MoGua

SimBanking 12.APK 分析报告

APP名称: SimBanking

包名:	apps.crdbbank.com.mobapp
域名线索:	17条
URL线索:	20条
邮箱线索:	2条
分析日期:	2025年1月9日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: apps-crdbbank-com-mobapp-158-64936343-73cbd1544728ad9b4758e616635eb0e0.apk
文件大小: 41.15MB
MD5值: 73cbd1544728ad9b4758e616635eb0e0
SHA1值: ff203392905a34aaa629f3f5ee2ad40ab7e2e47a
SHA256值: cf75781e17b3564291135651796933 3dd0c2320266ac67bde83308f4c866014c

APP 信息

App名称: SimBanking
包名: apps.crdbbank.com.mobapp
主活动Activity: com.crdbbank.simbanking.ui.splash.activity.SplashActivity
安卓版本名称: 12
安卓版本: 158

域名线索

域名	服务器信息
developer.android.com	**IP**: 172.217.14.206 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
m.facebook.com	**IP**: 104.244.46.246 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
schemas.android.com	没有服务器地理信息.
	IP: 142.251.215.238

play.google.com	**所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
escrowagm.com	IP: 154.120.235.206 **所属国家**: Zimbabwe **地区**: Bulawayo **城市**: Bulawayo **纬度**: -20.150000 **经度**: 28.583330
simbanking.crdbbank.co.tz	IP: 102.217.211.67 **所属国家**: Tanzania, United Republic of **地区**: Dar es Salaam **城市**: Dar es Salaam **纬度**: -6.823193 **经度**: 39.270412
xml.apache.org	IP: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
accounts.google.com	IP: 93.46.8.90 **所属国家**: Italy **地区**: Lombardia **城市**: Milan **纬度**: 45.464336 **经度**: 9.188547
crdbbank.co.tz	IP: 104.26.10.184 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

ns.adobe.com	没有服务器地理信息.
licensemgr.identy.io	**IP**: 3.130.131.2 **所属国家**: United States of America **地区**: Ohio **城市**: Columbus **纬度**: 39.961380 **经度**: -82.997749
twitter.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
plus.google.com	**IP**: 98.159.108.61 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052986 **经度**: -118.263687
www.youtube.com	**IP**: 142.250.217.110 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
java.sun.com	**IP**: 104.126.37.129 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996
simbanking.crdbbank.com	没有服务器地理信息.

instagram.com	**IP**: 114.43.24.59 **所属国家**: Taiwan (Province of China) **地区**: Taipei **城市**: Taipei **纬度**: 25.038172 **经度**: 121.563599

URL线索

URL**信息**	Url**所在文件**
https://licensemgr.identy.io/getMobileModel/v1	com/identy/LManager.java
http://java.sun.com/javase/downloads/index.jsp)	com/identy/support/encryption/AESCrypt.java
https://simbanking.crdbbank.co.tz	com/crdbbank/simbanking/core/models/UserData.java
https://simbanking.crdbbank.co.tz/api/service	com/crdbbank/simbanking/core/network/cards/CardServices.java
https://simbanking.crdbbank.co.tz/api/service	com/crdbbank/simbanking/core/network/qr/QrServices.java
https://simbanking.crdbbank.co.tz/api/parser	com/crdbbank/simbanking/core/network/qr/QrServices.java
https://play.google.com/store/apps/details?id=	com/crdbbank/simbanking/ui/splash/activity/SplashActivity.java
http://schemas.android.com/apk/res/android	o/getDecoratedHint.java
http://ns.adobe.com/xap/1.0/\u0000	o/setUseCompatPadding.java
https://plus.google.com/	o/lambda$handleLukuRetrieval$20$BillPaymentsFragment.java
https://developer.android.com/reference/com/google/android/play/core/install/model/InstallErrorCode	o/TvPaymentsFragment$$ExternalSyntheticLambda2.java

http://xml.apache.org/xslt	o/BottomSheetConfirmationSkip.java
http://schemas.android.com/apk/res/android	o/lambda$getServices$35.java
http://schemas.android.com/apk/res-auto	o/lambda$getServices$35.java
https://accounts.google.com/o/oauth2/revoke?token=	o/setShadowRadius.java
https://crdbbank.co.tz/en/forms-and-guides	o/QrServices$$ExternalSyntheticLambda1.java
https://instagram.com/crdbbankplc?igshid=1p0aud27tom9x	o/getSelectedPosition.java
https://www.youtube.com/channel/UC1ymNdbXSXL5CjE4n-qf1rA	o/getSelectedPosition.java
https://twitter.com/crdbbankplc?s=11	o/getSelectedPosition.java
https://m.facebook.com/crdbbank	o/getSelectedPosition.java
https://crdbbank.co.tz/	o/getSelectedPosition.java
https://crdbbank.co.tz/wp-content/uploads/2018/02/General-Terms-and-Condition.pdf	o/getIsBlur.java
https://crdbbank.co.tz/salary-advance-loan/	o/setUtilityLukuAmount.java
https://crdbbank.co.tz/boom-advance-loan/	o/setUtilityLukuAmount.java
https://crdbbank.co.tz/	o/setUtilityLukuAmount.java
https://escrowagm.com/crdb/signup.aspx	o/getEmailAddress.java
https://escrowagm.com/crdb/Login.aspx	o/getEmailAddress.java
https://crdbbank.co.tz/fixed-deposit-account/	o/lambda$processCheckPANResponse$35$QrServices.java

https://crdbbank.co.tz/customer-complaints/	o/lambda$processCheckPANResponse$35$QrServices.java
https://simbanking.crdbbank.co.tz/open-account	摸瓜V1引擎
https://simbanking.crdbbank.com/open-account	摸瓜V1引擎

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	o/BillPaymentsFragment$$ExternalSyntheticLambda22.java
someone@example.com customer@mail.com jina@mfano.com	摸瓜V1引擎

手机线索

手机号	所在文件
17179869184	com/identy/ScriptC_Yuv2Rgb.java
17179869184	com/identy/FingerActivity.java
15222222222	com/identy/FingerActivity.java
13222222222	com/identy/FingerActivity.java
17179869184	com/identy/IdentySdk.java

17179869184	com/identy/FingersProcessor.java
17179869184	com/identy/Capture4FActivity.java
17179869184	com/identy/CaptureFingersActivity.java
17179869184	com/identy/Enroll4FActivity.java
17179869184	com/identy/Legacy4FActivity.java
17179869184	com/identy/EnrollFingersActivity.java
17179869184	com/identy/Enroll2TActivity.java
17179869184	com/identy/LegacyFingersActivity.java
17179869184	com/identy/CaptureThumbActivity.java
17179869184	com/identy/EnrollThumbActivity.java
17179869184	com/identy/LegacyThumbActivity.java
17179869184	com/identy/Verify2TActivity.java
17179869184	com/identy/VerifyFingersActivity.java
17179869184	com/identy/VerifyThumbActivity.java
17179869184	com/identy/Verify4FActivity.java
17179869184	com/identy/IntroActivity.java
17179869184	com/identy/support/MainActivity.java

17179869184	com/identy/support/MyApplicationInterface.java
17179869184	com/identy/enums/Template.java
17179869184	com/identy/ui/dialog/FourFFingerDisplay.java
17179869184	com/identy/ui/dialog/TwoThumbFingerDisplay.java
17179869184	com/identy/ui/dialog/ThumbFingerDisplay.java
17179869184	com/crdbbank/simbanking/core/models/TxnObject.java
17179869184	com/crdbbank/simbanking/core/models/accountopening/AppSignatureHelper.java
17179869184	com/crdbbank/simbanking/core/models/accountopening/store/IncomingSmsReader.java
17179869184	com/crdbbank/simbanking/core/models/accountopening/store/AccountOpeningData.java
17179869184	com/crdbbank/simbanking/core/models/accountopening/dynamica/DynaForms.java
17179869184	com/crdbbank/simbanking/core/models/loans/LoanUIObject.java
17179869184	com/crdbbank/simbanking/core/models/loans/LoansData.java
17179869184	com/crdbbank/simbanking/core/models/loans/staffloans/SalaryDetails.java
17179869184	com/crdbbank/simbanking/core/network/ServerConnection.java
17179869184	com/crdbbank/simbanking/core/network/qr/QrServices.java
17179869184	com/crdbbank/simbanking/core/tools/AppTools.java
17179869184	com/crdbbank/simbanking/ui/custom/view/CircularIconButton.java
17179869184	com/crdbbank/simbanking/ui/custom/view/BalanceView.java

17179869184	com/crdbbank/simbanking/ui/main/fragment/services/HospitalPaymentsFragment.java
17179869184	com/crdbbank/simbanking/ui/main/fragment/services/TvPaymentsFragment.java
17179869184	com/crdbbank/simbanking/ui/splash/activity/SplashActivity.java
17179869184	com/esotericsoftware/kryo/io/KryoDataOutput.java
17179869184	com/esotericsoftware/kryo/serializers/OptionalSerializers.java
17179869184	com/esotericsoftware/kryo/serializers/DefaultSerializers.java
17179869184	com/esotericsoftware/kryo/util/IntArray.java
17179869184	com/visa/mvisa/tlvparser/QrCodeData.java
17179869184	o/addPlaceholderTextView.java
17179869184	o/notifyListenerResponseNotUsable.java
17179869184	o/EducationPaymentsFragment$$ExternalSyntheticLambda26.java
17179869184	o/TvPaymentsFragment$$ExternalSyntheticLambda18.java
15222222222	o/TvPaymentsFragment$$ExternalSyntheticLambda18.java
17179869184	o/position.java
17179869184	o/getTransactionDetails.java
17179869184	o/getTabTextColors.java
17179869184	o/lambda$initViews$1$ActivityDiasporaFingerSelection.java

17179869184	o/checkCompletedStatus.java
17179869184	o/setSecondDrawableLabel.java
17179869184	o/lambda$processAccountDetails$29$TvPaymentsFragment.java
17179869184	o/lambda$renderVerifyDetailsScreen$17.java
17179869184	o/completeScroll.java
17179869184	o/getUseMemRegions.java
17179869184	o/TvPaymentsFragment$$ExternalSyntheticLambda36.java
17179869184	o/onOptionsItemSelected.java
17179869184	o/getDocumentTypeId.java
17179869184	o/setWillNotDrawFlag.java
17179869184	o/setMaxInlineActionWidth.java
17179869184	o/OtherPaymentsFragment$$ExternalSyntheticLambda21.java
17179869184	o/clearOnCheckedChangeListeners.java
17179869184	o/setTranslateX.java
17179869184	o/getLeftIndex.java
17179869184	o/CircularButton.java
17179869184	o/getLeftThumbPng.java
17179869184	o/addViewInternal.java

17179869184	o/getGeneralTerms.java
17179869184	o/lambda$initViews$4$AssistedStaffNidaNumber.java
17179869184	o/CurrencyDropDown.java
17179869184	o/lambda$onPostCreate$1$ActivityDiasporaMultipleSelection.java
17179869184	o/assertNotMainThread.java
17179869184	o/initViews.java
17179869184	o/updateDropDown.java
17179869184	o/MethodAccess.java
17179869184	o/drawInactive.java
17179869184	o/getByte.java
17179869184	o/getMenuInflater.java
17179869184	o/Generics.java
17179869184	o/setSelectedTabIndicator.java
17179869184	o/getProductName.java
17179869184	o/setKeyClass.java
17179869184	o/lambda$init$4$AgmDashboardActivity.java
17179869184	o/lambda$getServices$36$OtherPaymentsFragment.java

17179869184	o/QrServices$$ExternalSyntheticLambda50.java
17179869184	o/CustomScroller.java
17179869184	o/ServicesFragment$$ExternalSyntheticLambda3.java
17179869184	o/isRequiredAtm.java
17179869184	o/DefaultArraySerializers.java
17179869184	o/TimeSerializers.java
17179869184	o/AllServicesFragment$$ExternalSyntheticLambda10.java
17179869184	o/setOtpApplicationId.java
17179869184	o/LoanStatus.java
17179869184	o/setEmail.java
17179869184	o/CardServices$$ExternalSyntheticLambda11.java
17179869184	o/setExpiryDateTextColor.java
17179869184	o/QrServices$$ExternalSyntheticLambda48.java
17179869184	o/setLoanMonth.java
17179869184	o/getNotEnrolledFas.java
17179869184	o/getPriceCode.java
17179869184	o/GridLayoutManager.java

17179869184	o/getMaritalValues.java
17179869184	o/lambda$processChangeCardStatusResponse12CardServices.java
17179869184	o/processGetCardsResponse.java
17179869184	o/lambda$initViews$2$AssistedStaffAdditionalInformation.java
17179869184	o/getPreferredLanguage.java
17179869184	o/QrServices$$ExternalSyntheticLambda1.java
17179869184	o/DefaultStreamFactory.java
17179869184	o/addAnimatorUpdateListener.java
17179869184	o/TextInputLayout2.java
17179869184	o/lambda$processCheckPANResponse$32.java
17179869184	o/lambda$processDefaultCardResponse$8.java
17179869184	o/QrServices$$ExternalSyntheticLambda40.java
17179869184	o/getAccount_number.java
17179869184	o/isPlayStorePossiblyUpdating.java
17179869184	o/CardServices$$ExternalSyntheticLambda4.java
17179869184	o/renderLipaNumberScreen.java
17179869184	o/DiasporaIdTypes.java
17179869184	o/Status.java

17179869184	o/getDeviceId.java
17179869184	o/getFeatures.java
17179869184	o/lambda$removeAlias$22$QrServices.java
17179869184	o/startScroll.java
17179869184	o/setEventCategory.java
17179869184	o/lambda$processAccountDetails$13$GovernmentPaymentsFragment.java
17179869184	o/ResponseAccountOpening.java
17179869184	o/isActive.java
17179869184	o/writeShorts.java
17179869184	o/toArray.java
17179869184	o/lambda$processCheckAliasResponse15QrServices.java
17179869184	o/getCountriesCodeList.java
17179869184	o/getRightLittle.java
17179869184	o/getOtpApplicationId.java
17179869184	o/QrServices$$ExternalSyntheticLambda31.java
17179869184	o/setScrollDurationFactor.java
17179869184	o/getWard.java

17179869184	o/isOTPSent.java
17179869184	o/ActivityC0046setOccupation.java
17179869184	o/getLeftRing.java
17179869184	o/setCircleRadius.java
17179869184	o/setHeader.java
17179869184	o/ActivityC0038getPhoneNumber.java
17179869184	o/setResidenceType.java
17179869184	o/LoanUIObject.java
17179869184	o/IdToken.java
17179869184	o/getSelectedCurrencies.java
17179869184	o/setPostalAddress.java
17179869184	o/setDocumentTypeId.java
17179869184	o/setRightIndexPng.java
17179869184	o/setIdentificationNumber.java
17179869184	o/processAddAliasResponse.java
17179869184	o/setItemBackgroundResource.java
17179869184	o/setMaritalValues.java

17179869184	o/getCardsByAccount.java
17179869184	o/QrServices$$ExternalSyntheticLambda4.java
17179869184	o/setLoanFullDate.java
17179869184	o/FahariFloatAccounts.java
17179869184	o/showKeyBoard.java
17179869184	o/setNotEnrolledFas.java
17179869184	o/setTopUps.java
17179869184	o/getElligibility.java
17179869184	o/processHistoryResponse.java
17179869184	o/getField12.java
17179869184	o/QrServices$$ExternalSyntheticLambda37.java
17179869184	o/setLoanStatus.java
17179869184	o/getEmploymentCodes.java
17179869184	o/getRightRingPng.java
17179869184	o/getBIRTHDISTRICT.java
17179869184	o/getLoanId.java
17179869184	o/QrServices$$ExternalSyntheticLambda5.java
17179869184	o/lambda$makeQrPayment$43.java

17179869184	o/ActivityC0040getSignature.java
17179869184	o/lambda$processRegisterAccountResponse5QrServices.java
17179869184	o/AppTools.java
17179869184	o/getIdNumber.java
17179869184	o/getFingerWsq.java
17179869184	o/setSalCodes.java
17179869184	o/getCustomerAccount.java
17179869184	o/getQrCodeData.java
17179869184	o/enableOrDisableHardwareLayer.java
17179869184	o/lambda$initViews$2$AssistedStaffSimBankingRegistration.java
17179869184	o/lambda$init$0$AssistedStaffCustomerDetails.java
17179869184	o/getCardService.java
17179869184	o/AmountTextWatcher.java
17179869184	o/getQrTxnHistory.java
17179869184	o/getEmailAddress.java
17179869184	o/lambda$processCheckPANResponse$35$QrServices.java
17179869184	o/getBasicSalary.java

17179869184	o/setSelectedCard.java
17179869184	o/CardServices$$ExternalSyntheticLambda9.java
17179869184	o/setLeftMiddlePng.java
17179869184	o/lambda$processAddAliasResponse$18.java
17179869184	o/disableExtraScaleModeInFitXY.java
17179869184	org/identy/opencv/core/MatOfDouble.java
17179869184	org/identy/opencv/imgproc/Subdiv2D.java
17179869184	org/tensorflow/demo/env/Logger.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=255, ST=ilala, L=Dar-es-salaam, O=Crdb Bank Plc, OU=ISD, CN=Crdb Team
签名算法: rsassa_pkcs1v15
有效期自: 2015-12-28 16:21:15+00:00
有效期至: 2040-12-21 16:21:15+00:00
发行人: C=255, ST=ilala, L=Dar-es-salaam, O=Crdb Bank Plc, OU=ISD, CN=Crdb Team
序列号: 0x5800e80b
哈希算法: sha256
md5值: 651f8277e1325bfd5305eab235c0eec3
sha1值: 4807671e80919d928a16772f55b920bb4685cb4e
sha256值: 061227a3360b67019965c1dee541f7300bc84f0103a683799dd7dd31a6b99d5d
sha512值: 149c7fb6b99e468dd937b2a23207bd5384afc87755ef312b2915f2ca0ea00bf24904fdbae38baf90bbcecf05ad04ddf651b9aa1a4e757f2c8322e5097a77dfad
公钥算法: rsa

密钥长度: 2048
指纹: 99acd686082e333947bd5bbba88796d17e2eb768b59d6046242e3cb22cbd5e60

硬编码敏感信息

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.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.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.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.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_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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.hardware.camera.autofocus	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.RECORD_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.BATTERY_STATS	合法	修改电池统计信息	允许修改收集的电池统计信息。不供普通应用程序使用
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_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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.crdbbank.simbanking.ui.splash.activity.SplashActivity	Schemes: https://, http://, simbanking://, Hosts: simbanking.crdbbank.co.tz, Path Patterns: /open-account, /download, /loans, /simbanking-visa, /home,

---