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

**妈妈我还要（ 2.2.0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 | 妈妈我还要 |
| 版本 | 2.2.0 |
| 包名 | com.androidjks.dyjm.d1738653427814151707 |
| 域名线索 | 81条 |
| URL线索 | 49条 |
| APP图标 |  |
| 分析日期 | 2025年10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 | 妈妈我还要〔懒2.2.0解锁〕.apk |
| 文件大小 | 39.78MB |
| MD5值 | 38fcfa3422b7ab6630c8a969c7cdd842 |
| SHA1值 | b0d6225761f9754b17e78efa621f4cdc3e232f22 |
| SHA256值 | ef0ffc8d3fb8f5d5812946d9ad77395095af9c60c5d881de3f57b02a8cd2d356 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 妈妈我还要 |
| 包名 | com.androidjks.dyjm.d1738653427814151707 |
| 主活动Activity | com.grass.mh.SplashActivity |
| 安卓版本名称 | 2.2.0 |
| 安卓版本 | 220 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 26.26357325.vip | IP: 20.2.32.0 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| data.flurry.com | IP: 69.147.80.12 所属国家: United States of America 地区: New York 城市: New York City  |
| wsall.vipsutbgzx.work.relartemis.com | 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  |
| cs.android.com | IP: 142.251.211.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| errlogos.umeng.com | IP: 47.246.110.96 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| dk31y0i1atafx.cloudfront.net | IP: 3.166.208.197 所属国家: United States of America 地区: Washington 城市: Seattle  |
| sd21.pbgyiqmcyd.work | IP: 45.202.214.75 所属国家: United States of America 地区: Illinois 城市: Chicago  |
| jhfkdnov21vfd.yywgqhhnwl.work | IP: 149.104.32.196 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| estratxts3.ycyrv.com | IP: 220.180.243.218 所属国家: China 地区: Anhui 城市: Hefei  |
| ssimimgdyjm2.kctsjj.com | IP: 218.29.50.248 所属国家: China 地区: Henan 城市: Xinxiang  |
| exoplayer.dev | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| 7seven-7-q751.zzmxkm.com | IP: 13.94.43.97 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| pslog.umeng.com | IP: 59.82.29.249 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dfvtzhm.memto6755.top | IP: 45.144.139.238 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| offmsg.umeng.com | IP: 59.82.60.43 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| jhfkdnov21vfd.bqyidnbczy.work | IP: 156.234.246.7 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| utoken.umeng.com | IP: 223.109.148.171 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| errnewlogos.umeng.com | IP: 47.246.110.96 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| alogus.umeng.com | IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| d1r1vv8zvbqvut.cloudfront.net | IP: 52.85.39.34 所属国家: United States of America 地区: California 城市: Los Angeles  |
| alogsus.umeng.com | IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| jhfkdnov21vfd.fbfuzonigi.work | IP: 45.202.214.154 所属国家: United States of America 地区: Illinois 城市: Chicago  |
| playready.directtaps.net | IP: 104.45.231.79 所属国家: United States of America 地区: California 城市: San Francisco  |
| ccs.umeng.com | IP: 123.183.232.14 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| sd01.ligzsmntmh.work | IP: 45.202.214.154 所属国家: United States of America 地区: Illinois 城市: Chicago  |
| t.me | IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Warrington  |
| dytt01.ykawyuuomh.shop | IP: 45.202.214.75 所属国家: United States of America 地区: Illinois 城市: Chicago  |
| edgedl.me.gvt1.com | IP: 34.104.35.123 所属国家: United States of America 地区: California 城市: Mountain View  |
| sd01.ssjzfiiqzx.work | IP: 45.202.214.154 所属国家: United States of America 地区: Illinois 城市: Chicago  |
| 22634231.top | IP: 20.2.32.0 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| errlog.umeng.com | IP: 223.109.148.142 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| android.googlesource.com | IP: 142.250.107.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| mgscj.brl012.vip | IP: 20.255.108.155 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| p189asdasd.com | IP: 65.9.42.120 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| amdcopen.m.umeng.com | 没有服务器地理信息.  |
| dpcwvq4v975l1.cloudfront.net | IP: 18.164.152.215 所属国家: United States of America 地区: California 城市: Los Angeles  |
| dytt01.ujmxvftztp.shop | IP: 45.202.214.154 所属国家: United States of America 地区: Illinois 城市: Chicago  |
| yctsdyjm.ftyu4.com | IP: 39.175.123.14 所属国家: China 地区: Zhejiang 城市: Zhoushan  |
| ulogs.umeng.com | IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| code.google.com | IP: 142.251.211.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| gyutbzpm.jixingcdn.com | 没有服务器地理信息.  |
| z.zcc0241.cc | IP: 20.6.177.148 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| handsomealidyjmts1.gdfihg.com | IP: 116.172.148.37 所属国家: China 地区: Gansu 城市: Lanzhou  |
| schemas.microsoft.com | IP: 13.107.253.39 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| aspect-upush.umeng.com | IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| vvfredfd.comquot | 没有服务器地理信息.  |
| 92187327.com | IP: 156.251.151.136 所属国家: United States of America 地区: California 城市: Los Angeles  |
| www.slf4j.org | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| issuetracker.google.com | IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| umengacs.m.taobao.com | IP: 110.253.189.208 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| dev.to | IP: 151.101.194.217 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| ns.adobe.com | 没有服务器地理信息.  |
| 1372.w13721113.com | IP: 48.218.60.250 所属国家: United States of America 地区: New Jersey 城市: Newark  |
| dashif.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| sd21.ytanvntuok.work | IP: 45.202.214.75 所属国家: United States of America 地区: Illinois 城市: Chicago  |
| errnewlog.umeng.com | IP: 223.109.148.143 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| jihulab.com | IP: 111.161.122.116 所属国家: China 地区: Tianjin 城市: Tianjin  |
| d3342cdebz3lve.cloudfront.net | IP: 13.32.53.38 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| developer.umeng.com | IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| d1vsc5rj1u9oqu.cloudfront.net | IP: 18.172.50.202 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| schemas.android.com | 没有服务器地理信息.  |
| aussdajx.xxkglea285129.top | IP: 154.198.225.123 所属国家: United States of America 地区: California 城市: Los Angeles  |
| txaw2dyjmtsyn.gbrgz.com | IP: 218.29.50.248 所属国家: China 地区: Henan 城市: Xinxiang  |
| msg.umengcloud.com | IP: 124.239.14.132 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| ycimgdyjm1.xmycds.com | IP: 39.174.97.18 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| plbslog.umeng.com | IP: 36.156.202.68 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| zhdyjm.zoncvbmihc.shop | IP: 3.169.5.107 所属国家: United States of America 地区: Washington 城市: Seattle  |
| ucc.umeng.com | IP: 203.119.169.41 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| sd01.glwbkbeikq.work | IP: 45.202.214.154 所属国家: United States of America 地区: Illinois 城市: Chicago  |
| sss.umeng.com | IP: 59.82.29.248 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| m.vipsutbgzx.work | IP: 156.234.246.7 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| sd21.ghanyvfeof.work | IP: 45.202.214.154 所属国家: United States of America 地区: Illinois 城市: Chicago  |
| taotao.cdn.wafsudun.com | IP: 45.202.215.154 所属国家: United States of America 地区: Illinois 城市: Chicago  |
| gist.github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| xmguzu.vipsutbgzx.work | IP: 43.252.173.36 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| jhfkdnov21vfd.alxvjynbzl.work | IP: 45.202.214.75 所属国家: United States of America 地区: Illinois 城市: Chicago  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| audid.umeng.com | IP: 36.143.252.104 所属国家: China 地区: Beijing 城市: Beijing  |
| clsp.fun | IP: 143.92.53.203 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | b/j/b/b/e.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | b/n/a/a.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/mp3cache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/danikula/mp3cache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/danikula/mp3cache/HttpUrlSource.java  |
| http://%s:%d/%s  | com/danikula/mp3cache/Pinger.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/danikula/mp3cache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/mp3cache/HttpProxyCacheServer.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/danikula/videocache/HttpUrlSource.java  |
| http://%s:%d/%s  | com/danikula/videocache/Pinger.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/danikula/videocache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/videocache/HttpProxyCacheServer.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  |
| https://dytt01.ujmxvftztp.shop  | com/grass/mh/SplashActivity.java  |
| https://dytt01.ykawyuuomh.shop  | com/grass/mh/SplashActivity.java  |
| https://dpcwvq4v975l1.cloudfront.net/dyjm\_ldy.json  | com/grass/mh/SplashActivity.java  |
| https://d1r1vv8zvbqvut.cloudfront.net/dyjm.json  | com/grass/mh/SplashActivity.java  |
| https://d3342cdebz3lve.cloudfront.net/dyjm.json  | com/grass/mh/SplashActivity.java  |
| https://clsp.fun  | com/grass/mh/databinding/ActivityShareLayoutBindingImpl.java  |
| https://errlogos.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlog.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://aspect-upush.umeng.com/occa/v1/event/report  | com/umeng/analytics/pro/ap.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/l.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://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://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.java  |
| https://offmsg.umeng.com/log/upload  | com/umeng/message/common/UPLog.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://msg.umengcloud.com/v3/tag/add  | com/umeng/message/proguard/bd.java  |
| https://msg.umengcloud.com/v3/tag/delete  | com/umeng/message/proguard/bd.java  |
| https://msg.umengcloud.com/v3/tag/get  | com/umeng/message/proguard/bd.java  |
| https://offmsg.umeng.com/v2/offmsg/switch  | com/umeng/message/proguard/aw.java  |
| https://offmsg.umeng.com/v2/offmsg/req  | com/umeng/message/proguard/t.java  |
| https://msg.umengcloud.com/admsg/v3/stats  | com/umeng/message/proguard/ai.java  |
| https://msg.umengcloud.com/admsg/v3/launch  | com/umeng/message/proguard/ai.java  |
| https://msg.umengcloud.com/admsg/v3/getmsg  | com/umeng/message/proguard/ai.java  |
| https://offmsg.umeng.com/log/switch  | com/umeng/message/proguard/p.java  |
| https://msg.umengcloud.com/v3/alias/set  | com/umeng/message/proguard/z.java  |
| https://msg.umengcloud.com/v3/alias/delete  | com/umeng/message/proguard/z.java  |
| https://msg.umengcloud.com/v3/alias  | com/umeng/message/proguard/z.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://errnewlogos.umeng.com/upload  | com/umeng/umcrash/UMCrash.java  |
| https://errnewlogos.umeng.com  | 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://utoken.umeng.com  | com/umeng/umzid/ZIDManager.java  |
| https://data.flurry.com/aap.do  | e/h/b/s0.java  |
| https://data.flurry.com/v1/flr.do  | e/h/b/t0.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | e/i/a/a/t0.java  |
| http://dashif.org/guidelines/last-segment-number  | e/i/a/a/h1/j0/j/c.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  |
| http://www.slf4j.org/codes.html  | l/e/c.java  |
| http://schemas.android.com/apk/res/android  | m/a/a/f.java  |
| http://schemas.android.com/apk/res/android  | org/dsq/library/widget/tablayout/SegmentTabLayout.java  |
| http://schemas.android.com/apk/res/android  | org/dsq/library/widget/tablayout/CommonTabLayout.java  |
| http://schemas.android.com/apk/res/android  | org/dsq/library/widget/tablayout/SlidingTabLayout.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.java  |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |
| https://gist.github.com/cypressious/91c4fb1455470d803a602838dfcd5774  | 摸瓜V3引擎  |
| https://sd21.pbgyiqmcyd.work/dyjm-15&quot;  | 摸瓜V3引擎  |
| https://github.com/square/leakcanary/issues/177  | 摸瓜V3引擎  |
| https://vvfredfd.com&quot;  | 摸瓜V3引擎  |
| https://github.com/android/platform\_frameworks\_base/commit/9b5257c9c99c4cb541d8e8e78fb04f008b1a9091  | 摸瓜V3引擎  |
| https://alogus.umeng.com  | 摸瓜V3引擎  |
| https://errnewlogos.umeng.com/upload  | 摸瓜V3引擎  |
| data.flurry.com  | 摸瓜V3引擎  |
| https://msg.umengcloud.com/v3/tag/add  | 摸瓜V3引擎  |
| wsall.vipsutbgzx.work.relartemis.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android((layout/activity\_usercenter\_reward\_list\_0  | 摸瓜V3引擎  |
| https://d1vsc5rj1u9oqu.cloudfront.net/xvhh001&quot;  | 摸瓜V3引擎  |
| http://www.slf4j.org/codes.html#StaticLoggerBinder  | 摸瓜V3引擎  |
| https://7seven-7-q751.zzmxkm.com/a970.html&quot;  | 摸瓜V3引擎  |
| jhfkdnov21vfd.yywgqhhnwl.work  | 摸瓜V3引擎  |
| https://msg.umengcloud.com/admsg/v3/getmsg  | 摸瓜V3引擎  |
| estratxts3.ycyrv.com  | 摸瓜V3引擎  |
| ssimimgdyjm2.kctsjj.com  | 摸瓜V3引擎  |
| https://sd21.pbgyiqmcyd.work/dyjm-47&quot;  | 摸瓜V3引擎  |
| https://clsp.fun  | 摸瓜V3引擎  |
| http://httpsfastopenijkapplicationLavf/57.83.100the  | 摸瓜V3引擎  |
| https://ucc.umeng.com/v2/inn/fetch  | 摸瓜V3引擎  |
| https://errnewlog.umeng.com/api/crashsdk/logcollect  | 摸瓜V3引擎  |
| jhfkdnov21vfd.bqyidnbczy.work  | 摸瓜V3引擎  |
| https://sd21.pbgyiqmcyd.work/dyjm-37&quot;  | 摸瓜V3引擎  |
| https://sd21.pbgyiqmcyd.work/dyjm-44&quot;  | 摸瓜V3引擎  |
| https://sd01.ligzsmntmh.work/dyjm-6&quot;  | 摸瓜V3引擎  |
| https://1372.w13721113.com/?cid  | 摸瓜V3引擎  |
| utoken.umeng.com  | 摸瓜V3引擎  |
| https://developer.umeng.com/docs/119267/detail/182050  | 摸瓜V3引擎  |
| https://t.me/dada166&quot;  | 摸瓜V3引擎  |
| https://sd21.ghanyvfeof.work/dyjm-35&quot;  | 摸瓜V3引擎  |
| https://dfvtzhm.memto6755.top:39006/3\_medp/mdp1/158898.csv?mlm583&quot;  | 摸瓜V3引擎  |
| https://utoken.umeng.com  | 摸瓜V3引擎  |
| https://github.com/android/platform\_frameworks\_base/commit/af7dcdf35a37d7a7dbaad7d9869c1c91bce2272b  | 摸瓜V3引擎  |
| https://errnewlog.umeng.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android&&layout/fragment\_blogger\_collec\_index\_0  | 摸瓜V3引擎  |
| https://offmsg.umeng.com/log/upload  | 摸瓜V3引擎  |
| jhfkdnov21vfd.fbfuzonigi.work  | 摸瓜V3引擎  |
| https://mgscj.brl012.vip:8620/mg/mg68.html?channelCode  | 摸瓜V3引擎  |
| https://github.com/android/platform\_frameworks\_base/commit/893d6fe48d37f71e683f722457bea646994a10  | 摸瓜V3引擎  |
| https://sd01.ligzsmntmh.work/dyjm-13&quot;  | 摸瓜V3引擎  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | 摸瓜V3引擎  |
| https://sd21.pbgyiqmcyd.work/dyjm-11&quot;  | 摸瓜V3引擎  |
| https://sd21.ytanvntuok.work/dyjm-48&quot;  | 摸瓜V3引擎  |
| https://dev.to/pyricau/beware-packagemanager-leaks-223g  | 摸瓜V3引擎  |
| https://ulogs.umeng.com  | 摸瓜V3引擎  |
| https://data.flurry.com/v1/flr.do  | 摸瓜V3引擎  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | 摸瓜V3引擎  |
| https://aspect-upush.umeng.com/occa/v1/event/report  | 摸瓜V3引擎  |
| https://26.26357325.vip/?cid  | 摸瓜V3引擎  |
| https://data.flurry.com/aap.do  | 摸瓜V3引擎  |
| https://errnewlogos.umeng.com/api/crashsdk/logcollect  | 摸瓜V3引擎  |
| https://22634231.top/my/445.html?channelCode  | 摸瓜V3引擎  |
| https://msg.umengcloud.com/v3/tag/delete  | 摸瓜V3引擎  |
| edgedl.me.gvt1.com  | 摸瓜V3引擎  |
| https://92187327.com/?channelCode  | 摸瓜V3引擎  |
| https://d3342cdebz3lve.cloudfront.net/dyjm.json  | 摸瓜V3引擎  |
| https://github.com/square/leakcanary/issues/32  | 摸瓜V3引擎  |
| https://sd01.glwbkbeikq.work/dyjm-41&quot;  | 摸瓜V3引擎  |
| https://z.zcc0241.cc:8443/?shareName  | 摸瓜V3引擎  |
| amdcopen.m.umeng.com  | 摸瓜V3引擎  |
| https://sd21.ghanyvfeof.work/dyjm-4400&quot;  | 摸瓜V3引擎  |
| https://sd01.glwbkbeikq.work/dyjm-2&quot;  | 摸瓜V3引擎  |
| https://sd01.ligzsmntmh.work/dyjm-9&quot;  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android$$layout/activity\_chat\_square\_search\_0  | 摸瓜V3引擎  |
| yctsdyjm.ftyu4.com  | 摸瓜V3引擎  |
| https://msg.umengcloud.com/v3/tag/get  | 摸瓜V3引擎  |
| https://errnewlog.umeng.com/upload  | 摸瓜V3引擎  |
| https://dytt01.ykawyuuomh.shop  | 摸瓜V3引擎  |
| https://gist.github.com/andaag/b05ab66ed0f06167d6e0  | 摸瓜V3引擎  |
| ulogs.umeng.com  | 摸瓜V3引擎  |
| https://aussdajx.xxkglea285129.top:57009/1\_xxzb/et.htm?yxo332&quot;  | 摸瓜V3引擎  |
| https://github.com/android/platform\_frameworks\_base/commit/e0bef71662d81caaaa0d7214fb0bef5d39996a69  | 摸瓜V3引擎  |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx  | 摸瓜V3引擎  |
| https://github.com/square/leakcanary/issues/696#issuecomment-296420756  | 摸瓜V3引擎  |
| gyutbzpm.jixingcdn.com  | 摸瓜V3引擎  |
| https://offmsg.umeng.com/v2/offmsg/req  | 摸瓜V3引擎  |
| https://dk31y0i1atafx.cloudfront.net/pphh001&quot;  | 摸瓜V3引擎  |
| https://github.com/android/platform\_frameworks\_base/commit  | 摸瓜V3引擎  |
| handsomealidyjmts1.gdfihg.com  | 摸瓜V3引擎  |
| https://sd01.glwbkbeikq.work/dyjm-4900&quot;  | 摸瓜V3引擎  |
| https://developer.umeng.com/docs/119267/detail/118637#3091c7c11fx3q  | 摸瓜V3引擎  |
| https://sd01.ssjzfiiqzx.work/dyjm-45&quot;  | 摸瓜V3引擎  |
| umengacs.m.taobao.com  | 摸瓜V3引擎  |
| https://developer.umeng.com/docs/193624/detail/194590#h2-n5n-d0l-fmj  | 摸瓜V3引擎  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | 摸瓜V3引擎  |
| https://github.com/square/leakcanary/issues/1#issuecomment-100579429  | 摸瓜V3引擎  |
| http://www.slf4j.org/codes.html#multiple\_bindings  | 摸瓜V3引擎  |
| errnewlog.umeng.com  | 摸瓜V3引擎  |
| jihulab.com  | 摸瓜V3引擎  |
| https://sd01.ssjzfiiqzx.work/dyjm-49&quot;  | 摸瓜V3引擎  |
| https://github.com/square/leakcanary/issues/1819  | 摸瓜V3引擎  |
| https://github.com/android/platform\_frameworks\_base/commit/b3a9bc038d3a218b1dbdf7b5668e3d6c12be5e  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android--layout/include\_connotation\_details\_top\_view\_0  | 摸瓜V3引擎  |
| txaw2dyjmtsyn.gbrgz.com  | 摸瓜V3引擎  |
| ycimgdyjm1.xmycds.com  | 摸瓜V3引擎  |
| https://gist.github.com/jankovd/a210460b814c04d500eb12025902d60d  | 摸瓜V3引擎  |
| https://sd21.ghanyvfeof.work/dyjm-42&quot;  | 摸瓜V3引擎  |
| zhdyjm.zoncvbmihc.shop  | 摸瓜V3引擎  |
| https://ycimgdyjm1.xmycds.com/&quot;  | 摸瓜V3引擎  |
| https://sd21.pbgyiqmcyd.work/dyjm-14&quot;  | 摸瓜V3引擎  |
| https://sd21.pbgyiqmcyd.work/dyjm-27&quot;  | 摸瓜V3引擎  |
| ucc.umeng.com  | 摸瓜V3引擎  |
| https://github.com/danikula/AndroidVideoCache/issues.  | 摸瓜V3引擎  |
| https://github.com/android/platform\_frameworks\_base/commit/7a96f3c917e0001ee739b65da37b2fadec7d7765  | 摸瓜V3引擎  |
| https://offmsg.umeng.com/v2/offmsg/switch  | 摸瓜V3引擎  |
| m.vipsutbgzx.work  | 摸瓜V3引擎  |
| https://sd01.glwbkbeikq.work/dyjm-30&quot;  | 摸瓜V3引擎  |
| https://XmgUZu.vipsutbgzx.work  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android$$org.dsq.library.widget.ShapeTextView  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android))layout/activity\_choose\_collection\_index\_0  | 摸瓜V3引擎  |
| https://cs.android.com/android/\_/android/platform/frameworks/base/  | 摸瓜V3引擎  |
| taotao.cdn.wafsudun.com  | 摸瓜V3引擎  |
| https://sd21.pbgyiqmcyd.work/dyjm-7&quot;  | 摸瓜V3引擎  |
| https://sd21.ytanvntuok.work/dyjm-19&quot;  | 摸瓜V3引擎  |
| xmguzu.vipsutbgzx.work  | 摸瓜V3引擎  |
| https://sd01.ligzsmntmh.work/dyjm-51&quot;  | 摸瓜V3引擎  |
| jhfkdnov21vfd.alxvjynbzl.work  | 摸瓜V3引擎  |
| https://sd01.glwbkbeikq.work/dyjm-33&quot;  | 摸瓜V3引擎  |
| https://dpcwvq4v975l1.cloudfront.net/dyjm\_ldy.json  | 摸瓜V3引擎  |
| https://gist.github.com/jankovd/891d96f476f7a9ce24e2  | 摸瓜V3引擎  |
| https://p189asdasd.com/yj/30678/oshpz1soul&quot;  | 摸瓜V3引擎  |
| audid.umeng.com  | 摸瓜V3引擎  |
| http://www.slf4j.org/codes.html#substituteLogger  | 摸瓜V3引擎  |
| https://developer.umeng.com/docs/66632/detail/  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | com/danikula/mp3cache/HttpUrlSource.java  |
| danikula@gmail.com  | com/danikula/videocache/HttpUrlSource.java  |
| dyjm2016@gmail.com  | com/grass/mh/ui/mine/activity/LoginActivity.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17246994432  | com/grass/mh/databinding/FragmentElegantDetailInfoBindingImpl.java  |
| 17246978048  | com/grass/mh/databinding/FragmentElegantDetailInfoBindingImpl.java  |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 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: C=CN 签名算法: rsassa\_pkcs1v15 有效期自: 2024-04-12 00:49:21+00:00 有效期至: 2049-04-06 00:49:21+00:00 发行人: C=CN 序列号: 0x583488cd 哈希算法: sha256 md5值: ecdfc654ae638d857d64ccd488db9bcb sha1值: 8216459ad94fb552d07491ec6a819bf7322c308c sha256值: df740279934ad9f3032ccf4e31212f93559eac09cd23c2959fbc6fc404950d3a sha512值: b5471766b9e78f8abc4a5c2dd657304b9d195982e54f502cd6fbef259881126091e1ad4651346c0ce3a2103bd2d55552d4cf5dc261e51c0d7419cc74f264dd7a 公钥算法: rsa 密钥长度: 2048 指纹: bbb32c475b78efc58fa1e901324e3d98f9f41c98e07349694aa6b54276cb911e**

## **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.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.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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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\_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.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.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.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| 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.READ\_PRIVILEGED\_PHONE\_STATE | 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.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 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 |

## **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。**