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

**Ajaib（ 2.71.0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 | Ajaib |
| 版本 | 2.71.0 |
| 包名 | ajaib.co.id |
| 域名线索 | 71条 |
| URL线索 | 113条 |
| APP图标 |  |
| 分析日期 | 2025年6月21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 | ajaib.co.id.apk |
| 文件大小 | 65.19MB |
| MD5值 | 61d07a8bf007a892e5e6e838a39d8f46 |
| SHA1值 | c0f6ed4f161abbb4fa32d6cf9aaa02db9e451da8 |
| SHA256值 | 481aeebd8869bd0c44d676a20c04fde0ee15c1e3fb0791399b78b221a5239152 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Ajaib |
| 包名 | ajaib.co.id |
| 主活动Activity | ajaib.co.id.pages.splash.SplashActivity |
| 安卓版本名称 | 2.71.0 |
| 安卓版本 | 292 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| wa.me | IP: 31.13.70.49 所属国家: United States of America 地区: California 城市: Los Angeles  |
| ajaib.co.id | IP: 35.219.122.218 所属国家: Indonesia 地区: Jakarta Raya 城市: Jakarta  |
| referral.kripto.ajaib.co.id | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| simpression.s | 没有服务器地理信息.  |
| academy-public.coinmarketcap.com | IP: 96.44.137.28 所属国家: United States of America 地区: California 城市: Los Angeles  |
| embrace.io | IP: 3.165.39.81 所属国家: United States of America 地区: Washington 城市: Seattle  |
| alpha.ajaib.co.id | IP: 35.219.122.218 所属国家: Indonesia 地区: Jakarta Raya 城市: Jakarta  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| goo.gl | IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| svalidate.s | 没有服务器地理信息.  |
| chart.ajaib.co.id | IP: 34.128.157.217 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| www.youtube.com | IP: 142.251.33.78 所属国家: Canada 地区: Ontario 城市: Toronto  |
| console.firebase.google.com | IP: 108.177.98.113 所属国家: United States of America 地区: California 城市: Mountain View  |
| scdn-ssettings.s | 没有服务器地理信息.  |
| app.yellowmessenger.com | IP: 104.18.0.51 所属国家: United States of America 地区: California 城市: San Francisco  |
| plus.google.com | IP: 104.244.46.165 所属国家: United States of America 地区: California 城市: San Francisco  |
| sgcdsdk.s | 没有服务器地理信息.  |
| sinapps.s | 没有服务器地理信息.  |
| accounts.google.com | IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan  |
| firebase-settings.crashlytics.com | IP: 114.250.67.34 所属国家: China 地区: Beijing 城市: Beijing  |
| sonelink.s | 没有服务器地理信息.  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| form.typeform.com | IP: 50.19.18.130 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| webview-stg.ajaib.tech | IP: 35.219.33.165 所属国家: Indonesia 地区: Jakarta Raya 城市: Jakarta  |
| x.com | IP: 172.66.0.227 所属国家: United States of America 地区: California 城市: San Francisco  |
| dash-api.embrace.io | IP: 54.149.136.13 所属国家: United States of America 地区: Oregon 城市: Portland  |
| external-api.ajaib.co.id | IP: 35.219.102.145 所属国家: Indonesia 地区: Jakarta Raya 城市: Jakarta  |
| chart-v2.ajaib.co.id | IP: 34.149.242.52 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| ssdk-services.s | 没有服务器地理信息.  |
| www.instagram.com | IP: 104.244.46.211 所属国家: United States of America 地区: California 城市: San Francisco  |
| aps-webhandler.appsflyer.com | IP: 13.225.158.120 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| referral.ajaib.co.id | IP: 151.101.65.195 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.mixpanel.com | IP: 35.190.25.25 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| coinmarketcap.com | IP: 103.246.246.144 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| svalidate-and-log.s | 没有服务器地理信息.  |
| sconversions.s | 没有服务器地理信息.  |
| firebase.google.com | IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| slaunches.s | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| play.google.com | IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe  |
| docs.google.com | IP: 31.13.94.36 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| sars.s | 没有服务器地理信息.  |
| img.youtube.com | IP: 199.16.158.182 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.tiktok.com | IP: 80.87.199.46 所属国家: Russian Federation 地区: Irkutskaya oblast' 城市: Irkutsk  |
| webview.ajaib.cloud | IP: 35.219.102.145 所属国家: Indonesia 地区: Jakarta Raya 城市: Jakarta  |
| www.googleadservices.com | IP: 114.250.67.38 所属国家: China 地区: Beijing 城市: Beijing  |
| httpbin.org | IP: 35.169.248.232 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| firebaseremoteconfigrealtime.googleapis.com | IP: 142.250.217.74 所属国家: United States of America 地区: California 城市: Mountain View  |
| simpleicon.com | IP: 35.194.90.46 所属国家: United States of America 地区: District of Columbia 城市: Washington  |
| javax.xml.xmlconstants | 没有服务器地理信息.  |
| www.example.com | IP: 92.122.244.34 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| oid.ajaib.co.id | IP: 35.219.102.145 所属国家: Indonesia 地区: Jakarta Raya 城市: Jakarta  |
| tradingview.ajaib.co.id | IP: 35.219.102.145 所属国家: Indonesia 地区: Jakarta Raya 城市: Jakarta  |
| sattr.s | 没有服务器地理信息.  |
| smonitorsdk.s | 没有服务器地理信息.  |
| ajaib.onelink.me | IP: 3.173.254.28 所属国家: United States of America 地区: Washington 城市: Seattle  |
| app-measurement.com | IP: 114.250.69.33 所属国家: China 地区: Beijing 城市: Beijing  |
| sviap.s | 没有服务器地理信息.  |
| developer.android.com | IP: 142.251.33.78 所属国家: Canada 地区: Ontario 城市: Toronto  |
| www.e-ipo.co.id | IP: 104.18.12.96 所属国家: United States of America 地区: California 城市: San Francisco  |
| scdn-stestsettings.s | 没有服务器地理信息.  |
| sdlsdk.s | 没有服务器地理信息.  |
| sadrevenue.s | 没有服务器地理信息.  |
| sapp.s | 没有服务器地理信息.  |
| tradingview-stg.ajaib.tech | IP: 35.219.33.165 所属国家: Indonesia 地区: Jakarta Raya 城市: Jakarta  |
| sregister.s | 没有服务器地理信息.  |
| kripto.ajaib.co.id | IP: 35.219.122.218 所属国家: Indonesia 地区: Jakarta Raya 城市: Jakarta  |
| www.tradingview.com | IP: 31.13.90.19 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| static.wizrocket.com | IP: 3.165.39.75 所属国家: United States of America 地区: Washington 城市: Seattle  |
| login.ajaib.co.id | IP: 35.219.102.145 所属国家: Indonesia 地区: Jakarta Raya 城市: Jakarta  |
| google.com | IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://webview.ajaib.cloud/faq/detail?topic=25&title=Transaksi%20Otomatis%20Reksa%20Dana  | a10/j.java  |
| https://oid.ajaib.co.id/api/  | ajaib/co/id/AjaibApp.java  |
| https://external-api.ajaib.co.id/api/  | ajaib/co/id/AjaibApp.java  |
| https://docs.google.com/viewerng/viewer?embedded=true&url=  | ajaib/co/id/pages/webView/WebViewPdfActivity.java  |
| https://webview.ajaib.cloud/goals/usp  | b10/g.java  |
| https://webview.ajaib.cloud/tnc/coin  | c7/n1.java  |
| https://console.firebase.google.com  | c7/f7.java  |
| https://aps-webhandler.appsflyer.com/api/trigger  | com/appsflyer/internal/AFj1xSDK.java  |
| https://app.yellowmessenger.com/api/chat/upload?bot=  | com/yellowmessenger/ymchat/t.java  |
| https://app.yellowmessenger.com  | com/yellowmessenger/ymchat/t.java  |
| https://app.yellowmessenger.com/api/presence/usersPresence/log\_user\_profile  | com/yellowmessenger/ymchat/t.java  |
| http://javax.xml.XMLConstants/feature/secure-processing  | com/chuckerteam/chucker/internal/data/entity/HttpTransaction.java  |
| http://xml.apache.org/xslt  | com/chuckerteam/chucker/internal/data/entity/HttpTransaction.java  |
| https://ajaib.onelink.me/cmDI?isin\_code=  | d7/m7.java  |
| https://ajaib.onelink.me/2AJb?fund\_id=  | d7/n7.java  |
| https://coinmarketcap.com/alexandria/article/luna-off-to-a-bad-start-after-re-launch-dumps-75  | d3/a.java  |
| https://academy-public.coinmarketcap.com/optimized-uploads/a1b35a5ebcf64d4dadf43607f4902d43.jpeg  | d3/a.java  |
| https://webview.ajaib.cloud/tnc/qris  | e40/e.java  |
| https://webview.ajaib.cloud/tnc/privacy-policy  | e40/e.java  |
| https://www.youtube.com  | ec/a.java  |
| https://www.example.com  | e3/k.java  |
| https://app-measurement.com/a  | g7/r2.java  |
| https://goo.gl/NAOOOI.  | g7/v5.java  |
| https://goo.gl/NAOOOI  | g7/v5.java  |
| https://firebase.google.com/support/guides/disable-analytics  | g7/u2.java  |
| https://www.googleadservices.com/pagead/conversion/app/deeplink?id\_type=adid&sdk\_version=%s&rdid=%s&bundleid=%s&retry=%s  | g7/g4.java  |
| https://alpha.ajaib.co.id/sahamas/  | f90/k.java  |
| http://simpleicon.com/wp-content/uploads/rocket.png  | ei/p.java  |
| http://simpleicon.com/wp-content/uploads/rocket.png  | ei/n.java  |
| http://static.wizrocket.com/android/ico//  | g3/b.java  |
| https://)?(www.)?(([a-zA-Z0-9-])  | id/co/ajaib/base/android/ExtentionsKt.java  |
| https://play.google.com/store/apps/details?id=  | id/co/ajaib/base/android/utils/IntentUtils.java  |
| https://ajaib.co.id/trade-limit-cashback-50-ribu/  | id/co/ajaib/base/layout/stock/customviews/buyform/StockBuyFormSectionView.java  |
| https://ajaib.co.id/trade-limit-cashback-50-ribu/  | id/co/ajaib/base/layout/stock/customviews/buyform/StockBuyFormSectionView$updateFormCashTLParams$1$4$1.java  |
| https://webview.ajaib.cloud/tnc/margin-trading  | id/co/ajaib/feature/mt/pages/mtUSPActivation/mtUSPTNC/MTUSPTNCActivity.java  |
| https://webview.ajaib.cloud/tnc/margin-trading  | id/co/ajaib/feature/kyc/pages/submit/marginTrading/tnc/MTTNCActivationFragment.java  |
| https://webview.ajaib.cloud/kyc/coin-info?contentCopy=  | id/co/ajaib/feature/kyc/pages/submitCoinCrossSell/KYCCoinCrossSellSubmitViewModel.java  |
| https://webview.ajaib.cloud/kyc/coin-info  | id/co/ajaib/feature/kyc/pages/submitCoinCrossSell/KYCCoinCrossSellSubmitViewModel.java  |
| https://webview.ajaib.cloud/tnc/coin-permata  | id/co/ajaib/feature/kyc/view/kycTncForm/KYCTncFormView.java  |
| https://webview.ajaib.cloud/tnc/coin-bca  | id/co/ajaib/feature/kyc/view/kycTncForm/KYCTncFormView.java  |
| https://webview.ajaib.cloud/tnc/kyc-bca  | id/co/ajaib/feature/kyc/view/kycTncForm/KYCTncFormView.java  |
| https://webview.ajaib.cloud/tnc/kyc-mandiri  | id/co/ajaib/feature/kyc/view/kycTncForm/KYCTncFormView.java  |
| https://webview.ajaib.cloud/tnc/kyc  | id/co/ajaib/feature/kyc/view/kycTncForm/KYCTncFormView.java  |
| https://ajaib.onelink.me/DXmL  | id/co/ajaib/feature/shared/search/fragments/emptyState/topGainerSection/TopGainerSectionViewModel.java  |
| https://ajaib.onelink.me/DXmL  | id/co/ajaib/feature/shared/search/fragments/emptyState/topLoserSection/TopLoserSectionViewModel.java  |
| https://ajaib.onelink.me/DXmL  | id/co/ajaib/feature/shared/search/fragments/typingState/searchCenterAsset/SearchCenterViewModel.java  |
| https://ajaib.onelink.me/WnsZ  | id/co/ajaib/feature/shared/search/fragments/typingState/searchCenterAsset/SearchCenterViewModel.java  |
| https://ajaib.onelink.me/DXmL  | id/co/ajaib/feature/shared/search/fragments/typingState/searchAllAsset/SearchAllAssetViewModel.java  |
| https://ajaib.onelink.me/WnsZ  | id/co/ajaib/feature/shared/search/fragments/typingState/searchAllAsset/SearchAllAssetViewModel.java  |
| https://webview.ajaib.cloud/faq/detail?topic=24&title=Kantong  | id/co/ajaib/feature/pocket/pages/creation/PocketCreationActivity.java  |
| https://webview.ajaib.cloud/pocket/usp  | id/co/ajaib/feature/pocket/pages/usp/PocketUSPActivity.java  |
| https://ajaib.onelink.me/DXmL/  | id/co/ajaib/feature/widget/view/watchlist/stock/WidgetStockWatchlistProvider.java  |
| https://ajaib.onelink.me/DXmL/  | id/co/ajaib/feature/widget/view/stock/WidgetStockProvider.java  |
| https://webview.ajaib.cloud/faq/  | id/co/ajaib/feature/faq/pages/faqWeb/FAQWebActivity.java  |
| https://webview.ajaib.cloud/coin/btc-halving  | id/co/ajaib/coin/feature/catalogue/pages/halving/CoinHalvingActivity.java  |
| http://www.youtube.com/watch?v=  | hc/b.java  |
| https://a-  | io/embrace/android/embracesdk/config/behavior/SdkEndpointBehavior.java  |
| https://developer.android.com/studio/write/java8-support  | io/embrace/android/embracesdk/injection/OpenTelemetryModuleImpl$openTelemetrySdk$2.java  |
| https://embrace.io/docs/android/changelog/  | io/embrace/android/embracesdk/samples/VerificationActions.java  |
| https://dash-api.embrace.io/external/sdk/android/version  | io/embrace/android/embracesdk/samples/VerificationActions.java  |
| https://httpbin.org/post  | io/embrace/android/embracesdk/samples/VerificationActions.java  |
| https://httpbin.org/deaasd/ASdasdkjl  | io/embrace/android/embracesdk/samples/VerificationActions.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| https://webview.ajaib.cloud/tnc/mutual-fund  | k00/i.java  |
| https://google.com/search?  | k6/e.java  |
| https://ajaib.co.id/xtra-bonus-reksa-dana/  | mp0/f.java  |
| https://webview.ajaib.cloud/tnc/mutual-fund  | m00/j.java  |
| https://plus.google.com/  | n6/p0.java  |
| https://form.typeform.com/to/W4eJ26vW  | o0/e0.java  |
| https://webview.ajaib.cloud/bonds/discovery/usp?isin\_code=  | pn0/f.java  |
| https://www.e-ipo.co.id/id/login  | rz0/g.java  |
| https://www.e-ipo.co.id/id/register  | rz0/g.java  |
| https://www.e-ipo.co.id/id/login  | rz0/e0.java  |
| https://www.e-ipo.co.id/id/register  | rz0/e0.java  |
| https://github.com/mixpanel/mixpanel-android/issues/567)  | sa/c.java  |
| https://api.mixpanel.com/track/  | sa/j.java  |
| https://api.mixpanel.com/engage/  | sa/j.java  |
| https://api.mixpanel.com/groups/  | sa/j.java  |
| https://kripto.ajaib.co.id/otc  | r40/a.java  |
| https://firebaseremoteconfigrealtime.googleapis.com/v1/projects/%s/namespaces/%s:streamFetchInvalidations  | r9/n.java  |
| https://webview.ajaib.cloud/tnc/stock  | rr/j.java  |
| https://webview.ajaib.cloud/tnc/stock  | sr/i.java  |
| https://ajaib.onelink.me/SgM5  | st0/p.java  |
| https://chart.ajaib.co.id/coin?type=  | sen/com/coin/fragments/coinChart/PCoinChart.java  |
| https://chart((.ajaib.co.id)  | sen/com/coin/fragments/coinChart/FCoinChart.java  |
| https://tradingview.ajaib.co.id/  | sen/com/coin/pages/tradingView/CoinTradingViewPresenter.java  |
| https://tradingview-stg.ajaib.tech/  | sen/com/coin/pages/tradingView/CoinTradingViewPresenter.java  |
| https://ajaib.onelink.me/DXmL/  | sen/com/stock/pages/stockDetailV2/StockDetailActivity.java  |
| https://webview.ajaib.cloud/stock/tradelimit/usp  | sen/com/stock/pages/stockTradingLimitUSP/StockTradingLimitUSPActivity.java  |
| https://webview.ajaib.cloud/tnc/eipo  | sen/com/stock/pages/stockEIPOTermCondition/StockEIPOTermConditionActivity.java  |
| https://chart-v2.ajaib.co.id/  | sen/com/common/customView/webChartV2/WebChartV2ViewModel.java  |
| https://wa.me/62818918200  | uh/d.java  |
| https://webview-stg.ajaib.tech/stock/first-transaction  | wa0/j.java  |
| https://firebase.google.com/support/privacy/init-options.  | w8/c.java  |
| https://referral.kripto.ajaib.co.id  | bl0/e.java  |
| https://kripto.ajaib.co.id/sign-up/?referral-code=  | bl0/e.java  |
| https://webview.ajaib.cloud/tnc/coin-referral  | bl0/b.java  |
| https://ajaib.co.id/program-referral-ajaib-undang-teman-dapat-reksa-dana-gratis/  | bl0/b.java  |
| https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings  | ck0/a.java  |
| https://firebase.google.com/docs/crashlytics/get-started?platform=android  | ck0/a.java  |
| https://webview.ajaib.cloud/tnc/kyc  | fk0/c.java  |
| https://webview.ajaib.cloud/tnc/kyc  | gk0/c.java  |
| https://ajaib.co.id/program-referral-ajaib-undang-teman-dapat-reksa-dana-gratis/  | gl0/a.java  |
| https://form.typeform.com/to/W4eJ26vW  | i0/h.java  |
| https://accounts.google.com/o/oauth2/revoke?token=  | j6/d.java  |
| https://img.youtube.com/vi/  | kr0/b.java  |
| https://webview.ajaib.cloud/tnc/kyc  | lk0/a.java  |
| https://form.typeform.com/to/yMFG25f5  | ls0/a.java  |
| https://webview.ajaib.cloud/tnc  | s60/b.java  |
| https://www.tradingview.com/chart/?symbol=COMPOSITE-INDEX  | sm0/a.java  |
| https://webview.ajaib.cloud/coin/analysis/  | t/d.java  |
| https://ajaib.co.id/ajaib-fast-trade/  | tv0/c.java  |
| https://webview.ajaib.cloud/tnc/update-bank-account  | tv/a.java  |
| https://webview.ajaib.cloud/tnc/qris  | v0/f.java  |
| https://webview.ajaib.cloud/tnc/bca  | v0/f.java  |
| https://webview.ajaib.cloud/tnc/permata  | v0/f.java  |
| https://webview.ajaib.cloud/tnc/mutual-fund  | v0/f.java  |
| https://webview.ajaib.cloud/tnc/stock  | v0/f.java  |
| https://webview.ajaib.cloud/tnc/coin-blue  | v0/f.java  |
| https://webview.ajaib.cloud/tnc/privacy-policy  | v0/f.java  |
| https://webview.ajaib.cloud/tnc/ajaib  | v0/f.java  |
| https://tradingview.ajaib.co.id/?ticker=  | v01/a.java  |
| https://ajaib.co.id/cara-kerja-kode-referral-ajaib/  | vk0/b.java  |
| https://ajaib.co.id/program-referral-ajaib-undang-teman-dapat-reksa-dana-gratis/  | vk0/b.java  |
| https://ajaib.co.id/daftar-saham-regular-untuk-day-trading/  | xx/a.java  |
| https://coinmarketcap.com/alexandria/article/luna-off-to-a-bad-start-after-re-launch-dumps-75  | nt/a.java  |
| https://academy-public.coinmarketcap.com/optimized-uploads/a1b35a5ebcf64d4dadf43607f4902d43.jpeg  | nt/a.java  |
| https://coinmarketcap.com/alexandria/article/luna-off-to-a-bad-start-after-re-launch-dumps-75,  | nt/a.java  |
| https://academy-public.coinmarketcap.com/optimized-uploads/a1b35a5ebcf64d4dadf43607f4902d43.jpeg,  | nt/a.java  |
| https://ajaib.co.id/ais/  | yd/f.java  |
| https://login.ajaib.co.id/sign-up/?referral-code=  | i8/d.java  |
| https://referral.ajaib.co.id  | i8/d.java  |
| https://www.instagram.com/ajaib\_investasi/  | pl0/a.java  |
| https://x.com/ajaib\_investasi  | pl0/a.java  |
| https://www.tiktok.com/@ajaibinvestasi  | pl0/a.java  |
| https://www.youtube.com/@ajaib.investasi  | pl0/a.java  |
| https://webview.ajaib.cloud/faq/detail?topic=25&title=Transaksi%20Otomatis%20Reksa%20Dana  | ez/f.java  |
| https://webview.ajaib.cloud/tnc/coin-permata  | kw/b.java  |
| https://webview.ajaib.cloud/tnc/coin-bca  | kw/b.java  |
| https://webview.ajaib.cloud/tnc/kyc  | kw/b.java  |
| https://webview.ajaib.cloud/tnc/kyc-bca  | kw/b.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| support@embrace.io  | io/embrace/android/embracesdk/EmbraceAutomaticVerification.java  |
| support@embrace.io  | io/embrace/android/embracesdk/ndk/EmbraceNdkService.java  |
| automated@embrace.io  | io/embrace/android/embracesdk/samples/VerificationActions.java  |
| support@ajaib.co  | uh/d.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15552000000  | g7/n4.java  |
| 15778476000  | org/joda/time/chrono/GregorianChronology.java  |
| 15778800000  | org/joda/time/chrono/JulianChronology.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=aj, ST=ajaib, L=ajaib, O=ajaib, OU=ajaib, CN=ajaib 签名算法: rsassa\_pkcs1v15 有效期自: 2018-12-05 05:31:43+00:00 有效期至: 2046-04-22 05:31:43+00:00 发行人: C=aj, ST=ajaib, L=ajaib, O=ajaib, OU=ajaib, CN=ajaib 序列号: 0x3b3612c7 哈希算法: sha256 md5值: 72ad7d2f3f4fee891e5e493b3d5a39f6 sha1值: 924ce9ab70453711a1221d8f2b6c8aac49ec9e32 sha256值: 5311addbc93b6ae0bda84ae449208e8b82ed2acc27476b428ce2dbe82e521e4d sha512值: 39ae2ddb39ff22788c3a87dc2f3462980f3f778aba60009257c1d18a1630081bed3a339c3063428aec9d0a51f1c5269621aa02ac6363de031f4bab66897f0c52 公钥算法: rsa 密钥长度: 2048 指纹: 9c48f4eb588f405f53dac08bf61b0c94bb9d5c0bcb1b2fd8317558d8f2e1fa10**

## **6. 硬编码敏感信息**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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\_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.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.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.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\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 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 |
| 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.ACCESS\_ADSERVICES\_ATTRIBUTION | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| 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 |
| 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 |
| 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。 |
| ajaib.co.id.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.vending.CHECK\_LICENSE | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.providers.gsf.permission.READ\_GSERVICES | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| ajaib.co.id.pages.splash.ToSplashActivity | **Schemes**: https://, **Hosts:** @string/ONE\_LINK\_HOST, @string/INVEST\_LINK\_HOST, @string/GURU\_LINK\_HOST, @string/THEME\_LINK\_HOST, **Path Prefixes:** /SgM5, /q7hl, /HgMe, /adFJ, /mzJ0, /E9kG, /49PH, /3yT0, /SXXS, /Zo5R, /uM66, /KyEB, /eOCw, /aufj, /saham, /bond-list, /DXmL, /Dw86, /ZYuX, /7hOo, /mVFa, /pAfZ, /J8ZM, /78A1, /0esb, /AK7E, /BJfU, /gV4S, /YvdC, /7849, /2AJb, /uBMN, /dR5G, /yKiu, /T5YT, /thKq, /zi6m, /qXXf, /Zoup, /ASrN, /BTNe, /HOOa, /XDUD, /Ju2Q, /xRkr, /woZY, /cMx1, /2hGP, /k9YZ, /0c71, /ohZN, /wL6z, /gaxa, /b3Jm, /kvnr, /0mti, /WcrM, /w9Es, /Vo8r, /dOF8, /p7TH, /LTKV, /7ei6, /N3K1, /HxKr, /azjr, /Ybnz, /BQXo, /e9rp, /mox3, /dkrN, /yPYF, /ydBZ, /cmDI,  |

**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。**