



MoGua

米多赚钱 1.8.0.APK 分析报告



APP名称:

米多赚钱

包名:	com.sakura.mizhuan
域名线索:	18条
URL线索:	6条
邮箱线索:	0条
分析日期:	2025年7月3日
分析平台:	摸瓜APK反编译平台

文件名: base.apk
文件大小: 25.94MB
MD5值: 5bb8f35d4d20da6e1d648abdba9968e3
SHA1值: 95007417fc68583a248a8f9a3f6d37f2aa523214
SHA256值: 1fb8db6b0a5012297f9a5faeefea8341f09bcd23ba7d8ddf5c6353d96b0ac06d

i APP 信息

App名称: 米多赚钱
包名: com.sakura.mizhuan
主活动Activity: com.sakura.mizhuan.activity.FlashActivity
安卓版本名称: 1.8.0
安卓版本: 180

🔍 域名线索

域名	服务器信息
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
gcc.gnu.org	IP: 8.43.85.97 所属国家: United States of America 地区: North Carolina 城市: Raleigh 纬度: 35.773994 经度: -78.632759
www.mob.com	IP: 180.188.26.28 所属国家: China 地区: Zhejiang

	城市: Taizhou 纬度: 28.666668 经度: 121.349998
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.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
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
grs.platform.dbankcloud.ru	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
metrics2.data.hicloud.com	IP: 80.158.38.48 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
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
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
grs.dbankcloud.cn	IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
	IP: 159.138.204.140 所属国家: Russian Federation

metrics.dt.dbankcloud.ru	地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
grs.dbankcloud.asia	IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
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.eu	没有服务器地理信息.

 URL线索

URL信息	Url所在文件
http://www.mob.com/policy/en>http://www.mob.com/policy/en.	摸瓜V1引擎
http://www.mob.com/about/policy>http://www.mob.com/about/policy	摸瓜V1引擎
https://www.mob.com	摸瓜V1引擎
http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en.lf	摸瓜V1引擎
http://www.mob.com/policy/zh>http://www.mob.com/policy/zh	摸瓜V1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://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://metrics.dt.dbankcloud.ru	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://github.com/...	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V3引擎
http://gcc.gnu.org/bugs.html):	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3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=Guangdong, L=Shenzhen, O=Seabeach, OU=Seabeach, CN=admin
签名算法: rsassa_pkcs1v15
有效期自: 2019-12-23 03:52:53+00:00
有效期至: 2044-12-16 03:52:53+00:00
发行人: C=CN, ST=Guangdong, L=Shenzhen, O=Seabeach, OU=Seabeach, CN=admin
序列号: 0x1ec1871b
哈希算法: sha256
md5值: 0e228cc812c2ce9ce2eb135e0dd3b6fe
sha1值: 3597c9c6eea1bee153ad047fa37deee0ebb346d8
sha256值: 1e6c9674298f943faf965b79f311886b7ceff7088d6338239a4013412859c19b
sha512值: c5ad60b8d96691039c34e022fc54baef36f19ab049aa7384f398f89ff7d285064c42cdf29a95431085c765b2b3b6d463a16bc5b28165f86682ec3f92acb16e60

公钥算法: rsa
密钥长度: 2048
指纹: 1cfd6dae63e5ac4ba56eaf46cf569778661d453720fb8f75c90402b8d13394a0

硬编码敏感信息

可能的敏感信息
"Modify_user_name" : "修改用户名"
"mobcommon_authorize_dialog_accept" : "Accept"
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click http://www.mob.com/policy/en. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"mobdemo_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见http://www.mob.com/about/policy。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"
"mobdemo_authorize_dialog_title" : "服务授权"
"ssdk_cmcc_auth" : "手机认证服务由中国移动提供"
"ssdk_cmcc_login_one_key" : "本机号码一键登录"
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"mobcommon_authorize_dialog_accept" : "Accept"

"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click http://www.mob.com/policy/en. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"mobdemo_authorize_dialog_content" : "In order to provide you with Mobservice related products and services, please check our privacy policy in detail, see detailshttp://www.mob.com/about/policy/en.If you agree with our privacy policy, please click accept. If you disagree with our privacy policy, please click reject."
"mobdemo_authorize_dialog_title" : "service authority"
"ssdk_cmcc_auth" : "Provided by China Mobile"
"ssdk_cmcc_login_one_key" : "PhoneNum Login"
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"
"mobcommon_authorize_dialog_accept" : "同意"
"mobcommon_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见http://www.mob.com/policy/zh。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"
"mobcommon_authorize_dialog_reject" : "拒绝"
"mobcommon_authorize_dialog_title" : "服务授权"

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.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.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.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.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference

android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_INSTALL	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
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
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_PRIVILEGED_PHONE_STATE	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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.PERMISSIONS_STORAGE	未知	Unknown permission	Unknown permission from android reference
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.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	Unknown permission from android reference

		permission	
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.WRITE_MEDIA_STORAGE	未知	Unknown permission	Unknown permission from android reference
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_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
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.sakura.mizhuan.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.sakura.mizhuan.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.sakura.mizhuan.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.sakura.mizhuan.permission.PUSH_PROVIDER	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
com.sakura.mizhuan.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.vivo.notification.permission.BADGE_ICON	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
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.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

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.sakura.mizhuan.activity.RenWuDetailActivity	Schemes: miduo://, Hosts: app, Package: com.sakura.mizhuan

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。