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

**Pi Pay（ 2.5.5.0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 | Pi Pay |
| 版本 | 2.5.5.0 |
| 包名 | com.pipay.app.android |
| 域名线索 | 45条 |
| URL线索 | 100条 |
| APP图标 |  |
| 分析日期 | 2025年6月16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 | pipay-v2.5.5.apk |
| 文件大小 | 36.28MB |
| MD5值 | 07f0a626cd1649a769f6e375ca6a1656 |
| SHA1值 | 184af937110e57a66619e46ddbed35caf9245e3e |
| SHA256值 | 115dd1faafb2698cc8eb49c984935c00d2ec61d91fe5f3d81b5d9577f54d64f1 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Pi Pay |
| 包名 | com.pipay.app.android |
| 主活动Activity | com.pipay.app.android.SplashActivity |
| 安卓版本名称 | 2.5.5.0 |
| 安卓版本 | 75000 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| osu-alpha.appspot.com | IP: 108.160.162.109  所属国家: United States of America  地区: California  城市: San Francisco |
| digicash-uat.pipay.com | IP: 104.22.40.166  所属国家: United States of America  地区: California  城市: San Francisco |
| chat.pipay.com | IP: 104.22.41.166  所属国家: United States of America  地区: California  城市: San Francisco |
| www.mobitexter.net | IP: 198.177.120.25  所属国家: United States of America  地区: Georgia  城市: Atlanta |
| apps.applozic.com | 没有服务器地理信息. |
| s3-ap-southeast-1.amazonaws.com | IP: 199.59.150.13  所属国家: United States of America  地区: California  城市: San Francisco |
| piruin.me | 没有服务器地理信息. |
| links.pipay.com | IP: 104.22.40.166  所属国家: United States of America  地区: California  城市: San Francisco |
| pipay-static-content.s3-ap-southeast-1.amazonaws.com | IP: 31.13.95.33  所属国家: Ireland  地区: Dublin  城市: Dublin |
| play.google.com | IP: 93.46.8.90  所属国家: Italy  地区: Lombardia  城市: Milan |
| static.wizrocket.com | IP: 3.165.39.127  所属国家: United States of America  地区: Washington  城市: Seattle |
| pi-pay-v2.firebaseio.com | IP: 34.120.206.254  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| pddstudio.com | IP: 46.30.213.75  所属国家: Denmark  地区: Hovedstaden  城市: Copenhagen |
| www.tensorflow.org | IP: 172.217.14.206  所属国家: United States of America  地区: California  城市: Mountain View |
| digicash-sit.pipay.com | 没有服务器地理信息. |
| lottery-test.pipay.com | IP: 104.22.40.166  所属国家: United States of America  地区: California  城市: San Francisco |
| pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com | IP: 69.162.134.178  所属国家: United States of America  地区: Illinois  城市: Chicago |
| applozic.appspot.com | IP: 103.252.115.221  所属国家: Singapore  地区: Singapore  城市: Singapore |
| 43.230.193.188 | IP: 43.230.193.188  所属国家: Cambodia  地区: Phnom Penh  城市: Phnom Penh |
| api.kommunicate.io | IP: 23.21.236.132  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| api-test.kommunicate.io | IP: 54.210.101.164  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| www.londatiga.net | IP: 103.93.130.55  所属国家: Indonesia  地区: Jakarta Raya  城市: Jakarta |
| bit.ly | IP: 67.199.248.11  所属国家: United States of America  地区: New York  城市: New York City |
| api.ws.prepay.simfonie.gfggroup.com | IP: 13.248.169.48  所属国家: United States of America  地区: Washington  城市: Seattle |
| maps.googleapis.com | IP: 142.251.33.106  所属国家: Canada  地区: Ontario  城市: Toronto |
| digicash.pipay.com | IP: 104.22.40.166  所属国家: United States of America  地区: California  城市: San Francisco |
| agg.pipay.com | IP: 104.22.41.166  所属国家: United States of America  地区: California  城市: San Francisco |
| ws.simfonie.gfggroup.com | IP: 13.248.169.48  所属国家: United States of America  地区: Washington  城市: Seattle |
| auth-uat.pipay.com | IP: 104.22.40.166  所属国家: United States of America  地区: California  城市: San Francisco |
| o460956.ingest.sentry.io | IP: 34.120.195.249  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| www.instagram.com | IP: 128.121.146.228  所属国家: United States of America  地区: California  城市: Sacramento |
| ws.mpayment.simfonie.gfggroup.com | IP: 13.248.169.48  所属国家: United States of America  地区: Washington  城市: Seattle |
| web.facebook.com | IP: 168.143.162.42  所属国家: United States of America  地区: Washington  城市: Redmond |
| instagram.com | IP: 108.160.161.83  所属国家: United States of America  地区: California  城市: San Francisco |
| maps.google.com | IP: 172.217.14.238  所属国家: United States of America  地区: California  城市: Mountain View |
| plus.codes | IP: 216.239.34.21  所属国家: United States of America  地区: California  城市: Mountain View |
| material.io | IP: 216.239.34.21  所属国家: United States of America  地区: California  城市: Mountain View |
| facebook.com | IP: 66.220.146.94  所属国家: United States of America  地区: California  城市: Menlo Park |
| 10.1.40.161 | IP: 10.1.40.161  所属国家: -  地区: -  城市: - |
| services-prod.pipay.com | IP: 172.67.43.73  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 |
| schemas.android.com | 没有服务器地理信息. |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| bakong-pg-prod.pipay.com | IP: 104.22.40.166  所属国家: United States of America  地区: California  城市: San Francisco |
| schemas.xmlsoap.org | IP: 13.107.246.73  所属国家: United States of America  地区: Washington  城市: Redmond |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://material.io/design/components/dialogs.html | com/afollestad/materialdialogs/MaterialDialog.java |
| https://github.com/airbnb/epoxy/wiki/Avoiding-Memory-Leaks | com/airbnb/epoxy/EpoxyController.java |
| http://maps.google.com/?q= | com/applozic/mobicomkit/uiwidgets/conversation/fragment/ConversationFragment.java |
| http://maps.google.com/maps?q= | com/applozic/mobicomkit/uiwidgets/conversation/adapter/DetailedConversationAdapter.java |
| https://osu-alpha.appspot.com | com/applozic/mobicomkit/api/MobiComKitServer.java |
| https://apps.applozic.com | com/applozic/mobicomkit/api/MobiComKitServer.java |
| https://osu-alpha.appspot.com/rest/ws/error/submit | com/applozic/mobicomkit/api/MobiComKitServer.java |
| https://api.kommunicate.io | com/applozic/mobicomkit/api/MobiComKitClientService.java |
| https://api-test.kommunicate.io | com/applozic/mobicomkit/api/MobiComKitClientService.java |
| https://applozic.appspot.com | com/applozic/mobicomkit/api/MobiComKitClientService.java |
| https://maps.googleapis.com/maps/api/staticmap?center= | com/applozic/mobicommons/commons/core/utils/LocationUtils.java |
| http://static.wizrocket.com/android/ico/ | com/clevertap/android/sdk/Constants.java |
| http://static.wizrocket.com/android/ico// | com/clevertap/android/sdk/Utils.java |
| https://agg.pipay.com:8443/aggregator-2/ | com/pipay/app/android/BuildConfig.java |
| https://auth-uat.pipay.com/pi/ | com/pipay/app/android/BuildConfig.java |
| https://bakong-pg-prod.pipay.com/pipay-bakong/ | com/pipay/app/android/BuildConfig.java |
| https://services-prod.pipay.com/ | com/pipay/app/android/BuildConfig.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/BuildConfig.java |
| https://links.pipay.com/ | com/pipay/app/android/BuildConfig.java |
| https://pipay-static-content.s3-ap-southeast-1.amazonaws.com/PROD/ | com/pipay/app/android/BuildConfig.java |
| https://chat.pipay.com | com/pipay/app/android/BuildConfig.java |
| https://b3529e4eff1a4c7bb912252423577aa8@o460956.ingest.sentry.io/5503942 | com/pipay/app/android/BuildConfig.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/api/data/response/MerchantProfile.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/api/model/account/Customer.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/api/model/smallBusinessOwner/GetBusinessProfileResponse.java |
| https://web.facebook.com/ | com/pipay/app/android/common/AppConstants.java |
| https://www.instagram.com/ | com/pipay/app/android/common/AppConstants.java |
| https://bit.ly/2Jw3lFf | com/pipay/app/android/common/AppConstants.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/common/AppConstants.java |
| https://s3-ap-southeast-1.amazonaws.com/pipay-sit-webapp-pb/static-content-pipay/pinkpackets.png | com/pipay/app/android/common/AppConstants.java |
| http://bit.ly/pi-pay | com/pipay/app/android/common/AppConstants.java |
| https://pipay-static-content.s3-ap-southeast-1.amazonaws.com/PROD/ | com/pipay/app/android/common/AppConstants.java |
| https://services-prod.pipay.com/sym/rs/pipay/ | com/pipay/app/android/common/AppConstants.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/common/IconsResolver.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/common/Utils.java |
| https://play.google.com/store/apps/details?id= | com/pipay/app/android/common/pkg/PackageCommon.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/deals/DealDetailsActivity.java |
| https://maps.googleapis.com/maps/api/staticmap?zoom=16&size=600x300&maptype=roadmap&markers= | com/pipay/app/android/ui/activity/deals/PlaceDetailsActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/deals/PlaceDetailsActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/qr/QrAmountEnterActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/topUp/SelectAmountActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/chat/GroupFriendListActivity.java |
| https://maps.googleapis.com/maps/api/staticmap?zoom=16&size=600x300&maptype=roadmap&markers= | com/pipay/app/android/ui/activity/chat/ConversationAdapter.java |
| http://maps.google.com/maps?q=loc: | com/pipay/app/android/ui/activity/chat/ConversationAdapter.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/receive/ReceiveInitialQrActivity.java |
| https://pipay-static-content.s3-ap-southeast-1.amazonaws.com/PROD/ | com/pipay/app/android/ui/activity/me/PoliciesActivity.java |
| http://plus.codes/7P36HW65+4V | com/pipay/app/android/ui/activity/me/ContactInfoData.java |
| https://facebook.com/ | com/pipay/app/android/ui/activity/me/ContactInfoData.java |
| https://instagram.com/ | com/pipay/app/android/ui/activity/me/ContactInfoData.java |
| https://maps.googleapis.com/maps/api/staticmap?zoom=16&size=600x300&maptype=roadmap&markers=11.560260,104.909661&key=AIzaSyCNGpaXA21bqeJPkOQShE7qcqggvNjssaA | com/pipay/app/android/ui/activity/me/ContactUsActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/externalCatalog/ExternalCatalogueActivity.java |
| https://pipay-static-content.s3-ap-southeast-1.amazonaws.com/PROD/ | com/pipay/app/android/ui/activity/joyRide/joyRideReceive/JoyRideReceiveTermsConditionActivity.java |
| https://pipay-static-content.s3-ap-southeast-1.amazonaws.com/PROD/ | com/pipay/app/android/ui/activity/wallet/UpdateWalletReviewActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/home/MainExpCardFragment.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/coupon/CouponClaimSelectWalletActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/coupon/ClaimedCouponDetailsActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/coupon/detail/CouponDetailsActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/biller/PayBillerSuccessActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/biller/PayBillerActivity.java |
| https://pipay-static-content.s3-ap-southeast-1.amazonaws.com/PROD/ | com/pipay/app/android/ui/activity/quickPay/QuickPayTermsConditionsActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/quickPay/QuickPayQrActivity.java |
| https://pipay-static-content.s3-ap-southeast-1.amazonaws.com/PROD/ | com/pipay/app/android/ui/activity/account/RegisterMobileNumberActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/friends/FriendListActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/friends/FriendFragment.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/friends/ChatFragment.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/documents/customers/ | com/pipay/app/android/ui/activity/friends/addFriend/AddFriendResultActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/friends/addFriend/addFriendByQR/AddFriendQrConfirm.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/friends/groupChat/InitChatActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/friends/groupChat/CreateChatGroupActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/transfer/TransferP2PEnterAmountSuccessActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/transfer/TransferP2PEnterAmountActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/transfer/TransferFriendListActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/pinkPacket/PinkPackToFriendListActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/activity/pinkPacket/PinkPackSuccessActivity.java |
| http://lottery-test.pipay.com/lotteryhome/%1$s/kh | com/pipay/app/android/ui/master/ExternalCatalogUrl.java |
| https://play.google.com/store/apps/details?id= | com/pipay/app/android/ui/master/LoadAction.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/adapter/ImgViewPagerAdapter.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/adapter/AdapterSetRowData.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/adapter/BillerAdapter.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/adapter/DealAdapter.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/adapter/SubExpCardAdapter.java |
| https://play.google.com/store/apps/details?id=com.pipay.app.android | com/pipay/app/android/ui/alert/ForceUpgradeActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/ui/viewholder/BannerViewHolder.java |
| http://schemas.android.com/apk/res/android | com/pipay/app/android/v3/common/PiPayV3OtpView.java |
| https://pipay-static-content.s3-ap-southeast-1.amazonaws.com/PROD/ | com/pipay/app/android/v3/module/payment/international/AlipayTransferActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/v3/module/payment/international/model/InternationalRemittancePartner.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/v3/module/payment/transfer/P2PTransferActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/v3/module/payment/ptu/PhoneTopUpActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/v3/module/payment/qr/QrPaymentActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/v3/module/setting/LinkAccountStatusActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/v3/module/setting/LinkAccountKeyActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/v3/module/setting/LinkAccountAppsActivity.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/v3/module/wallet/CouponListAdapter.java |
| https://auth-uat.pipay.com/pi/authorization?response\_type=code&client\_id=pipaymobileapp&state=active&scope=credential&msisdn= | com/pipay/app/android/v3/module/auth/AuthServerLoginActivity.java |
| https://pipay-static-content.s3-ap-southeast-1.amazonaws.com/PROD/ | com/pipay/app/android/activity/applink/AppLinkIntents.java |
| https://play.google.com/store/apps/details?id= | com/pipay/app/android/activity/browser/linkhandler/InstalledAppLinkHandler.java |
| https://s3-ap-southeast-1.amazonaws.com/pipayprodpublic/ | com/pipay/app/android/adapter/CouponsListAdapter.java |
| http://schemas.android.com/apk/res/android | com/hbb20/CountryCodePicker.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/Observable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Flowable.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 |
| http://api.ws.prepay.simfonie.gfggroup.com/ | wirecard/com/api/SimfonieBillPayments.java |
| http://api.ws.prepay.simfonie.gfggroup.com/ | wirecard/com/api/SimfonieAccountActions.java |
| http://api.ws.prepay.simfonie.gfggroup.com/ | wirecard/com/api/wallet/SimfonieFinancialWalletTransfers.java |
| http://ws.simfonie.gfggroup.com/ | wirecard/com/api/wallet/SimfonieTransferSubscriberWallet.java |
| http://api.ws.prepay.simfonie.gfggroup.com/ | wirecard/com/api/wallet/SimfonieTransferSubscriberWallet.java |
| https://digicash.pipay.com | wirecard/com/simfonie/network/SimfonieBase.java |
| http://43.230.193.188:8181 | wirecard/com/simfonie/network/SimfonieBase.java |
| https://digicash-uat.pipay.com | wirecard/com/simfonie/network/SimfonieBase.java |
| http://10.1.40.161:8080 | wirecard/com/simfonie/network/SimfonieBase.java |
| https://digicash-sit.pipay.com | wirecard/com/simfonie/network/SimfonieBase.java |
| http://schemas.xmlsoap.org/soap/envelope/ | wirecard/com/simfonie/network/soap/generators/SoapEnvelopeGenerator.java |
| http://ws.mpayment.simfonie.gfggroup.com/ | wirecard/com/simfonie/network/soap/generators/SoapEnvelopeGenerator.java |
| http://api.ws.prepay.simfonie.gfggroup.com/ | wirecard/com/network/request/account/TransactionsHistoryRequest.java |
| http://ws.simfonie.gfggroup.com/ | wirecard/com/network/request/account/Registration.java |
| http://api.ws.prepay.simfonie.gfggroup.com/ | wirecard/com/network/request/account/ChangePinCode.java |
| http://ws.simfonie.gfggroup.com/ | wirecard/com/network/request/topup/TopUpOwnAirtimeSubs.java |
| http://api.ws.prepay.simfonie.gfggroup.com/ | wirecard/com/network/request/payment/PayBillAccountCompletionRequest.java |
| http://api.ws.prepay.simfonie.gfggroup.com/ | wirecard/com/network/request/transfer/FinancialToFinancialExchangeRateRequest.java |
| https://pi-pay-v2.firebaseio.com | 摸瓜V1引擎 |
| http://pddstudio.com/ | 摸瓜V1引擎 |
| https://github.com/PDDStudio/EncryptedPreferences | 摸瓜V1引擎 |
| https://piruin.me | 摸瓜V1引擎 |
| http://www.londatiga.net/ | 摸瓜V1引擎 |
| https://piruin.me/quickaction | 摸瓜V1引擎 |
| https://github.com/piruin/quickaction | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_button\_en.webp | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_ride\_en.webp | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_need\_ride\_en.webp | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_logo.webp | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_map.webp | 摸瓜V1引擎 |
| http://www.mobitexter.net/ | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_button\_jp.webp | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_ride\_jp.webp | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_need\_ride\_jp.webp | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_button\_km.webp | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_ride\_km.webp | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_need\_ride\_km.webp | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_button\_zh.webp | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_ride\_zh.webp | 摸瓜V1引擎 |
| https://pipay-uat-webapp-pb.s3-ap-southeast-1.amazonaws.com/images/tada/icons/ic\_tada\_need\_ride\_zh.webp | 摸瓜V1引擎 |
| https://www.tensorflow.org/lite/guide/ops\_select | lib/arm64-v8a/libbarhopper\_v3.so |
| http://http | lib/arm64-v8a/libbarhopper\_v3.so |
| https://www.tensorflow.org/lite/guide/ops\_custom | lib/arm64-v8a/libbarhopper\_v3.so |
| https://www.tensorflow.org/lite/guide/ops\_select | lib/armeabi-v7a/libbarhopper\_v3.so |
| http://http | lib/armeabi-v7a/libbarhopper\_v3.so |
| https://www.tensorflow.org/lite/guide/ops\_custom | lib/armeabi-v7a/libbarhopper\_v3.so |
| https://www.tensorflow.org/lite/guide/ops\_select | lib/x86/libbarhopper\_v3.so |
| http://http | lib/x86/libbarhopper\_v3.so |
| https://www.tensorflow.org/lite/guide/ops\_custom | lib/x86/libbarhopper\_v3.so |
| https://www.tensorflow.org/lite/guide/ops\_select | lib/x86\_64/libbarhopper\_v3.so |
| http://http | lib/x86\_64/libbarhopper\_v3.so |
| https://www.tensorflow.org/lite/guide/ops\_custom | lib/x86\_64/libbarhopper\_v3.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| support@applozic.com | com/applozic/mobicommons/ALSpecificSettings.java |
| 4c7bb912252423577aa8@o460956.ingest | com/pipay/app/android/BuildConfig.java |
| dara.p@pipay.com | com/pipay/app/android/common/Credentials.java |
| tobe@update.com | com/pipay/app/android/common/Utils.java |
| support@mobitexter.net | 摸瓜V1引擎 |
| android-sdk-releaser@vopo7.prod | lib/arm64-v8a/libbarhopper\_v3.so |
| android-sdk-releaser@vopo7.prod | lib/armeabi-v7a/libbarhopper\_v3.so |
| android-sdk-releaser@vopo7.prod | lib/x86/libbarhopper\_v3.so |
| android-sdk-releaser@vopo7.prod | lib/x86\_64/libbarhopper\_v3.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13721473389 | com/pipay/app/android/v3/module/payment/international/AlipayTransferActivity.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=KH, ST=NA, L=Phnom Penh, O=Pi Pay Co., Ltd, OU=IT, CN=Chenda Nhean 签名算法: rsassa\_pkcs1v15 有效期自: 2017-01-28 06:41:32+00:00 有效期至: 2044-06-15 06:41:32+00:00 发行人: C=KH, ST=NA, L=Phnom Penh, O=Pi Pay Co., Ltd, OU=IT, CN=Chenda Nhean 序列号: 0x3223da53 哈希算法: sha256 md5值: fead56c022a5d95c3519cb4d6dd48dde sha1值: 9da6cd9bbece7ec6aa31fe1e5e1a5155379cdba0 sha256值: bf2f2e384a3b252e6652040da384298e865f49dd3e6520f8198106f15c3cff5a sha512值: 1be5a8fcb9d86edb1c888b36a004953fd719794012f61061d1099d19a4c65651f9b5df60948ef5ce1aad9d35e5aed923a7955cd542001fe53464a9bd23dff03b 公钥算法: rsa 密钥长度: 2048 指纹: 1b30378a5f74a29d96764f61455bca88b7955040fdea33f9c0ee57af47575523**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "adding\_channel\_user" : "Adding…" |
| "deleting\_channel\_user" : "Deleting…" |
| "delivery\_report\_pref\_key" : "DELIVERY\_REPORT\_ENABLE" |
| "dialog\_add\_group\_user" : "Add [name] to [group]?" |
| "dialog\_remove\_group\_user" : "Remove [name] from [group]?" |
| "firebase\_database\_url" : "https://pi-pay-v2.firebaseio.com" |
| "google\_api\_key" : "AIzaSyALpauwfaPUF2BXqixa5-fXowijiv9BSSY" |
| "google\_crash\_reporting\_api\_key" : "AIzaSyALpauwfaPUF2BXqixa5-fXowijiv9BSSY" |
| "group\_sms\_freq\_key" : "GROUP\_SMS\_FREQ\_KEY" |
| "key" : "Key" |
| "library\_EncryptedPreferences\_author" : "Patrick J" |
| "library\_EncryptedPreferences\_authorWebsite" : "http://pddstudio.com/" |
| "phone\_number\_key" : "phone\_number\_key" |
| "received\_sms\_sync\_pref\_key" : "RECEIVED\_SMS\_SYNC\_FLAG" |
| "removing\_channel\_user" : "Removing…" |
| "sent\_sms\_sync\_pref\_key" : "SENT\_SMS\_SYNC\_FLAG" |
| "str\_reg\_session\_time\_head" : "Session timed out" |
| "str\_reg\_session\_time\_msg" : "Your session has timed out. Please sign in again." |
| "str\_session\_time\_out" : "Your session has timed out. Please sign in again." |
| "user\_name" : "User Name" |
| "webhook\_enable\_key" : "WEBHOOK\_ENABLE\_KEY" |
| "adding\_channel\_user" : "जोड़ा जा रहा है ...." |
| "deleting\_channel\_user" : "हटा रहा है ..." |
| "dialog\_add\_group\_user" : "[नाम] को [समूह] में जोड़ें?" |
| "dialog\_remove\_group\_user" : "[समूह] से [नाम] निकालें?" |
| "removing\_channel\_user" : "निकाला जा रहा है" |
| "user\_name" : "User Name" |
| "key" : "Key" |
| "key" : "Key" |

## **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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| 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.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.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.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| com.pipay.app.android.permission.MAPS\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.pipay.app.android.activity.applink.AppLinkActivity | **Schemes**: pipay://, |

**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。**