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

**当贝AI（ 1.0.8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 | 当贝AI |
| 版本 | 1.0.8 |
| 包名 | com.dangbei.ai |
| 域名线索 | 64条 |
| URL线索 | 59条 |
| APP图标 |  |
| 分析日期 | 2025年6月16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 | DBAI\_v1.0.8\_prod\_20250530\_144318.apk |
| 文件大小 | 53.57MB |
| MD5值 | de6ae5190ef44377e99b29f35886fcf9 |
| SHA1值 | c32e6a3b65addb1f5bc4a3a06a2a7bdaf702a168 |
| SHA256值 | f245335eee0553c03cfdc307d48f857e22842d1940edc827b0f2befdb44279de |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 当贝AI |
| 包名 | com.dangbei.ai |
| 主活动Activity | com.dangbei.ai.MainActivity |
| 安卓版本名称 | 1.0.8 |
| 安卓版本 | 108 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api-push.meizu.com | IP: 221.5.93.66  所属国家: China  地区: Guangdong  城市: Foshan |
| issuetracker.google.com | IP: 142.250.217.110  所属国家: United States of America  地区: California  城市: Mountain View |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215  所属国家: Russian Federation  地区: Sverdlovskaya oblast'  城市: Yekaterinburg |
| sss.umeng.com | IP: 59.82.31.210  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ccs.umeng.com | IP: 36.143.252.41  所属国家: China  地区: Beijing  城市: Beijing |
| errlogos.umeng.com | IP: 47.246.110.96  所属国家: Singapore  地区: Singapore  城市: Singapore |
| grs.dbankcloud.asia | IP: 121.36.116.8  所属国家: China  地区: Beijing  城市: Beijing |
| xml.org | IP: 104.239.142.8  所属国家: United States of America  地区: Texas  城市: Windcrest |
| data-drcn.push.dbankcloud.com | IP: 118.194.33.160  所属国家: China  地区: Shanghai  城市: Shanghai |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.jsdelivr.com | IP: 172.67.208.113  所属国家: United States of America  地区: California  城市: San Francisco |
| dev.to | IP: 151.101.194.217  所属国家: United States of America  地区: California  城市: San Francisco |
| norma-external-collect.meizu.com | 没有服务器地理信息. |
| www.unicode.org | IP: 64.182.27.164  所属国家: United States of America  地区: Texas  城市: Dallas |
| 10.38.162.35 | IP: 10.38.162.35  所属国家: -  地区: -  城市: - |
| metrics5.data.hicloud.com | IP: 159.138.203.215  所属国家: Russian Federation  地区: Sverdlovskaya oblast'  城市: Yekaterinburg |
| grs.platform.dbankcloud.ru | 没有服务器地理信息. |
| utoken.umeng.com | IP: 223.109.148.171  所属国家: China  地区: Jiangsu  城市: Nanjing |
| ns.adobe.com | 没有服务器地理信息. |
| dartbug.com | IP: 216.239.36.21  所属国家: United States of America  地区: California  城市: Mountain View |
| developer.mozilla.org | IP: 34.111.97.67  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| yumao.puata.info | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| pslog.umeng.com | IP: 59.82.60.44  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| gist.github.com | IP: 46.82.174.68  所属国家: Germany  地区: Niedersachsen  城市: Braunschweig |
| resolve.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| ulogs.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100  所属国家: Singapore  地区: Singapore  城市: Singapore |
| errnewlog.umeng.com | IP: 223.109.148.143  所属国家: China  地区: Jiangsu  城市: Nanjing |
| errnewlogos.umeng.com | IP: 47.246.110.18  所属国家: Singapore  地区: Singapore  城市: Singapore |
| mp.weixin.qq.com | IP: 116.128.169.212  所属国家: China  地区: Shanghai  城市: Shanghai |
| xmlpull.org | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| metrics2.data.hicloud.com | IP: 80.158.2.190  所属国家: Germany  地区: Schleswig-Holstein  城市: Kiel |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244  所属国家: Germany  地区: Schleswig-Holstein  城市: Kiel |
| www.example.com | IP: 92.122.244.33  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| developer.umeng.com | IP: 59.82.31.210  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| cn.register.xmpush.xiaomi.com | IP: 123.125.102.39  所属国家: China  地区: Beijing  城市: Beijing |
| open.weixin.qq.com | IP: 116.128.171.214  所属国家: China  地区: Shanghai  城市: Shanghai |
| grs.dbankcloud.eu | 没有服务器地理信息. |
| ulogs.umengcloud.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| offmsg.umeng.com | IP: 59.82.29.249  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| aspect-upush.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| msg.umengcloud.com | IP: 124.239.14.132  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| resolver.msg.xiaomi.net | IP: 110.43.0.169  所属国家: China  地区: Beijing  城市: Beijing |
| cnlogs.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| grs.dbankcloud.cn | IP: 49.4.45.231  所属国家: China  地区: Guangdong  城市: Guangzhou |
| code.google.com | IP: 142.250.217.78  所属国家: United States of America  地区: California  城市: Mountain View |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252  所属国家: China  地区: Beijing  城市: Beijing |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| audid.umeng.com | IP: 123.183.232.72  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| cs.android.com | IP: 142.250.69.174  所属国家: United States of America  地区: California  城市: Mountain View |
| developer.android.com | IP: 142.250.69.174  所属国家: United States of America  地区: California  城市: Mountain View |
| schemas.android.com | 没有服务器地理信息. |
| android.googlesource.com | IP: 142.250.99.82  所属国家: United States of America  地区: California  城市: Mountain View |
| api-push.in.meizu.com | IP: 206.161.233.191  所属国家: United States of America  地区: Virginia  城市: Herndon |
| errlog.umeng.com | IP: 223.109.148.142  所属国家: China  地区: Jiangsu  城市: Nanjing |
| alogsus.umeng.com | IP: 223.109.148.176  所属国家: China  地区: Jiangsu  城市: Nanjing |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31  所属国家: Russian Federation  地区: Sverdlovskaya oblast'  城市: Yekaterinburg |
| docs.flutter.dev | IP: 199.36.158.100  所属国家: United States of America  地区: California  城市: Mountain View |
| ucc.umeng.com | IP: 203.119.169.43  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| alogus.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| grs.dbankcloud.com | IP: 60.28.200.159  所属国家: China  地区: Tianjin  城市: Tianjin |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/Kotlin/kotlinx.coroutines/issues, | aa/s1.java |
| https://github.com/Baseflow/flutter-permission-handler/issues | c5/q.java |
| https://errnewlogos.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errnewlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errnewlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/d/c.java |
| https://issuetracker.google.com/issues/139738913 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/af7dcdf35a37d7a7dbaad7d9869c1c91bce2272b | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/9b5257c9c99c4cb541d8e8e78fb04f008b1a9091 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/893d6fe48d37f71e683f722457bea646994a10 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/b3a9bc038d3a218b1dbdf7b5668e3d6c12be5e | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=171190 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://gist.github.com/pyricau/4df64341cc978a7de414 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/square/leakcanary/issues/1 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=171830 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=172542 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=172659 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://gist.github.com/andaag/b05ab66ed0f06167d6e0 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=173689 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=173788 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=173789 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/27db46850b708070452c0ce49daf5f79503fbde6 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/7a96f3c917e0001ee739b65da37b2fadec7d7765 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=152173 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://gist.github.com/jankovd/891d96f476f7a9ce24e2 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=188551 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://android.googlesource.com/platform/frameworks/base/+/5b734f2430e9f26c769d6af8ea5645e390fcf5af%5E%21/ | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://code.google.com/p/android/issues/detail?id=198852 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/android/platform\_frameworks\_base/commit/e0bef71662d81caaaa0d7214fb0bef5d39996a69 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://android.googlesource.com/platform/frameworks/base/+/193520e3dff5248ddcf8435203bf99d2ba667219%5E%21/core/java/android/view/accessibility/AccessibilityNodeInfo.java | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/aosp-mirror/platform\_frameworks\_base/commit/86b326012813f09d8f1de7d6d26c986a909d | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://issuetracker.google.com/issues/112792715 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/square/leakcanary/issues/1210 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://issuetracker.google.com/issues/129250419 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://cs.android.com/android/\_/android/platform/frameworks/base/+/89608118192580ffca026b5dacafa637a556d578\nFixed | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://cs.android.com/android/\_/android/platform/frameworks/base/+/1f771846c51148b7cb6283e6dc82a216ffaa5353\nRelated | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://dev.to/pyricau/beware-packagemanager-leaks-223g | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://gist.github.com/cypressious/91c4fb1455470d803a602838dfcd5774 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://gist.github.com/jankovd/a210460b814c04d500eb12025902d60d | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/square/leakcanary/issues/32 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/square/leakcanary/issues/177 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/square/leakcanary/issues/1819 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| https://github.com/square/leakcanary/issues/696 | com/efs/sdk/memleaksdk/monitor/internal/ak.java |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/f.java |
| http://xml.org/sax/features/namespaces | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java |
| http://xml.org/sax/features/validation | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java |
| http://xml.org/sax/features/namespaces | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/namespace-prefixes | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/validation | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/external-general-entities | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/external-parameter-entities | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/string-interning | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xmlpull.org/v1/doc/features.html | com/huawei/secure/android/common/xml/XmlNewPullParserSecurity.java |
| http://xmlpull.org/v1/doc/features.html | com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java |
| https://api-push.meizu.com/garcia/api/server/getPublicKey | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| https://api-push.meizu.com/garcia/api/server/getPushConf | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| https://api-push.in.meizu.com | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| https://api-push.meizu.com | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| https://norma-external-collect.meizu.com/android/exchange/getpublickey.do | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| https://norma-external-collect.meizu.com/push/android/external/add.do | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| https://api-push.meizu.com/garcia/api/client/ | com/meizu/f0/a.java |
| https://api-push.in.meizu.com/garcia/api/client/ | com/meizu/f0/a.java |
| https://api-push.meizu.com/garcia/api/client/log/upload | com/meizu/f0/a.java |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | com/tencent/mm/opensdk/diffdev/a/c.java |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s | com/tencent/mm/opensdk/diffdev/a/b.java |
| https://mp.weixin.qq.com/publicpoc/opensdkconf?action=GetShareConf&appid=%s&sdkVersion=%s&buffer=%s | com/tencent/mm/opensdk/openapi/WXAPiSecurityHelper.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/l.java |
| https://aspect-upush.umeng.com/occa/v1/event/report | com/umeng/analytics/pro/aq.java |
| https://cnlogs.umeng.com/ext\_event | com/umeng/analytics/pro/aq.java |
| https://cnlogs.umeng.com/uapp\_ekverr\_logs | com/umeng/analytics/pro/aq.java |
| https://resolve.umeng.com/resolve | com/umeng/analytics/pro/by.java |
| https://ucc.umeng.com/v2/inn/fetch | com/umeng/analytics/pro/ar.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogsus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://ulogs.umengcloud.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://developer.umeng.com/docs/119267/detail/182050 | com/umeng/commonsdk/debug/UMLogCommon.java |
| https://developer.umeng.com/docs/119267/detail/118637 | com/umeng/commonsdk/debug/UMLogCommon.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://alogus.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://pslog.umeng.com | com/umeng/commonsdk/vchannel/a.java |
| https://pslog.umeng.com/ | com/umeng/commonsdk/vchannel/a.java |
| https://ccs.umeng.com/aa | com/umeng/message/proguard/m.java |
| https://sss.umeng.com/api/v2/al | com/umeng/message/proguard/m.java |
| https://offmsg.umeng.com/log/switch | com/umeng/message/proguard/p.java |
| https://yumao.puata.info/cc\_info | com/umeng/message/proguard/n.java |
| https://offmsg.umeng.com/v2/offmsg/switch | com/umeng/message/proguard/ax.java |
| https://offmsg.umeng.com/v2/offmsg/req | com/umeng/message/proguard/u.java |
| https://msg.umengcloud.com/admsg/v3/stats | com/umeng/message/proguard/aj.java |
| https://msg.umengcloud.com/admsg/v3/launch | com/umeng/message/proguard/aj.java |
| https://msg.umengcloud.com/admsg/v3/getmsg | com/umeng/message/proguard/aj.java |
| https://msg.umengcloud.com/v3/alias/delete | com/umeng/message/proguard/aa.java |
| https://msg.umengcloud.com/v3/alias/set | com/umeng/message/proguard/aa.java |
| https://msg.umengcloud.com/v3/alias | com/umeng/message/proguard/aa.java |
| https://offmsg.umeng.com/log/upload | com/umeng/message/common/UPLog.java |
| https://msg.umengcloud.com/v3/tag/add | com/umeng/message/tag/TagManager.java |
| https://msg.umengcloud.com/v3/tag/delete | com/umeng/message/tag/TagManager.java |
| https://msg.umengcloud.com/v3/tag/get | com/umeng/message/tag/TagManager.java |
| https://utoken.umeng.com | com/umeng/umzid/ZIDManager.java |
| https://audid.umeng.com/v3/a/audid/req | com/umeng/ut/a/b/g.java |
| https://errnewlog.umeng.com | com/umeng/umcrash/UMCrashContent.java |
| https://errnewlogos.umeng.com | com/umeng/umcrash/UMCrashContent.java |
| https://developer.umeng.com/docs/193624/detail/194590 | com/umeng/umcrash/UMCrash.java |
| https://errnewlog.umeng.com/upload | com/umeng/umcrash/UMCrash.java |
| https://errnewlog.umeng.com | com/umeng/umcrash/UMCrash.java |
| https://errnewlogos.umeng.com/upload | com/umeng/umcrash/UMCrash.java |
| https://errnewlogos.umeng.com | com/umeng/umcrash/UMCrash.java |
| http://www.example.com | com/pichillilorenzo/flutter\_inappwebview\_android/chrome\_custom\_tabs/CustomTabsHelper.java |
| https://errlogos.umeng.com | com/uc/crashsdk/a/d.java |
| https://errlog.umeng.com | com/uc/crashsdk/a/d.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/fg.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/fv.java |
| https://%1$s/gslb/?ver=5.0 | com/xiaomi/push/cg.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/fw.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/ew.java |
| http://10.38.162.35:9085 | com/xiaomi/push/service/q.java |
| https://cn.register.xmpush.xiaomi.com | com/xiaomi/push/service/q.java |
| https://resolver.msg.xiaomi.net/psc/?t=a | com/xiaomi/push/service/ax.java |
| http://ns.adobe.com/xap/1.0/\u0000 | f2/b.java |
| https://developer.android.com/guide/topics/permissions/overview | l9/d.java |
| http://schemas.android.com/apk/res/android | j0/n.java |
| https://docs.flutter.dev/deployment/android | x8/f.java |
| https://www.example.com | x/e.java |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md | xyz/luan/audioplayers/AudioplayersPlugin.java |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md | xyz/luan/audioplayers/player/WrappedPlayer.java |
| 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.dbankcloud.eu | 摸瓜V2引擎 |
| https://www.jsdelivr.com/using-sri-with-dynamic-files | 摸瓜V2引擎 |
| https://github.com/apvarun/toastify-js | 摸瓜V2引擎 |
| https://github.com/richtr/NoSleep.js/issues/15 | 摸瓜V2引擎 |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released) | 摸瓜V2引擎 |
| http://www.unicode.org/copyright.html | lib/arm64-v8a/libflutter.so |
| https://docs.flutter.dev/release/breaking-changes/android-surface-plugins | 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 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| appro@openssl.org | lib/arm64-v8a/libflutter.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15222222222 | xa/h.java |
| 16222222222 | xa/h.java |
| 17222222222 | xa/h.java |
| 18222222222 | xa/h.java |
| 19222222222 | xa/h.java |
| 15000000596 | 摸瓜V2引擎 |

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: ST=dangbei, L=dangbei, O=dangbei, OU=dangbei, CN=dangbei 签名算法: rsassa\_pkcs1v15 有效期自: 2019-08-30 07:33:01+00:00 有效期至: 2044-08-23 07:33:01+00:00 发行人: ST=dangbei, L=dangbei, O=dangbei, OU=dangbei, CN=dangbei 序列号: 0x4813e1c5 哈希算法: sha256 md5值: 79fa71cdf1e1f1e0f4ab37c8ff95a291 sha1值: a8aa1767b339e7ebfabd8f184e7ed4c1a3d9f80e sha256值: ffc5f19a14f0cc09ce7b0568f67cd4041270e201731be6cfd52d500b59f76727 sha512值: 89cfb171ada632a028932421fa040f12d99354c698d537ef1264d1901f175c250e1e3e206bb8295f1924c6594fd67bf48dce74ae05d1ea895a2ae16a75b44221 公钥算法: rsa 密钥长度: 2048 指纹: 156d691700379b9ef14243b7b2d9e2842365c5471f4e509afc9fbf04b66681f2**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "security\_public\_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8hzUojzHX8jDL+97pqr7CaLiKSsZ0aOES7FUcX7vh9PoEDbCKNCTakRXdS5EiurPk3QpvsAGbfyIs7JWKm4py9KcIdJsZRh9onknVeAVlU++jnrGFGEYfQb8iKzClN059gYeeJBs9mwi7RGU9tj0KHUG659v5sMBxv7zNse3fJQIDAQAB" |

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。 |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_MICROPHONE | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.dangbei.ai.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.dangbei.ai.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.dangbei.ai.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 |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.dangbei.ai.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.dangbei.ai.permission.C2D\_MESSAGE | 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 |
| com.vivo.aiengine.permission.READ\_AWARE\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.aiengine.permission.WRITE\_AWARE\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.dangbei.ai.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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 |
| 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.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.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.umeng.message.UmengOfflineMessageActivity | **Schemes**: agoo://,  **Hosts:** com.dangbei.ai,  **Paths:** /thirdpush, |
| com.dangbei.ai.MainActivity | **Schemes**: dangbei://, |

**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。**