MoGua

UKU 6.9.16.APK 分析报告

APP名称:	UKU

包名:	com.mintq.gocash
域名线索:	31条
URL线索:	23条
邮箱线索:	1条
分析日期:	2025年4月27日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.mintq.gocash_2024-08-28.apk
文件大小: 34.66MB
MD5值: 9782def7b903092ea5e4b35436f39c97
SHA1值: 9364333338e2a0980f8d0014d192ff7f611efaaf
SHA256值: e95ac836d6dd021dad0625f68c12a29003348d936f0ac801c16d21bb3c6394ec

APP 信息

App名称: UKU
包名: com.mintq.gocash
主活动Activity: com.mintq.gocash.MainActivity
安卓版本名称: 6.9.16
安卓版本: 60916001

域名线索

域名	服务器信息
codepush.appcenter.ms	**IP**: 52.232.227.249 **所属国家**: United States of America **地区**: Virginia **城市**: Boydton **纬度**: 36.667641 **经度**: -78.387497
sstats.s	没有服务器地理信息.
ukuindo-85d87.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

svalidate.s	没有服务器地理信息.
sattr.s	没有服务器地理信息.
sdlsdk.s	没有服务器地理信息.
en.wikipedia.org	**IP**: 31.13.68.169 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
sadrevenue.s	没有服务器地理信息.
docs.swmansion.com	**IP**: 104.21.27.136 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
manual.sensorsdata.cn	**IP**: 125.39.47.209 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
scdn-stestsettings.s	没有服务器地理信息.
scdn-ssettings.s	没有服务器地理信息.
github.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000

	经度: 0.000000
sonelink.s	没有服务器地理信息.
sars.s	没有服务器地理信息.
simpression.s	没有服务器地理信息.
ssdk-services.s	没有服务器地理信息.
slaunches.s	没有服务器地理信息.
ai.80rr.com.sg	**IP**: 129.126.254.131 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
www.samsungapps.com	**IP**: 54.229.93.185 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
sregister.s	没有服务器地理信息.
smonitorsdk.s	没有服务器地理信息.
datahub.ukuindo.com	**IP**: 149.129.192.54 **所属国家**: Indonesia **地区**: Jakarta Raya **城市**: Jakarta **纬度**: -6.208678 **经度**: 106.845490

sinapps.s	没有服务器地理信息.
sconversions.s	没有服务器地理信息.
sapp.s	没有服务器地理信息.
sgcdsdk.s	没有服务器地理信息.
play.google.com	**IP**: 172.217.14.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
192.168.133.11	**IP**: 192.168.133.11 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
sviap.s	没有服务器地理信息.
crashpad.chromium.org	**IP**: 142.250.69.211 **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**

https://en.wikipedia.org/wiki/Hostname	com/sensorsdata/analytics/android/sdk/SensorsDataAPI.java
https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_web_access-7545017.html\	com/sensorsdata/analytics/android/sdk/visual/ViewSnapshot.java
https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenabledroot	com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java
https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting	com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java
https://github.com/software-mansion/react-native-screens/issues/17	com/swmansion/rnscreens/ScreenFragment.java
https://github.com/software-mansion/react-native-screens/issues/17	com/swmansion/rnscreens/ScreenStackFragment.java
http://www.samsungapps.com/appquery/appDetail.as?appId=	com/mintq/gocash/CommunicationModule.java
http://play.google.com/store/apps/details?id=	com/mintq/gocash/CommunicationModule.java
https://datahub.ukuindo.com/log/sensors/upload	com/mintq/gocash/MainApplication.java
https://codepush.appcenter.ms/	com/microsoft/codepush/react/CodePush.java
https://ukuindo-85d87.firebaseio.com	摸瓜V1引擎
http://192.168.133.11:9801/	lib/arm64-v8a/libaailiveness_v2.1.2.so
http://k8s-%s/intl	lib/arm64-v8a/libaailiveness_v2.1.2.so
http://k8s-%s	lib/arm64-v8a/libaailiveness_v2.1.2.so
http://k8s-%s-%s/%s	lib/arm64-v8a/libaailiveness_v2.1.2.so
http://k8s-%s-%s/intl	lib/arm64-v8a/libaailiveness_v2.1.2.so
https://k8s-%s/intl	lib/arm64-v8a/libaailiveness_v2.1.2.so

https://k8s-%s	lib/arm64-v8a/libaailiveness_v2.1.2.so
https://k8s-%s-%s/%s	lib/arm64-v8a/libaailiveness_v2.1.2.so
https://k8s-%s-%s/intl	lib/arm64-v8a/libaailiveness_v2.1.2.so
http://ai.80rr.com.sg:%d	lib/arm64-v8a/libaailiveness_v2.1.2.so
https://crashpad.chromium.org/	lib/arm64-v8a/libcrashlytics-common.so
https://crashpad.chromium.org/bug/new	lib/arm64-v8a/libcrashlytics-common.so

邮箱线索

邮箱地址	所在文件
ftp@example.com	lib/arm64-v8a/libaailiveness_v2.1.2.so

手机线索

手机号	所在文件
15555215554	com/mintq/gocash/device/EmulatorChecker.java
15555215556	com/mintq/gocash/device/EmulatorChecker.java
15555215558	com/mintq/gocash/device/EmulatorChecker.java
15555215560	com/mintq/gocash/device/EmulatorChecker.java

15555215562	com/mintq/gocash/device/EmulatorChecker.java
15555215564	com/mintq/gocash/device/EmulatorChecker.java
15555215566	com/mintq/gocash/device/EmulatorChecker.java
15555215568	com/mintq/gocash/device/EmulatorChecker.java
15555215570	com/mintq/gocash/device/EmulatorChecker.java
15555215572	com/mintq/gocash/device/EmulatorChecker.java
15555215574	com/mintq/gocash/device/EmulatorChecker.java
15555215576	com/mintq/gocash/device/EmulatorChecker.java
15555215578	com/mintq/gocash/device/EmulatorChecker.java
15555215580	com/mintq/gocash/device/EmulatorChecker.java
15555215582	com/mintq/gocash/device/EmulatorChecker.java
15555215584	com/mintq/gocash/device/EmulatorChecker.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=86, ST=beijing, L=beijing, O=mintq, OU=CN, CN=mintq_gocash
签名算法: rsassa_pkcs1v15

有效期自: 2017-08-28 09:06:56+00:00
有效期至: 2042-08-22 09:06:56+00:00
发行人: C=86, ST=beijing, L=beijing, O=mintq, OU=CN, CN=mintq_gocash
序列号: 0x7c6d0d4b
哈希算法: sha256
md5值: 9d7f5b08dccce1f89d410ab4b273efcc
sha1值: 4c9dc895416ee2aa4db436282a5fed15b3b4493d
sha256值: 601dc0ad523218d5caf2060324a5dfbc2ba41c66e8ea3485242546fb2aedc1d3
sha512值: d7ae6b3993abd4df356979194c12b853b1549624316c91a05b695f114200a2c05c8310ad74259fd4981d3e92e74f24e502d46392b26e757cc4283d5cf59b7058
公钥算法: rsa
密钥长度: 2048
指纹: 53ca5083073ed19974b7fd8e97b123f5685a3214b2a6b2f8b787649906c92d4a

硬编码敏感信息

可能的敏感信息
"CodePushDeploymentKey" : "5YZDg29LKZOFPkT28W0D2q3LRKHBdFaMoXSO-"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"com_facebook_device_auth_instructions" : "Visit facebook.com/device and enter the code shown above."
"facebook_client_token" : "929f7c0f0837c4c83be7da894ecdd8c5"
"firebase_database_url" : "https://ukuindo-85d87.firebaseio.com"
"google_api_key" : "AIzaSyD4L1J8UPZfOOlj_GCieYI-S0sncWeWdQc"
"google_crash_reporting_api_key" : "AIzaSyD4L1J8UPZfOOlj_GCieYI-S0sncWeWdQc"
"liveness_auth_check" : "Please Wait"
"liveness_failed_reason_auth_failed" : "Authorization failed, please check network"

"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" : "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" : "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" : "ולהזין את הקוד המוצג למעלה facebook.com/device</b&gt יש לבקר בכתובת"
"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" : "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 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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
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.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
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.TRANSMIT_IR	正常		允许使用该设备'小号IR发射器,如果有的话。
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
		Unknown	

com.google.android.gms.permission.AD_ID	未知	permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
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.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.mintq.gocash.MainActivity	Schemes: uku://, Hosts: mintq.com, Path Prefixes: /link,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.mintq.gocash,

---