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

**土豆密聊（ 1.0.3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 | 土豆密聊 |
| 版本 | 1.0.3 |
| 包名 | com.hmljs.cswe |
| 域名线索 | 48条 |
| URL线索 | 79条 |
| APP图标 |  |
| 分析日期 | 2025年5月4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 | 970335af49624787b5b55829bb05346f.apk |
| 文件大小 | 153.6MB |
| MD5值 | c362e548f6fd963da63c0e2a0e446ef7 |
| SHA1值 | e17a1bbd9bd316bacbb677228f47f61bcb29a94c |
| SHA256值 | e5bc38698f31e2acb5e1f91019289368bafddbeb9e45a9e02d129456f06f7804 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 土豆密聊 |
| 包名 | com.hmljs.cswe |
| 主活动Activity | com.dokiwei.module\_host.LauncherActivity |
| 安卓版本名称 | 1.0.3 |
| 安卓版本 | 4 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| apps.bytesfield-b.com | IP: 60.222.11.199  所属国家: China  地区: Shanxi  城市: Taiyuan |
| p1-lm.adkwai.com | IP: 36.248.64.7  所属国家: China  地区: Fujian  城市: Fuzhou |
| api.szshicheng.top | IP: 120.76.118.253  所属国家: China  地区: Guangdong  城市: Shenzhen |
| cloudapi.bytedance.net | IP: 10.8.7.220  所属国家: -  地区: -  城市: - |
| picupapi.tukeli.net | IP: 116.62.148.84  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| sf6-ttcdn-tos.pstatp.com | IP: 183.255.33.70  所属国家: China  地区: Hainan  城市: Haikou |
| www.szshicheng.top | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| open.e.kuaishou.com | IP: 116.136.202.194  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| aspect-upush.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| static.yximgs.com | IP: 221.194.162.226  所属国家: China  地区: Hebei  城市: Langfang |
| image.cnamedomain.com | 没有服务器地理信息. |
| www.videolan.org | IP: 213.36.253.2  所属国家: France  地区: Ile-de-France  城市: Paris |
| apis.tianapi.com | IP: 106.14.251.28  所属国家: China  地区: Shanghai  城市: Shanghai |
| lame.sf.net | IP: 104.18.20.237  所属国家: United States of America  地区: California  城市: San Francisco |
| mt.aliyuncs.com | IP: 106.11.162.170  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| style-browse-openapi.test.gifshow.com | IP: 103.102.202.41  所属国家: China  地区: Beijing  城市: Beijing |
| oss-cn-hangzhou.aliyuncs.com | IP: 118.31.219.232  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| developer.android.google.cn | IP: 114.250.69.34  所属国家: China  地区: Beijing  城市: Beijing |
| apps.samsung.com | IP: 104.17.142.17  所属国家: United States of America  地区: California  城市: San Francisco |
| oss-cn-.aliyuncs.comor | 没有服务器地理信息. |
| plbslog.umeng.com | IP: 36.156.202.68  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| pslog.umeng.com | IP: 59.82.31.210  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| schemas.android.com | 没有服务器地理信息. |
| www.baidu.com | IP: 110.242.70.57  所属国家: China  地区: Hebei  城市: Baoding |
| www.samsungapps.com | IP: 52.31.24.56  所属国家: Ireland  地区: Dublin  城市: Dublin |
| alogus.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| utoken.umeng.com | IP: 223.109.148.171  所属国家: China  地区: Jiangsu  城市: Nanjing |
| ijj-admin.ijianji.cn | IP: 42.192.80.105  所属国家: China  地区: Beijing  城市: Beijing |
| apps.bytesfield.com | IP: 60.222.11.204  所属国家: China  地区: Shanxi  城市: Taiyuan |
| apps.oceanengine.com | IP: 120.52.77.210  所属国家: China  地区: Hebei  城市: Langfang |
| alogsus.umeng.com | IP: 223.109.148.176  所属国家: China  地区: Jiangsu  城市: Nanjing |
| ulogs.umengcloud.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| greenrobot.org | IP: 85.13.163.69  所属国家: Germany  地区: Thuringen  城市: Friedersdorf |
| ios-1254945822.cos.ap-guangzhou.myqcloud.com | IP: 36.248.13.180  所属国家: China  地区: Fujian  城市: Fuzhou |
| video.54yks.cn | IP: 81.68.81.230  所属国家: China  地区: Beijing  城市: Beijing |
| oss.aliyuncs.com | IP: 118.178.29.5  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.bestkids.net | IP: 113.6.79.154  所属国家: China  地区: Heilongjiang  城市: Suihua |
| ss.bscstorage.com | IP: 101.66.255.231  所属国家: China  地区: Zhejiang  城市: Jinhua |
| ulogs.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| ucc.umeng.com | IP: 203.119.169.43  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| android.googlesource.com | IP: 108.177.98.82  所属国家: United States of America  地区: California  城市: Mountain View |
| i.snssdk.com | IP: 123.125.216.194  所属国家: China  地区: Beijing  城市: Beijing |
| developer.umeng.com | IP: 59.82.29.249  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| app.szshicheng.top | IP: 112.74.1.166  所属国家: China  地区: Guangdong  城市: Shenzhen |
| 203.107.1.1 | IP: 203.107.1.1  所属国家: China  地区: Zhejiang  城市: Hangzhou |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://ip. | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-hangzhou.aliyuncs.com | com/alibaba/sdk/android/oss/common/OSSConstants.java |
| https://203.107.1.1/181345/d?host= | com/alibaba/sdk/android/oss/common/utils/HttpdnsMini.java |
| http://oss.aliyuncs.com | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://127.0.0.1 | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/LogUtils.java |
| https://i.snssdk.com/ | com/bytedance/sdk/openadsdk/downloadnew/core/AdBaseConstants.java |
| https://cloudapi.bytedance.net/faas/services/tty8am/invoke/user\_alog\_upload | com/bytedance/tools/a/a.java |
| http://www.bestkids.net/cut-video/app/generalPolicy/autoDeductionpolicy.html? | com/dokiwei/lib\_base/PrivacyWebActivity.java |
| https://www.bestkids.net/cut-video/app/generalPolicy/purchaseInstructions.html? | com/dokiwei/lib\_base/PrivacyWebActivity.java |
| https://api.szshicheng.top/prod/ | com/dokiwei/lib\_base/adswitch/SwitchNetConstants.java |
| http://video.54yks.cn/ | com/dokiwei/lib\_base/adswitch/SwitchNetConstants.java |
| https://www.baidu.com | com/dokiwei/lib\_base/utils/download/FileDownloadUtils$client$2.java |
| https://ios-1254945822.cos.ap-guangzhou.myqcloud.com/android/request\_permission.json | com/dokiwei/lib\_base/utils/permission/OldPermissionUtils$getPermissionData$2.java |
| https://ios-1254945822.cos.ap-guangzhou.myqcloud.com/resource/ | com/dokiwei/lib\_base/constants/ModuleConstants.java |
| https://ios-1254945822.cos.ap-guangzhou.myqcloud.com/baseconfig/macfanyi2/config.json | com/dokiwei/lib\_base/translate/api/TranslateConstants.java |
| http://mt.aliyuncs.com/ | com/dokiwei/lib\_base/translate/api/TranslateConstants.java |
| https://www.bestkids.net/chatlink.html?eid=a589f0cc0aa1e64691c5dc7236279fa3&subSource=sub\_source\_2 | com/dokiwei/module\_setting/customer/CustomerServiceActivity.java |
| https://apis.tianapi.com/ | com/dokiwei/lib\_net/request/BaseTianXingRequest.java |
| https://developer.android.google.cn/reference/android/Manifest.permission?hl=zh\_cn | com/dokiwei/lib\_permission/XXPermission.java |
| https://ss.bscstorage.com/ios-web/resource/common/tiezhi2/ | com/dokiwei/module\_video\_edit/feature/StickerPage.java |
| https://api.szshicheng.top/prod | com/dokiwei/baseproject/BuildConfig.java |
| https://app.szshicheng.top/an-app/app-config/com-hmljs-cswe/HWprivacyPolicy.html | com/dokiwei/baseproject/BuildConfig.java |
| https://app.szshicheng.top/an-app/app-config/com-hmljs-cswe/HWuserPolicy.html | com/dokiwei/baseproject/BuildConfig.java |
| http://www.szshicheng.top/chatlink.html?groupid=e73db0352b48b08f58868253226b8ac9 | com/dokiwei/baseproject/BuildConfig.java |
| https:///api/v1\_test/ | com/dokiwei/baseproject/MyApplication.java |
| https:///api/v1/ | com/dokiwei/baseproject/MyApplication.java |
| https://app.szshicheng.top/an-app/app-config/com-hmljs-cswe/HWuserPolicy.html | com/dokiwei/baseproject/MyApplication.java |
| https://ios-1254945822.cos.ap-guangzhou.myqcloud.com/resource/ | com/dokiwei/module\_kaman/Constants.java |
| https://ss.bscstorage.com/ios-web/resource/common/tiezhi2/ | com/dokiwei/module\_kaman/Constants.java |
| https://picupapi.tukeli.net/api/v1/ | com/dokiwei/module\_kaman/Constants.java |
| https://ss.bscstorage.com/ios-web/resource/huashu/html/ | com/dokiwei/module\_love/utils/HuaShuRepository.java |
| https://ios-1254945822.cos.ap-guangzhou.myqcloud.com/resource/love/class\_en.json | com/dokiwei/module\_love/utils/LoveChatRepository.java |
| https://ios-1254945822.cos.ap-guangzhou.myqcloud.com/resource/love/ | com/dokiwei/module\_love/utils/LoveChatRepository.java |
| https://ios-1254945822.cos.ap-guangzhou.myqcloud.com/resource/love/class\_en.json | com/dokiwei/module\_love/utils/LoveChatRepository$getLoveChatClassifyIds$2.java |
| https://apis.tianapi.com/ | com/chenwenlv/module\_tianxing/RequestAPIUtil.java |
| https://apis.tianapi.com/ | com/chenwenlv/tianxingshuju/utils/RequestAPIUtil.java |
| http://schemas.android.com/apk/res/android | com/hjq/permissions/AndroidManifestParser.java |
| https://github.com/kongzue/DialogX/wiki | com/kongzue/dialogx/DialogX.java |
| https://github.com/kongzue/DialogX | com/kongzue/dialogx/interfaces/BaseDialog.java |
| https://github.com/kongzue/DialogX | com/kongzue/dialogx/impl/ActivityLifecycleImpl.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/tk/ks\_so-tachikomaNoSoRelease-3.3.65-d66a132dd8-547.zip | com/kwad/components/offline/c/c.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v8\_lite\_3358 | com/kwad/components/offline/c/b/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v8\_3358 | com/kwad/components/offline/c/b/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v7\_lite\_3358 | com/kwad/components/offline/c/b/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v7\_3358 | com/kwad/components/offline/c/b/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/obiwan/ks\_so-obiwanNoSoRelease-3.3.56-445ef4f109-409.zip | com/kwad/components/offline/b/b.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/adLive/ks\_so-adLiveNoSoRelease-3.3.68-9a2e5abfa5-559.zip | com/kwad/components/offline/a/b.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adLive/ks\_so-adLiveArm64v8aRelease-3.3.44.2-e8fbb3a5f8-666.apk | com/kwad/components/offline/a/a/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adLive/ks\_so-adLiveArmeabiv7aRelease-3.3.44.2-e8fbb3a5f8-666.apk | com/kwad/components/offline/a/a/a.java |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties | com/kwad/framework/filedownloader/services/a.java |
| https://style-browse-openapi.test.gifshow.com//rest/e/internal/adBrowse | com/kwad/sdk/h.java |
| https://open.e.kuaishou.com/rest/e/v3/open/sdk2 | com/kwad/sdk/api/loader/v.java |
| http://%s:%d/%s | com/kwad/sdk/core/videocache/f.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/kwad/sdk/core/videocache/h.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/kwad/sdk/core/videocache/h.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/kwad/sdk/core/videocache/h.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArm64v8aRelease-3.3.14.apk | com/kwad/sdk/collector/d.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArmeabiv7aRelease-3.3.14.apk | com/kwad/sdk/collector/d.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/exception/202406211433/ks\_so-exceptionArm64v8aRelease-3.3.67-e8fbb3a5f8-666.apk | com/kwad/sdk/crash/g.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/exception/202406211433/ks\_so-exceptionArmeabiv7aRelease-3.3.67-e8fbb3a5f8-666.apk | com/kwad/sdk/crash/g.java |
| http://apps.samsung.com/appquery/appDetail.as?appId= | com/kwad/sdk/utils/d.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/kmac/ks\_kmac64 | com/kwad/sdk/kgeo/c.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/kmac/ks\_kmac32 | com/kwad/sdk/kgeo/c.java |
| http://xml.apache.org/xslt | com/orhanobut/logger/LoggerPrinter.java |
| https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html | com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java |
| https://apps.oceanengine.com/customer/api/app/pkg\_info? | com/ss/android/downloadlib/addownload/compliance/b.java |
| https://apps.bytesfield.com | com/ss/android/downloadlib/addownload/compliance/f.java |
| https://apps.bytesfield-b.com | com/ss/android/downloadlib/addownload/compliance/f.java |
| https://www.samsungapps.com/appquery/appDetail.as?appId= | com/ss/android/downloadlib/g/h.java |
| https://i.snssdk.com/ | com/ss/android/downloadad/api/constant/AdBaseConstants.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/ap.java |
| https://ucc.umeng.com/v2/inn/fetch | com/umeng/analytics/pro/aq.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://pslog.umeng.com | com/umeng/commonsdk/vchannel/a.java |
| https://pslog.umeng.com/ | com/umeng/commonsdk/vchannel/a.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://plbslog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://alogus.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://utoken.umeng.com | com/umeng/umzid/ZIDManager.java |
| http://ijj-admin.ijianji.cn/ | com/sy/lib\_secretkey/SecretkeyUtils.java |
| https://ios-1254945822.cos.ap-guangzhou.myqcloud.com/resource/english/ | com/example/module/setting2/request/Setting2RequestUtils.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Completable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Single.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Maybe.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Observable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Flowable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Completable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Single.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Maybe.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Flowable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Observable.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/rxjava3/exceptions/UndeliverableException.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | io/reactivex/exceptions/OnErrorNotImplementedException.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/exceptions/UndeliverableException.java |
| https://greenrobot.org/greendao/documentation/database-encryption/ | org/greenrobot/greendao/database/DatabaseOpenHelper.java |
| http://lame.sf.net | lib/arm64-v8a/libavcodec.so |
| http://www.videolan.org/x264.html | lib/arm64-v8a/libavcodec.so |
| https://android.googlesource.com/toolchain/llvm-project | lib/arm64-v8a/libffmpeg-exec.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| .apk@classes.dex | com/kuaishou/weapon/p0/ac.java |
| danikula@gmail.com | com/kwad/sdk/core/videocache/h.java |
| appro@openssl.org | lib/arm64-v8a/libconscrypt\_jni.so |
| ffmpeg-devel@ffmpeg.org | lib/arm64-v8a/libffmpeg-exec.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13516237631 | com/haibin/calendarview/SolarTermUtil.java |
| 17882652114 | com/haibin/calendarview/SolarTermUtil.java |
| 18914945834 | com/haibin/calendarview/SolarTermUtil.java |
| 16832995016 | com/haibin/calendarview/SolarTermUtil.java |
| 13846158196 | com/haibin/calendarview/SolarTermUtil.java |
| 17471680261 | com/haibin/calendarview/SolarTermUtil.java |
| 18826691036 | com/haibin/calendarview/SolarTermUtil.java |
| 14159265359 | com/haibin/calendarview/SolarTermUtil.java |
| 13446589358 | com/haibin/calendarview/SolarTermUtil.java |
| 19870156017 | com/haibin/calendarview/SolarTermUtil.java |
| 19846674381 | com/haibin/calendarview/SolarTermUtil.java |
| 17387749012 | com/haibin/calendarview/SolarTermUtil.java |

## **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: C=, ST=, L=, O=, OU=, CN= 签名算法: rsassa\_pkcs1v15 有效期自: 2025-02-22 09:57:00+00:00 有效期至: 2999-11-03 09:57:00+00:00 发行人: C=, ST=, L=, O=, OU=, CN= 序列号: 0x13b72dad 哈希算法: sha256 md5值: 9285e9808ce39d3e0fb229a9b9f3e6cf sha1值: 6bedc0ce3ba86b1387f54b3529f0eaa0aa0235c1 sha256值: 2ee00b353d24b8e2596938206dccc64d21674c13796b5268c45eb19bb64da8d8 sha512值: d900b8b9cd4051e6f7ef0bc46545c8e8bbae92204d52b41e3b12722a02765ef63784510e4ad1aaf339f4a9ace1c5318211df90e847110984f84e3bccae3219a0 公钥算法: rsa 密钥长度: 2048 指纹: 018bb6d9ad4f4cc9dff5150a19fa81b1b3e95b5120098d8d4e8db544656c5c25**

## **6. 硬编码敏感信息**

## **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.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.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.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| 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.READ\_CALENDAR | 危险 | 读取日历事件 | 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.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.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| com.android.permission.GET\_INSTALLED\_APPS | 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。 |
| com.hmljs.cswe.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| com.hmljs.cswe.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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 |
| com.google.android.gms.permission.AD\_ID | 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。 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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。 |
| 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.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.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |

## **10. 应用内通信**

**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。**