MoGua

iDeal 2.5.235.APK 分析报告

APP名称: iDeal

包名:	cn.com.chinamoney.ideal.rmb
域名线索:	0条
URL线索:	0条
邮箱线索:	1条
分析日期:	2024年5月8日
分析平台:	摸瓜反编译平台

文件信息

文件名: iDeal_android_release.apk
文件大小: 98.32MB
MD5值: 564cba46f21311423ab13d5fc568ca7b
SHA1值: 881351ad8e4b1c848a2424f43366ad99a226fff7
SHA256值: ddd97f61b1024c5f6b95e6ce7f6458d8e0bb9deb0500a13c4aa2fa1e6617edcc

APP 信息

App名称: iDeal
包名: cn.com.chinamoney.ideal.rmb
主活动Activity: com.zhonghui.ZHChat.module.splash.SplashActivity
安卓版本名称: 2.5.235
安卓版本: 167

域名线索

URL线索

邮箱线索

邮箱地址	所在文件
cfetsonline@chinamoney.com	Mogua Engine V1

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=86, ST=beijing, L=beijing, O=ronglian, OU=ronglian, CN=rx
签名算法: rsassa_pkcs1v15
有效期自: 2015-11-24 03:18:18+00:00
有效期至: 2040-11-17 03:18:18+00:00
发行人: C=86, ST=beijing, L=beijing, O=ronglian, OU=ronglian, CN=rx
序列号: 0x4360789a
哈希算法: sha256
md5值: 756fee890e1e510a0b46a8b86640366e
sha1值: 802bee30a6c756dcdc892743b3049b68d7da3b72
sha256值: d17addcd5abb1445e9b641f423155d7d2d9631bd5834f83653ff8dffd86f63b4
sha512值: 7f656b7dcf4783505bac8a8704d73ba8ce7af869d7f0bb19460576a6a1c766775655bf84b86904831e2521144d9ad0dfc814a4e840b98ecc5a55f863783e1d5b

🔑 硬编码敏感信息

可能的敏感信息
"Enter_ideal_password" : "请输入iDeal密码"
"Enter_password" : "请输入登录密码"
"Forget_Password" : "忘记密码"
"Forget_iDeal_Password" : "忘记iDeal密码"
"Forget_pwd_hit" : "用于找回iDeal密码，若需找回本币、外汇账号密码请联系交易系统客服"
"Low_pwd_hip" : "您的密码安全等级较低，请重新设置"
"Low_pwd_hip_note" : "说明：密码较简单，需要提升复杂程度"
"Re_enter_password" : "请再次输入iDeal密码*"

"Username" : "用户名"

"enter_fx_password" : "请输入外汇账号密码"

"enter_rmb_password" : "请输入本币账号密码"

"enter_your_password" : "请输入旧iDeal密码"

"ideal_fx_user" : "外汇iDeal用户"

"ideal_idata_user" : "其他用户"

"ideal_rmb_user" : "本币iDeal用户"

"password" : "密码"

"please_agreement_user_private" : "请先同意用户许可协议和隐私协议"

"private_agree" : "已阅读并同意iDeal隐私协议"

"pwd_conPwd_incons" : "两次输入密码不一致，请重新输入"

"remove_user" : "删除用户"

"search_user" : "用户名/机构名"

"str_enter_origin_pwd" : "请输入原密码"

"str_enter_verify_pwd" : "请输入确认密码"

"str_forget_password" : "忘记密码"

"str_modify_pwd" : "修改密码"

"str_modify_pwd_fail" : "密码修改失败，请稍候重试"

"str_origin_pwd" : "原密码"

"str_passport_pwd" : "iDeal密码: %s"

"str_pwd_rule" : "密码必须是8-20位包含数字、字母与特殊符号组合"

"str_reset_pwd_tips" : "请联系iDeal FX中心场务重置密码4009787878-1-1"

"str_secret" : "保密"

"str_username" : "姓名"

"str_verify_pwd" : "确认密码"

"str_verify_pwd_tips" : "新密码格式有误，请重新输入"

"Enter_ideal_password" : "请输入iDeal密码"

"Enter_password" : "请输入登录密码"

"Forget_Password" : "忘记密码"

"Forget_iDeal_Password" : "忘记iDeal密码"

"Forget_pwd_hit" : "用于找回iDeal密码，若需找回本币、外汇账号密码请联系交易系统客服"

"Low_pwd_hip" : "您的密码安全等级较低，请重新设置"

"Low_pwd_hip_note" : "说明：密码较简单，需要提升复杂程度"

"Re_enter_password" : "请再次输入iDeal密码*"

"Username" : "用户名"

"enter_fx_password" : "请输入外汇账号密码"
"enter_rmb_password" : "请输入本币账号密码"
"enter_your_password" : "请输入旧iDeal密码"
"ideal_fx_user" : "外汇iDeal用户"
"ideal_idata_user" : "其他用户"
"ideal_rmb_user" : "本币iDeal用户"
"password" : "密码"
"please_agreement_user_private" : "请先同意用户许可协议和隐私协议"
"pwd_conPwd_incons" : "两次输入密码不一致，请重新输入"
"remove_user" : "删除用户"
"search_user" : "用户名/机构名"
"str_enter_origin_pwd" : "请输入原密码"
"str_enter_verify_pwd" : "请输入确认密码"
"str_forget_password" : "忘记密码"
"str_modify_pwd" : "修改密码"
"str_modify_pwd_fail" : "密码修改失败，请稍候重试"
"str_origin_pwd" : "原密码"

"str_passport_pwd" : "iDeal密码: %s"

"str_pwd_rule" : "密码必须是8-20位包含数字、字母与特殊符号组合"

"str_reset_pwd_tips" : "请联系iDeal FX中心场务重置密码4009787878-1-1"

"str_verify_pwd" : "确认密码"

"str_verify_pwd_tips" : "新密码格式有误，请重新输入"

"Enter_ideal_password" : "Enter password"

"Enter_password" : "Enter password"

"Forget_Password" : "Forget Password"

"Forget_iDeal_Password" : "Reset iDeal Password"

"Forget_pwd_hit" : "Please contact the customer service of the transaction system to find your RMB/FX password."

"Low_pwd_hip" : "Low password security level,please reset"

"Low_pwd_hip_note" : "Note: The password is relatively simple, please increase the complexity"

"Re_enter_password" : "Re-enter password"

"Username" : "Username"

"please_agreement_user_private" : "Please agree the user permission and privacy agreements."

"pwd_conPwd_incons" : "Passwords are inconsistent, please re-enter."

"str_reset_pwd_tips" : "Please contact iDeal FX administrator to reset password, contact 4009787878-1-1."

"enter_fx_password" : "Enter FX password"
"enter_rmb_password" : "Enter RMB password"
"enter_your_password" : "Enter your password"
"ideal_fx_user" : "iDeal FX User"
"ideal_idata_user" : "Other User"
"ideal_rmb_user" : "iDeal RMB User"
"remove_user" : "Remove"
"str_enter_origin_pwd" : "Enter current password"
"str_enter_verify_pwd" : "Enter the new password again"
"str_modify_pwd" : "Edit Password"
"str_modify_pwd_fail" : "Password modification failed. Please try again later."
"str_origin_pwd" : "Current Password"
"str_passport_pwd" : "iDeal Password: %s"
"str_pwd_rule" : "Letters, numbers, special characters are required (within 8-10 digits)."
"str_reset_pwd_tips" : "Please contact iDeal FX administrator to reset password, contact4009787878-1-1"
"str_verify_pwd" : "Enter the new password again"
"str_verify_pwd_tips" : "Invalid new password, please re-enter."

加壳分析

加壳类型	所属文件
腾讯Bugly	lib/arm64-v8a/libBugly.so
腾讯Bugly	libBugly.so
梆梆企业版	libDexHelper-x86.so
梆梆企业版	libDexHelper.so

第三方SDK

名称	分类	URL链接
梆梆加固	加壳加固, 开发辅助	https://reports.exodus-privacy.eu.org/trackers/458

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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

cn.com.chinamoney.ideal.rmb.permission.RECEIVE_MSG	未知	Unknown permission	Unknown permission from android reference
cn.com.chinamoney.ideal.rmb.permission.INCOMING_CALL	未知	Unknown permission	Unknown permission from android reference
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
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.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_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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.REAL_GET_TASKS	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.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.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。

com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
android.permission.READ_APP_BADGE	正常	显示应用程序通知	允许应用程序显示应用程序图标徽章
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.action.UPDATE_BADGE	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_DOWNLOAD_MANAGER	未知	Unknown permission	Unknown permission from android reference
android.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动
android.permission.BODY_SENSORS	危险		允许应用程序访问来自传感器的数据,用户使用这些数据来测量他/她体内发生的事情,例如心率
cn.com.chinamoney.ideal.rmb.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.zhonghui.ZHChat.module.splash.OutsideEntranceActivity	Schemes: chinamoney://, Hosts: ideal.chinamoney.com, Ports: 8888, Paths: /data,
com.zhonghui.ZHChat.module.share.ReceiverOutSideShareAcitivity	Schemes: file://, content://, Mime Types: text/plain, application/pdf, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, application/vnd.openxmlformats-officedocument.wordprocessingml.document, application/vnd.openxmlformats-officedocument.presentationml.template, application/vnd.openxmlformats-officedocument.presentationml.presentation, application/vnd.openxmlformats-officedocument.spreadsheetml.sheet, application/vnd.openxmlformats-officedocument.spreadsheetml.template, application/vnd.openxmlformats-officedocument.presentationml.slideshow, application/vnd.openxmlformats-officedocument.wordprocessingml.template,