MoGua

# 金护 1.0.3.APK 分析报告

APP名称: 金护

| | |
|---|---|
| 包名: | com.jinhu |
| 域名线索: | 27条 |
| URL线索: | 6条 |
| 邮箱线索: | 0条 |
| 分析日期: | 2025年6月26日 |
| 分析平台: | 摸瓜APK反编译平台 |

## 文件信息

**文件名**: 金护.apk
**文件大小**: 33.36MB
**MD5值**: 5462ad971f38c03787c044f469a44fe7
**SHA1值**: 62be0fe60c52b2fdf356ec62af7c0da21927c9ce
**SHA256值**: ce841fe1ebbcee3d548fbaf1ca0f3c9379e991343081d43af82c405ad8f902ac

# APP 信息

**App名称**: 金护
**包名**: com.jinhu
**主活动Activity**: com.jinhu.SplashActivity
**安卓版本名称**: 1.0.3
**安卓版本**: 103

# 域名线索

| 域名 | 服务器信息 |
| --- | --- |
| datacollector.dt.dbankcloud.eu | 没有服务器地理信息. |
| grs.dbankcloud.cn | **IP**: 49.4.40.185<br>**所属国家**: China<br>**地区**: Guangdong<br>**城市**: Guangzhou<br>**纬度**: 23.127361<br>**经度**: 113.264572 |
| data-drcn.push.dbankcloud.com | **IP**: 49.4.40.58<br>**所属国家**: China<br>**地区**: Guangdong<br>**城市**: Guangzhou<br>**纬度**: 23.127361<br>**经度**: 113.264572 |

| | |
|---|---|
| datacollector.dt.dbankcloud.asia | 没有服务器地理信息. |
| grs.platform.dbankcloud.ru | 没有服务器地理信息. |
| cpki-caweb.huawei.com | 没有服务器地理信息. |
| metrics2.data.hicloud.com | **IP**: 80.158.38.48<br>**所属国家**: Germany<br>**地区**: Schleswig-Holstein<br>**城市**: Kiel<br>**纬度**: 54.321358<br>**经度**: 10.134532 |
| data-dra.push.dbankcloud.com | **IP**: 119.8.163.189<br>**所属国家**: Singapore<br>**地区**: Singapore<br>**城市**: Singapore<br>**纬度**: 1.289987<br>**经度**: 103.850281 |
| android.googlesource.com | **IP**: 74.125.20.82<br>**所属国家**: United States of America<br>**地区**: California<br>**城市**: Mountain View<br>**纬度**: 37.405991<br>**经度**: -122.078514 |
| datacollector.dt.dbankcloud.ru | 没有服务器地理信息. |
| journeyapps.com | **IP**: 13.35.37.68<br>**所属国家**: Taiwan (Province of China)<br>**地区**: Taipei<br>**城市**: Taipei<br>**纬度**: 25.038172<br>**经度**: 121.563599 |
| | **IP**: 159.138.207.55<br>**所属国家**: Russian Federation<br>**地区**: Sverdlovskaya oblast' |

| | |
|---|---|
| datacollector-drru.dt.dbankcloud.ru | **城市**: Yekaterinburg<br>**纬度**: 56.857498<br>**经度**: 60.612499 |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31<br>**所属国家**: Russian Federation<br>**地区**: Sverdlovskaya oblast'<br>**城市**: Yekaterinburg<br>**纬度**: 56.857498<br>**经度**: 60.612499 |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252<br>**所属国家**: China<br>**地区**: Beijing<br>**城市**: Beijing<br>**纬度**: 39.907501<br>**经度**: 116.397102 |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215<br>**所属国家**: Russian Federation<br>**地区**: Sverdlovskaya oblast'<br>**城市**: Yekaterinburg<br>**纬度**: 56.857498<br>**经度**: 60.612499 |
| grs.dbankcloud.com | IP: 60.28.200.159<br>**所属国家**: China<br>**地区**: Tianjin<br>**城市**: Tianjin<br>**纬度**: 39.142181<br>**经度**: 117.176102 |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244<br>**所属国家**: Germany<br>**地区**: Schleswig-Holstein<br>**城市**: Kiel<br>**纬度**: 54.321358<br>**经度**: 10.134532 |
| | |

| | |
|---|---|
| grs.dbankcloud.asia | **IP**: 121.36.116.8<br>**所属国家**: China<br>**地区**: Beijing<br>**城市**: Beijing<br>**纬度**: 39.907501<br>**经度**: 116.397102 |
| datacollector-drcn.dt.dbankcloud.cn | **IP**: 49.4.37.205<br>**所属国家**: China<br>**地区**: Guangdong<br>**城市**: Guangzhou<br>**纬度**: 23.127361<br>**经度**: 113.264572 |
| www.apache.org | **IP**: 151.101.2.132<br>**所属国家**: United States of America<br>**地区**: California<br>**城市**: San Francisco<br>**纬度**: 37.775700<br>**经度**: -122.395203 |
| metrics5.data.hicloud.com | **IP**: 159.138.203.215<br>**所属国家**: Russian Federation<br>**地区**: Sverdlovskaya oblast'<br>**城市**: Yekaterinburg<br>**纬度**: 56.857498<br>**经度**: 60.612499 |
| metrics-dra.dt.hicloud.com | **IP**: 94.74.88.100<br>**所属国家**: Singapore<br>**地区**: Singapore<br>**城市**: Singapore<br>**纬度**: 1.289987<br>**经度**: 103.850281 |
| github.com | **IP**: 20.205.243.166<br>**所属国家**: Singapore<br>**地区**: Singapore<br>**城市**: Singapore<br>**纬度**: 1.289987 |

| | |
|---|---|
| | **经度**: 103.850281 |
| datacollector-dre.dt.dbankcloud.cn | **IP**: 80.158.17.115<br>**所属国家**: Germany<br>**地区**: Schleswig-Holstein<br>**城市**: Kiel<br>**纬度**: 54.321358<br>**经度**: 10.134532 |
| datacollector-dra.dt.dbankcloud.cn | **IP**: 159.138.90.129<br>**所属国家**: Singapore<br>**地区**: Singapore<br>**城市**: Singapore<br>**纬度**: 1.289987<br>**经度**: 103.850281 |
| grs.dbankcloud.eu | 没有服务器地理信息. |
| datacollector.dt.dbankcloud.cn | 没有服务器地理信息. |

## URL线索

| URL**信息** | Url**所在文件** |
|---|---|
| https://journeyapps.com/ | 摸瓜V1引擎 |
| https://github.com/journeyapps/zxing-android-embedded | 摸瓜V1引擎 |
| https://datacollector-drcn.dt.dbankcloud.cn | 摸瓜V2引擎 |
| https://datacollector.dt.dbankcloud.cn | 摸瓜V2引擎 |
| https://datacollector-dra.dt.dbankcloud.cn | 摸瓜V2引擎 |

| | |
|---|---|
| https://datacollector.dt.dbankcloud.asia | 摸瓜V2引擎 |
| https://datacollector-dre.dt.dbankcloud.cn | 摸瓜V2引擎 |
| https://datacollector.dt.dbankcloud.eu | 摸瓜V2引擎 |
| https://datacollector-drru.dt.dbankcloud.ru | 摸瓜V2引擎 |
| https://datacollector.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-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.platform.dbankcloud.ru | 摸瓜V2引擎 |
| https://grs.dbankcloud.eu | 摸瓜V2引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V3引擎 |
| http://schemas.android.com/aapt | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm-project | 摸瓜V3引擎 |
| http://cpki-caweb.huawei.com/cpki/servlet/crlFileDown.crl?certype=1&/rootcrl.crl0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android77material_textinput_timepicker | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/clang | 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: True

找到 1 个唯一证书
主题: CN=QiAnPangu, OU=QiAnPangu, O=QianPangu, L=ShangHai, ST=ShangHai, C=CN
签名算法: rsassa_pkcs1v15
有效期自: 2024-07-18 03:18:37+00:00
有效期至: 2049-07-12 03:18:37+00:00
发行人: CN=QiAnPangu, OU=QiAnPangu, O=QianPangu, L=ShangHai, ST=ShangHai, C=CN
序列号: 0x1
哈希算法: sha256
md5值: 255039b7904998419ec86fde54065818
sha1值: dab31c96e173fcfdf92073b917ee53287a90edbf
sha256值: fd3c86ef55f5cd069131b0142ce9f1766cafca02ab60ec0005167984b6bc20da
sha512值: 19a469cfde57533d5e19258d676d8bdd430b0b4bb2be6705e816d35c24a3c4bd12156296f5a43806c593da74d71c7cc52c8d0b77391fcdbfacc7a67e10a18d54
公钥算法: rsa
密钥长度: 2048
指纹: e8a7ec8b1199841f06c64a64385936c5bb3dbf86ad6e0caac353fc7a220b11e5

# 硬编码敏感信息

| 可能的敏感信息 |
| --- |
| "appsecret_oppopush" : "N2MyOTM4NjM3ZTk5NDNjYzkxYmNkMWI3NjYwOTA4YmY=" |
| "library_zxingandroidembedded_author" : "JourneyApps" |
| "library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/" |

# 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.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 permission | Unknown permission from android reference |
| android.permission.READ_MEDIA_VISUAL_USER_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND_SERVICE | 正常 | | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |

| | | | |
|---|---|---|---|
| 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.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.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_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.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_SPECIAL_USE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| android.permission.PACKAGE_USAGE_STATS | 合法 | 更新组件使用统计 | 允许修改收集的组件使用统计。不供普通应用程序使用 |
| android.permission.OBSERVE_APP_USAGE | 未知 | Unknown permission | Unknown permission from android reference |
| | 正 | | 应用程序必须持有的权限才能使用 |

| | | | |
|---|---|---|---|
| android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS | 常 | | Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。 |
| 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.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 |
| com.vivo.notification.permission.BADGE_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| 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.huawei.android.launcher.permission.READ_SETTINGS | 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.huawei.android.launcher.permission.WRITE_SETTINGS | 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.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.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 |
| com.jinhu.permission.MIPUSH_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.jinhu.permission.PROCESS_PUSH_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| | 未 | Unknown | |

| | | | |
|---|---|---|---|
| com.jinhu.permission.PUSH_PROVIDER | 知 | permission | Unknown permission from android reference |
| com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA | 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.hihonor.push.permission.READ_PUSH_NOTIFICATION_INFO | 未知 | Unknown permission | Unknown permission from android reference |

# 应用内通信

| **活动**(ACTIVITY) | **通信**(INTENT) |
|---|---|
| com.jinhu.ProtoActivity | Schemes: jinhuscheme://,<br>Hosts: com.jinhuapp.push,<br>Paths: /start-vpn, |

---