MoGua

Hola Cash 1.1.7.APK 分析报告

APP名称: Hola Cash

包名:	com.indiaholacash.holacash
域名线索:	40条
URL线索:	26条
邮箱线索:	2条
分析日期:	2024年12月23日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: Hola+Cash.apk
文件大小: 13.95MB
MD5值: b97305edcd72c707e0b35a687293ba85
SHA1值: 3ae40d44647706aeed7795d46f66980bf277e9b3
SHA256值: 03a87f3df4035318f172900e93be834dbc656504c7aa7f0c67f435cf6b00a64b

APP 信息

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

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 **纬度**: 33.448380 **经度**: -112.074043
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 **纬度**: 38.412731 **经度**: 27.138380

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 **纬度**: 36.668331 **经度**: 116.997223
app.adjust.world	IP: 185.151.204.40 **所属国家**: United States of America **地区**: Arizona **城市**: Phoenix **纬度**: 33.448380 **经度**: -112.074043
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 **纬度**: 33.448380 **经度**: -112.074043
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 **纬度**: 33.448380 **经度**: -112.074043
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 **纬度**: 33.448380 **经度**: -112.074043
gdpr.adjust.world	**IP**: 185.151.204.40 **所属国家**: United States of America **地区**: Arizona **城市**: Phoenix **纬度**: 33.448380 **经度**: -112.074043
app.tr.adjust.com	**IP**: 195.244.54.6 **所属国家**: Turkey **地区**: Izmir **城市**: Izmir **纬度**: 38.412731 **经度**: 27.138380
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 **纬度**: 33.448380 **经度**: -112.074043
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 **纬度**: 33.448380 **经度**: -112.074043

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 **纬度**: 47.682899 **经度**: -122.120903
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 **纬度**: 33.448380 **经度**: -112.074043
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 **纬度**: 40.457420 **经度**: 123.550629
subscription.adjust.net.in	**IP**: 185.151.204.34 **所属国家**: United States of America **地区**: Arizona **城市**: Phoenix **纬度**: 33.448380 **经度**: -112.074043
	IP: 128.121.146.109 **所属国家**: United States of America **地区**: California

www.facebook.com	**城市**: Milpitas **纬度**: 37.428268 **经度**: -121.906616
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 **纬度**: 33.448380 **经度**: -112.074043
uplog.qbox.me	**IP**: 42.202.211.91 **所属国家**: China **地区**: Liaoning **城市**: Chaoyang **纬度**: 40.457420 **经度**: 123.550629
app.adjust.com	**IP**: 185.151.204.7 **所属国家**: United States of America **地区**: Arizona **城市**: Phoenix **纬度**: 33.448380 **经度**: -112.074043
gdpr.adjust.net.in	**IP**: 185.151.204.51 **所属国家**: United States of America **地区**: Arizona **城市**: Phoenix **纬度**: 33.448380 **经度**: -112.074043
	IP: 185.151.204.44 **所属国家**: United States of America

subscription.adjust.world	**地区**: Arizona **城市**: Phoenix **纬度**: 33.448380 **经度**: -112.074043
admininwb.holymondy.com	**IP**: 172.67.214.2 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689507 **经度**: 139.691696
www.instagram.com	**IP**: 108.160.165.139 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
subscription.tr.adjust.com	**IP**: 195.244.54.6 **所属国家**: Turkey **地区**: Izmir **城市**: Izmir **纬度**: 38.412731 **经度**: 27.138380
subscription.eu.adjust.com	**IP**: 185.151.204.60 **所属国家**: United States of America **地区**: Arizona **城市**: Phoenix **纬度**: 33.448380 **经度**: -112.074043
adminyna.easycasher.club	**IP**: 172.67.157.150 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

URL线索

URL信息	Url所在文件
https://admininwb.holymondy.com/appapi/login/agreement	ළු/ළු/K/暟/C0730.java
http://adminyna.easycasher.club/adminappapi/	ළු/ළු/K/瓆/C0701.java
http://pv.sohu.com/cityjson?ie=utf-8	ළු/ළු/K/ẉ̀/RunnableC0646.java
https://uplog.qbox.me/log/3	ළු/ⁱ /K/K/C1260.java
https://uplog.qbox.me/log/3	ළු/ⁱ /K/ʬ/C1248.java
https://uc.qbox.me	ළු/ⁱ /K/ẉ̀/C1255.java
http://%s	ළු/ⁱ /K/ẉ̀/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

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

手机线索

手机号	所在文件

17222222222	com/appsflyer/AppsFlyerLibCore.java

✹ 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

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."
"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 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 ਵਿਜਿਟ 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" : "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" : "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 করান।"
"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" : "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 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。"
"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" : "[illegible]"

"liveness_failed_reason_auth_failed" : "การอนุญาตล้มเหลว กรุณาตรวจสอบเครือข่าย"
"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 facebook.com/device dan masukkan kode yang ditampilkan di atas."
"com_facebook_device_auth_instructions" : "Acesse facebook.com/device e insira o código mostrado acima."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e introduce el código que se muestra más arriba."

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_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

应用内通信

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

---