MoGua

豆豆钱 7.7.5.APK 分析报告

APP名称:	豆豆钱

包名:	com.vcredit.ddcash
域名线索:	22条
URL线索:	7条
邮箱线索:	10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: DDCashM.apk
文件大小: 99.45MB
MD5值: 34d390747146d9a1550905f43bf06afe
SHA1值: 8bac385ba96a0a1a6fc710da5adc22c52e64c490
SHA256值: 52fa4b761c004a6d2e81f0d1fa96153334461cfbba0898665c689791447a7c48

APP 信息

App名称: 豆豆钱
包名: com.vcredit.ddcash
主活动Activity: com.vcredit.ddcash.start.LaunchActivity
安卓版本名称: 7.7.5
安卓版本: 777

域名线索

域名	服务器信息
data-dra.push.dbankcloud.com	**IP**: 119.8.163.189 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
gw.alicdn.com	**IP**: 60.222.11.236 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
grs.dbankcloud.cn	**IP**: 49.4.40.185 **所属国家**: China **地区**: Guangdong

	城市: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
metrics2.data.hicloud.com	IP: 80.158.2.190 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
id.local.demo.ariver.com	没有服务器地理信息.
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
grs.dbankcloud.eu	没有服务器地理信息.
metrics1.data.hicloud.com	IP: 111.202.16.252 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ipcrs.pbccrc.org.cn	IP: 140.207.159.100 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
	IP: 104.18.22.19 **所属国家**: United States of America **地区**: California

www.w3.org	**城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
metrics5.dt.dbankcloud.ru	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
data-drcn.push.dbankcloud.com	**IP**: 118.194.33.160 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
data-drru.push.dbankcloud.com	**IP**: 159.138.202.31 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
grs.dbankcloud.asia	**IP**: 121.36.117.149 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.taobao.com	**IP**: 221.194.162.215 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717

grs.platform.dbankcloud.ru	没有服务器地理信息.
66666692.hybrid.miniapp.taobao.com	**IP**: 203.119.144.26 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
data-dre.push.dbankcloud.com	**IP**: 80.158.49.244 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
grs.dbankcloud.com	**IP**: 60.28.193.195 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
mini-app-packages-cdn.taobao.com	**IP**: 221.194.162.215 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
alipay-rmsdeploy-image.cn-hangzhou.alipay.aliyun-inc.com	**IP**: 110.75.228.252 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
	IP: 159.138.203.215

metrics5.data.hicloud.com	**所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499

URL线索

URL信息	Url所在文件
https://ipcrs.pbccrc.org.cn/	摸瓜V1引擎
http://www.taobao.com/market/photo/topsq.php	摸瓜V1引擎
https://mini-app-packages-cdn.taobao.com/yaoyy_66666692/afts/file/A*2zt6TrpcZuUAAAAAAAAAAAAAAQAAAQ	摸瓜V2引擎
http://alipay-rmsdeploy-image.cn-hangzhou.alipay.aliyun-inc.com/jet-dev/AP_66666692/u7dirm6ha3s/	摸瓜V2引擎
https://66666692.hybrid.miniapp.taobao.com	摸瓜V2引擎
https://data-drcn.push.dbankcloud.com	摸瓜V2引擎
https://data-dra.push.dbankcloud.com	摸瓜V2引擎
https://data-dre.push.dbankcloud.com	摸瓜V2引擎
https://data-drru.push.dbankcloud.com	摸瓜V2引擎
https://metrics1.data.hicloud.com:6447	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics2.data.hicloud.com:6447	摸瓜V2引擎

https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.dt.dbankcloud.ru:6447	摸瓜V2引擎
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://grs.platform.dbankcloud.ru	摸瓜V2引擎
https://grs.dbankcloud.eu	摸瓜V2引擎
https://gw.alicdn.com/bao/uploaded/TB1wrITdRUSMeJjSszcXXbnwVXa-144-144.png	摸瓜V2引擎
https://gw.alicdn.com/bao/uploaded/TB1l473QlLoK1RjSZFuXXXn0XXa.amr	摸瓜V2引擎
https://<id>.local.demo.ariver.com	摸瓜V2引擎
https://appx/	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
tousu@vcredit.com 13349843@126.com shenhuix@vcredit.com	摸瓜V1引擎
中速矩形@2x.png	摸瓜V2引擎

进度条色@2x.png 进度条光@2x.png	摸瓜V2引擎
vip_进度条@2x.png vip_光@2x.png	摸瓜V2引擎
分润中速矩形@2x.png	摸瓜V2引擎
进度条色@2x.png 进度条光@2x.png	摸瓜V2引擎
vip_进度条@2x.png vip_光@2x.png	摸瓜V2引擎
风险@2x.png 逾期@2x.png 网贷@2x.png	摸瓜V2引擎
loading@3x.png	摸瓜V2引擎
loading@3x.png	摸瓜V2引擎

手机线索

手机号	所在文件
19199999641	摸瓜V2引擎

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=CN, ST=上海, L=上海, O=维信理财, OU=维视投资咨询上海有限公司, CN=Vcredit App
签名算法: rsassa_pkcs1v15
有效期自: 2015-12-21 01:30:37+00:00
有效期至: 2040-12-14 01:30:37+00:00
发行人: C=CN, ST=上海, L=上海, O=维信理财, OU=维视投资咨询上海有限公司, CN=Vcredit App
序列号: 0x7a520574
哈希算法: sha256
md5值: 28aae1cdae88319ffc535a8b0efde50a
sha1值: b65f9714b3c88a7adb2292b2019aff2779391f43
sha256值: 0a87b1e293fe739e7226412b766643722a63fcea6f3499a8dd6183f711e8e457
sha512值: 1910fbdf04d1509ba9d62d757ce8851e1a89dc11df847e057709707bb3284719f960b8eb71f5638a1c66937476abf5eef1ccc7a29a1aa82b75b9a5faea6dec42
公钥算法: rsa
密钥长度: 2048
指纹: 209e312327c7a1e70024ff43630ef9edf6231606fa221567b4bfd537d4311869

硬编码敏感信息

可能的敏感信息
"academic_auth" : "学历学籍认证"
"agree_auth_persenal_information" : "同意并签署《个人信息授权书》"
"ali_auth_sms_veri_title" : "请输入 %s 收到的验证码"
"ali_auth_verification_reGetCode" : "重新获取验证码"
"beat_all_infi_user" : "您已经打败了全国"
"beat_infi_user" : "的用户"
"bind_tb_password" : "请输入密码"

"callcredit_phone_auth_dialog_tips" : "服务密码是指客户用以登陆运营商（中国移动/中国联通/中国电信）网上营业厅的身份识别密码，由多位阿拉伯数字组成"

"callcredit_phone_auth_tips" : "服务密码是指客户用以登录运营商（中国移动/中国联通/中国电信）网上营业厅的身份识别密码，如果忘记服务密码，可去对应网上营业厅找回服务密码。"

"callcredit_reset_phone_auth" : "真实姓名有变动，手机需要重新认证或是修改成最初真实姓名"

"com_taobao_tae_sdk_authorize_title" : "登录授权"

"edit_resetservicepwd_address" : "发送至 %1$s"

"edit_resetservicepwd_content" : "编辑短信 %1$s"

"fail_authorize_sesame" : "抱歉，芝麻信用分获取失败。"

"findservicepwd_tip" : "您可以根据以下提示，找回您手机号的服务密码"

"findservicepwd_title" : "找回服务密码"

"forget_password" : "忘记密码"

"illegal_user_name" : "用户名不合法"

"kf_ding_cai_sessionoff" : "会话结束，无法反馈"

"login_forget_pwd" : "忘记密码？"

"login_password" : "登录密码"

"modify_password" : "修改"

"no_register_authority" : "无开放注册权限"

"nrtc_setting_other_device_default_rotation_key" : "nrtc_setting_other_device_default_rotation_key"

"nrtc_setting_other_device_rotation_fixed_offset_key" : "nrtc_setting_other_device_rotation_fixed_offset_key"

"nrtc_setting_other_server_record_audio_key" : "nrtc_setting_other_server_record_audio_key"

"nrtc_setting_other_server_record_video_key" : "nrtc_setting_other_server_record_video_key"

"nrtc_setting_other_webrtc_compat_key" : "setting_other_webrtc_compat_key"

"nrtc_setting_vie_crop_ratio_key" : "nrtc_setting_vie_crop_ratio_key"

"nrtc_setting_vie_default_front_camera_key" : "nrtc_setting_vie_default_front_camera_key"

"nrtc_setting_vie_fps_reported_key" : "nrtc_setting_vie_fps_reported_key"

"nrtc_setting_vie_hw_decoder_key" : "nrtc_setting_vie_hw_decoder_key"

"nrtc_setting_vie_hw_encoder_key" : "nrtc_setting_vie_hw_encoder_key"

"nrtc_setting_vie_max_bitrate_key" : "nrtc_setting_vie_max_bitrate_key"

"nrtc_setting_vie_quality_key" : "nrtc_setting_vie_quality_key"

"nrtc_setting_vie_rotation_key" : "nrtc_setting_vie_rotation_key"

"nrtc_setting_voe_audio_aec_key" : "nrtc_setting_voe_audio_aec_key"

"nrtc_setting_voe_audio_ns_key" : "nrtc_setting_voe_audio_ns_key"

"nrtc_setting_voe_call_proximity_key" : "nrtc_setting_voe_call_proximity_key"

"nrtc_setting_voe_dtx_key" : "nrtc_setting_voe_dtx_key"

"nrtc_setting_voe_high_quality_key" : "nrtc_setting_voe_high_quality_key"

"phone_auth" : "手机实名"

"pwd_reset_success" : "修改成功"

"pwd_rule" : "0123456789abcdefghijklnmopqrstuvwxyzABCDEFGHIJKLNMOPQRSTUVWXYZ"

"reset_password" : "重置密码"

"reset_service_password" : "一键重置服务密码"

"reset_servicepwd" : "重置服务密码"

"send_msm_resetservicepassword" : "请按以下提示发送短信指令，根据短信提示即可重置服务密码"

"sesamescore_authorize_des" : "请您授权豆豆钱读取您的芝麻信 用分数，获取额度几率更高。"

"sesamescore_authorize_title" : "芝麻分授权"

"set_login_password" : "设置登录密码"

"set_password" : "设置初始密码"

"start_auth" : "开始认证"

"tb_appkey" : "33297616"

"tiny_being_init_authorization_panel" : "授权面正在显示中"

"tiny_user_cancel_authorization" : "用户取消授权"

"top_core_auth" : "用户授权"

"triver_core_auth" : "用户授权"

"triver_video_no_support_choosevideo_api" : "当前的系统版本暂不支持chooseVideo API"

"warning_camera_auth" : "无法打开摄像头，请检查是否给豆豆钱开启了相关权限"

"kf_ding_cai_sessionoff" : "Percakapan berakhir, tidak ada umpan balik"

"kf_ding_cai_sessionoff" : "Gespräch beendet, kein feedback"

"kf_ding_cai_sessionoff" : "Conversation ended, you can't send feedback"

"kf_ding_cai_sessionoff" : "Percakapan berakhir, tidak ada umpan balik"

"kf_ding_cai_sessionoff" : "انتهت المحادثة، لا يمكنك إرسال ملاحظاتك"

"kf_ding_cai_sessionoff" : "Conversation terminée. Pas commentaire"

"kf_ding_cai_sessionoff" : "Konuşma bitti,geri dönüt verilemez"

"kf_ding_cai_sessionoff" : "La sesión terminó, no se puede comentar"

"kf_ding_cai_sessionoff" : "Perbincangan tamat, tidak dapat maklumbalas"

"kf_ding_cai_sessionoff" : "Fine della conversazione, nessun feedback"

"kf_ding_cai_sessionoff" : "Fim da sessão, sem se poder dar feedback"

"kf_ding_cai_sessionoff" : "สนทนาจบลงแล้ว ไม่สามารถเสนอแนะได้"

"kf_ding_cai_sessionoff" : "Wprowadź adres e-mail"

"kf_ding_cai_sessionoff" : "Hội thoại kết thúc, không thể phản hồi"

"kf_ding_cai_sessionoff" : "会話が終わりました。フィードバックできません"

"kf_ding_cai_sessionoff" : "회화 종료, 피드백 없음"

"kf_ding_cai_sessionoff" : "Разговор завершен, вы не можете отправить отзыв"
"kf_ding_cai_sessionoff" : "會話結束，無法反饋"

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
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。

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.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
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.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.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_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.PROCESS_OUTGOING_CALLS	危险	拦截拨出电话	允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话
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.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_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.SET_DEBUG_APP	危险	启用应用程序调试	允许一个应用程序打开另一个应用程序的调试。恶意应用程序可以使用它来杀死其他应用程序
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证令牌
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作
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.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器

com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
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.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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
com.vcredit.ddcash.permission.RECEIVE_MSG	未知	Unknown permission	Unknown permission from android reference
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.READ_SETTING	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.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.WRITE_CALENDAR	危险	添加或修改日历事件并向客人发送电子邮件	允许应用程序添加或更改日历上的事件,这可能会向客人发送电子邮件。恶意应用程序可以使用它来删除或修改您的日历活动或向客人发送电子邮件
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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
com.vcredit.ddcash.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	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
com.vcredit.ddcash.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
com.google.android.apps.photos.permission.GOOGLE_PHOTOS	未知	Unknown permission	Unknown permission from android reference
	未	Unknown	

com.vcredit.ddcash.permission.PROCESS_PUSH_MSG	知	permission	Unknown permission from android reference
com.vcredit.ddcash.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.vcredit.ddcash.start.LaunchActivity	Schemes: sa19f94e4c://, https://, http://, doudoumoneyschem://, sa5d6dbd34://, Hosts: heatmap, h5.vchedai.com, m.ddcash.cn, Path Prefixes: /launchapp,
com.tencent.tauth.AuthActivity	Schemes: tencent1105087389://, tencent"1105087389"://,
com.vcredit.ddcash.push.PushTransferActivity	Schemes: ddpush://, Hosts: com.vcredit.ddcash, Paths: /pushtransfer,
com.alipay.sdk.app.AlipayResultActivity	Schemes: @string/alipay_result_scheme://,

---