MoGua

够花 5.2.18.APK 分析报告

APP名称: 够花

包名:	com.haiercash.gouhua
域名线索:	17条
URL线索:	9条
邮箱线索:	0条
分析日期:	2025年2月22日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.haiercash.gouhua.apk
文件大小: 38.85MB
MD5值: 866333f4292b90720aba78d7fe0b0e3f
SHA1值: 97797ef14fea8b9e0baffcf14b22a9939716dde2
SHA256值: 5d138db7d2aab4e328818c78b8fc65dad28bb41468351c69a57ef88f866de907

APP 信息

App名称: 够花
包名: com.haiercash.gouhua
主活动Activity: com.haiercash.gouhua.activity.SplashActivity
安卓版本名称: 5.2.18
安卓版本: 538

域名线索

域名	服务器信息
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
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
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.cn	**IP**: 49.4.35.251 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
metrics1-drcn.dt.dbankcloud.cn	**IP**: 111.202.16.252 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
metrics5.data.hicloud.com	**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
grs.platform.dbankcloud.ru	没有服务器地理信息.
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
www.haiercash.com	**IP**: 60.28.220.199 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

data-drcn.push.dbankcloud.com	**IP**: 121.36.117.8 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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
www.baidu.com	**IP**: 110.242.69.21 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
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
grs.dbankcloud.eu	没有服务器地理信息.
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
	IP: 60.28.193.195

grs.dbankcloud.com	**所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
www.bing.com	**IP**: 202.89.233.100 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL信息	Url所在文件
https://www.haiercash.com	摸瓜V1引擎
https://www.bing.com	摸瓜V2引擎
https://www.baidu.com	摸瓜V2引擎
https://www.bing.com	摸瓜V2引擎
https://www.baidu.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://data-drra.push.dbankcloud.com	摸瓜V2引擎
https://metrics1-drcn.dt.dbankcloud.cn:443	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://www.bing.com	摸瓜V2引擎
https://www.baidu.com	摸瓜V2引擎
https://www.bing.com	摸瓜V2引擎
https://www.baidu.com	摸瓜V2引擎
https://www.bing.com	摸瓜V2引擎
https://www.baidu.com	摸瓜V2引擎

邮箱线索

手机线索

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=shanghai, L=shanghai, O=www.haiercash.com, OU=www.gouhua.com, CN=gouhua
签名算法: rsassa_pkcs1v15
有效期自: 2017-07-19 10:16:08+00:00
有效期至: 2042-07-13 10:16:08+00:00
发行人: C=cn, ST=shanghai, L=shanghai, O=www.haiercash.com, OU=www.gouhua.com, CN=gouhua
序列号: 0x6fe99de3
哈希算法: sha256
md5值: 799e6969fb9af7e8cfe6081dd8b77737
sha1值: 36606c98aa4564c586de96bd5c4c6ebaa86b0243
sha256值: d999116ee281855c01f28c08e950911d7f2c9c855c5ae86513ff2c0ebc24a678
sha512值: 08e6fc0c901216358337a1b3e16d421c15c618c0192b5f1c10863b40e1342db7a4d097eab9497fdcdf13a1c4402cd3423f3d6790a3400b46f77fc999c27675b9
公钥算法: rsa
密钥长度: 2048
指纹: bde80e242e3ecbcf7fc002b291ea3f31f1d1a6556e2d6a139e7f5abeddcf8cf6

硬编码敏感信息

可能的敏感信息
"agree_gzx_authorization" : "您同意「够智选」获取以下权限"
"borrow_password" : "为了您的账号安全，请设置您的交易密码。"

"borrow_password" : "为了您的账号安全，请设置您的支物密码。"

"forget_password" : "忘记密码"

"gt_one_login_auth_btn" : "一键登录"

"loading_go_auth" : "Go to Alipay for authorization"

"locationKey" : "EWtoa5lbyt31PwwgYndPGwGiFruCYp8B"

"private_desc_info_collect_list" : "个人信息收集清单"

"private_desc_other_share_list" : "第三方共享信息清单"

"private_desc_private_protocol" : "海尔消费金融隐私政策"

"private_desc_private_protocol_simple" : "海尔消费金融隐私政策摘要版"

"safe_setting_pay_pwd" : "交易密码"

"safe_setting_pay_pwd_set" : "设置交易密码"

"safe_setting_set_login_pwd" : "设置登录密码"

"security_public_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8hzUojzHX8jDL+97pqr7CaLiKSsZ0aOES7FUcX7vh9PoEDbCKNCTakRXdS5EiurPk3QpvsAGbfyIs7JWKm4py9KcIdJsZRh9onknVeAVlU++jnrGFGEYfQb8iKzClN059gYeeJBs9mwi7RGU9tj0KHUG659v5sMBxv7zNse3fJQIDAQAB"

"service_authorization" : "服务授权"

"set_login_pwd_title" : "设置密码"

"set_login_pwd_verify_mobile" : "验证手机号"

"set_login_pwd_verify_mobile_detail" : "验证码已发送至%s"

"setting_private" : "隐私管理"

"setting_private_desc" : "隐私说明"
"loading_go_auth" : "去支付宝授权"

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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
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.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.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
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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
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
com.android.launcher.permission.READ_SETTINGS	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.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.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。
			允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的

android.permission.READ_CALENDAR	危险	读取日历事件	日历事件发送给其他人
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.RECEIVE_USER_PRESENT	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。
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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.android.permission.GET_INSTALLED_APPS	未知	Unknown permission	Unknown permission from android reference
android.permission.CAPTURE_VIDEO_OUTPUT	正常		允许应用程序捕获视频输出
android.permission.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference

android.permission.RESTART_PACKAGES	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
com.haiercash.gouhua.permission.XGPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.haiercash.gouhua.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.haiercash.gouhua.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
com.haiercash.gouhua.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.permission.PUSH	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.haiercash.gouhua.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.haiercash.gouhua.permission.C2D_MESSAGE	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
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
freemme.permission.msa.SECURITY_ACCESS	未知	Unknown permission	Unknown permission from android reference
oplus.permission.settings.LAUNCH_FOR_EXPORT	未知	Unknown permission	Unknown permission from android reference
com.vivo.identifier.permission.OAID_STATE_DIALOG	未知	Unknown permission	Unknown permission from android reference
com.asus.permission.READ_SDID_PROVIDER	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.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
com.haiercash.gouhua.permission.liantian.RECEIVE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.haiercash.gouhua.activity.SplashActivity	Schemes: gouhua://, atm.18670957://, tingyun.7000://, Hosts: com.haiercash,
com.haiercash.gouhua.MainActivity	Schemes: gouhua://, Hosts: home,
	Schemes: gouhua://,

com.haiercash.gouhua.activity.RePayAndRecordActivity	Hosts: repayRecrd,
com.haiercash.gouhua.activity.bankcard.MyCreditCardActivity	Schemes: gouhua://, Hosts: bankCardManager,
com.alipay.sdk.app.AlipayResultActivity	Schemes: gouhuaalipay://,
com.haiercash.gouhua.activity.accountsettings.SafetySettingActivity	Schemes: gouhua://, Hosts: accountSecurity,
com.haiercash.gouhua.activity.edu.NameAuthStartActivity	Schemes: gouhua://, Hosts: newuserexclusive,
com.haiercash.gouhua.activity.contract.ForActiveShareActivity	Schemes: gouhua://, Hosts: springfestival,
com.haiercash.gouhua.activity.contract.SharePageActivity	Schemes: gouhua://, Hosts: showsharepage,
com.haiercash.gouhua.activity.CouponBagActivity	Schemes: gouhua://, Hosts: couponbagV1,
com.haiercash.gouhua.activity.CouponBagActivityV2	Schemes: gouhua://, Hosts: couponbag,
com.haiercash.gouhua.activity.ProguardInfoActivity	Schemes: gouhua://, Hosts: infoProtect,
com.tencent.android.tpush.TpnsActivity	Schemes: tpns://, Hosts: com.haiercash.gouhua,
com.tencent.android.tpush.InnerTpnsActivity	Schemes: stpns://, Hosts: com.haiercash.gouhua,