bovenstaande code in." |
| "com\_facebook\_device\_auth\_instructions" : "Odwiedź stronę <b>facebook.com/device</b> i wprowadź powyższy kod." |
| "com\_facebook\_device\_auth\_instructions" : "Puntahan ang <b>facebook.com/device</b> at ilagay ang code na ipinapakita sa itaas." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> দেখুন এবং উপরে দেখানো কোডটিকে প্রবেশ করান৷" |
| "com\_facebook\_device\_auth\_instructions" : "Kunjungi <b>facebook.com/device</b> dan masukkan kode yang ditampilkan di bawah ini." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> ಗೆ ಭೇಟಿ ನೀಡಿ ಮತ್ತು ಮೇಲೆ ತೋರಿಸಿದ ಕೋಡ್ ಅನ್ನು ನಮೂದಿಸಿ." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>에 방문하여 위 코드를 입력하세요." |
| "com\_facebook\_device\_auth\_instructions" : "Vizitează <b>facebook.com/device</b> şi introdu codul de mai sus." |
| "com\_facebook\_device\_auth\_instructions" : "تفضل بزيارة <b>facebook.com/device</b> وإدخال الرمز الموضح أعلاه." |
| "com\_facebook\_device\_auth\_instructions" : "Consultez <b>facebook.com/device</b> et entrez le code affiché ci-dessus." |
| "com\_facebook\_device\_auth\_instructions" : "Posjetitw <b>facebook.com/device</b> i unesite gore prikazani kôd." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> भेट द्या आणि वरील कोड प्रविष्ट करा." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> adresine git ve yukarıda gösterilen kodu gir." |
| "com\_facebook\_device\_auth\_instructions" : "Přejděte na <b>facebook.com/device</b> a zadejte nahoře uvedený kód." |
| "com\_facebook\_device\_auth\_instructions" : "Ve a <b>facebook.com/device</b> e ingresa el código que se muestra arriba." |
| "com\_facebook\_device\_auth\_instructions" : "Lawati <b>facebook.com/device</b> dan masukkan kod yang ditunjukkan di atas." |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e inserisci il codice mostrato qui sotto." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b&gt ની મુલકાત લો; અને ઉપર આપેલો કોડ દાખલ કરો." |
| "com\_facebook\_device\_auth\_instructions" : "Keresd fel a <b>facebook.com/device</b> címet, és írd be a fent megjelenített kódot." |
| "com\_facebook\_device\_auth\_instructions" : "Откройте <b>facebook.com/device</b> и введите код, показанный выше." |
| "com\_facebook\_device\_auth\_instructions" : "Gå till <b>facebook.com/device</b> 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 <b>facebook.com/device</b> et entrez le code affiché ci-dessus." |
| "com\_facebook\_device\_auth\_instructions" : "前往<b>facebook.com/device</b&gt，並輸入上方顯示的代碼。" |
| "com\_facebook\_device\_auth\_instructions" : "请访问<b>facebook.com/device</b>并输入以上验证码。" |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e insere o código apresentado abaixo." |
| "com\_facebook\_device\_auth\_instructions" : "前往<b>facebook.com/device</b&gt，並輸入上方顯示的代碼。" |
| "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" |
| "liveness\_auth\_check" : "Espere." |
| "liveness\_failed\_reason\_auth\_failed" : "La autorización se ha fallado, examine la red." |
| "liveness\_auth\_check" : "Sila tunggu hingga selesai" |
| "liveness\_failed\_reason\_auth\_failed" : "Kebenaran tidak berjaya, sila periksa rangkaian anda" |
| "com\_facebook\_device\_auth\_instructions" : "Kunjungi <b>facebook.com/device</b> dan masukkan kode yang ditampilkan di atas." |
| "com\_facebook\_device\_auth\_instructions" : "Acesse <b>facebook.com/device</b> e insira o código mostrado acima." |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e introduce el código que se muestra más arriba." |

## **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.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.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.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.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.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.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.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.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.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.READ\_CALL\_LOG | 危险 |  | 允许应用程序读取用户的通话日志 |
| com.google.android.gms.permission.AD\_ID | 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.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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.facebook.CustomTabActivity | **Schemes**: fbconnect://,  **Hosts:** cct.com.indiaholacash.holacash, |

**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。**