Evaluation Warning: The document was created with Spire.Doc for Python.

**小金库钱包（ 2.0.0版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 小金库钱包 |
| 版本 | 2.0.0 |
| 包名 | com.pm.GkPocket |
| 域名线索 | 19条 |
| URL线索 | 15条 |
| APP图标 |  |
| 分析日期 | 2025年6月9日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | Android\_GKApp\_v2.0.0.apk |
| 文件大小 | 26.8MB |
| MD5值 | cdda3d5c050acb808adc07114bc269ee |
| SHA1值 | 5e15867b88bd94a4a85a6d93033368d00276906d |
| SHA256值 | 3c3e0834a731cc44053cd99731e4c01cdfe11234beb16f410b2a075a54d7f60d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 小金库钱包 |
| 包名 | com.pm.GkPocket |
| 主活动Activity | com.pm.GkPocket.MainActivity |
| 安卓版本名称 | 2.0.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.example.com | IP: 92.122.244.34 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| issuetracker.google.com | IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| proxy.capeleph.com | IP: 43.175.132.135 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| github.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| developer.android.com | IP: 142.250.69.174 所属国家: United States of America 地区: California 城市: Mountain View  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| docs.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| dartbug.com | IP: 216.239.38.21 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| journeyapps.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| grs.dbankcloud.asia | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| grs.dbankcloud.cn | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| proxy.elephbit.com | IP: 43.175.132.135 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| plus.google.com | IP: 104.244.46.93 所属国家: United States of America 地区: California 城市: San Francisco  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://plus.google.com/  | c2/k1.java  |
| https://)([\\s\\S]+)  | com/huawei/hms/scankit/p/C0167bd.java  |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview\_android/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/g.java  |
| https://github.com/Baseflow/flutter-permission-handler/issues  | h1/t.java  |
| https://docs.flutter.dev/deployment/android  | l5/d.java  |
| https://issuetracker.google.com/issues/new?component=618491&template=1257717  | r/g.java  |
| https://journeyapps.com/  | 摸瓜V1引擎  |
| https://github.com/journeyapps/zxing-android-embedded  | 摸瓜V1引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| http://www.unicode.org/copyright.html  | lib/arm64-v8a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |
| https://dartbug.com/52121.  | lib/arm64-v8a/libflutter.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| https://proxy.elephbit.com/  | lib/armeabi-v7a/libapp.so  |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Status  | lib/armeabi-v7a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/armeabi-v7a/libapp.so  |
| https://proxy.capeleph.com/  | lib/armeabi-v7a/libapp.so  |
| http://www.unicode.org/copyright.html  | lib/armeabi-v7a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/armeabi-v7a/libflutter.so  |
| https://dartbug.com/52121.  | lib/armeabi-v7a/libflutter.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/x86\_64/libapp.so  |
| http://www.unicode.org/copyright.html  | lib/x86\_64/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/x86\_64/libflutter.so  |
| https://dartbug.com/52121.  | lib/x86\_64/libflutter.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | z1/s.java  |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |
| authenticationscheme@13463476.fromstring \_list@0150898.of \_httpparser@13463476.responsepa \_list@0150898.generate \_typeerror@0150898.\_create \_list@0150898.\_ofgrowabl \_list@0150898.\_ofefficie \_growablelist@0150898.\_ofarray \_double@0150898.fromintege \_growablelist@0150898.\_literal3 \_future@4048458.immediate channelcontroller@26156646.implementa \_growablelist@0150898.\_literal \_growablelist@0150898.\_ofother \_compressednode@42137193.single \_link@14069316.fromrawpat \_growablelist@0150898.withcapaci \_timer@1026248.\_internal \_growablelist@0150898.\_literal6 \_growablelist@0150898.\_literal5 \_receiveportimpl@1026248.fromrawrec androidstorage@30339836.implementa \_list@0150898.\_ofarray \_timer@1026248.periodic \_growablelist@0150898.\_literal2 \_bigintimpl@0150898.from \_hashcollisionnode@42137193.fromcollis \_list@0150898.empty \_list@0150898.\_ofother \_bytebuffer@7027147.\_new \_directory@14069316.fromrawpat \_invocationmirror@0150898.\_withtype ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create \_nativesocket@14069316.normal \_uri@0150898.file \_growablelist@0150898.\_literal1 \_uri@0150898.directory \_growablelist@0150898.\_literal8 \_file@14069316.fromrawpat \_growablelist@0150898.\_literal4 \_growablelist@0150898.\_ofgrowabl \_growablelist@0150898.of \_growablelist@0150898.generate \_uri@0150898.notsimple \_growablelist@0150898.\_literal7 \_future@4048458.zonevalue \_growablelist@0150898.\_ofefficie \_future@4048458.immediatee  | lib/armeabi-v7a/libapp.so  |
| appro@openssl.org  | lib/x86\_64/libflutter.so  |

### **4.4 手机号线索**

## **5. 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: CN=Android Debug, O=Android, C=US 签名算法: rsassa\_pkcs1v15 有效期自: 2024-03-27 09:04:28+00:00 有效期至: 2054-03-20 09:04:28+00:00 发行人: CN=Android Debug, O=Android, C=US 序列号: 0x1 哈希算法: sha1 md5值: fb65742aa43f4be6a78aaf8be1057e12 sha1值: 2702c0935bba9bf405ad31dd5dc05da1a6ee4dc3 sha256值: 388d3ae47bf0d2a09c64bcfc3b3538a65e950b54acc3c5fab30a7a39b5b5e4b1 sha512值: 00e0b0378c3cecdf18fe912033c254c8e0de0ca568d16e03b53a4f3aaed9b44a511dd7d0dc06be611c56b0fd2419a7343d3405d4a22acbb88c3186298cee3231 公钥算法: rsa 密钥长度: 2048 指纹: df7139d565ef6685dfe0531a7470f7fd29b156cf778c97d4f184d4988ba3d08f**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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.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\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| 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.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.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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.ACCESS\_MEDIA\_LOCATION | 危险 | 访问的任何地理位置 | 允许应用程序访问的任何地理位置持久保存在用户的共享集合 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| com.pm.GkPocket.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.pm.GkPocket.MainActivity | **Schemes**: gkpocket://, **Hosts:** pay, transfer, widthdrawal, receive,  |

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