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

**特狗APP（ 3.2.2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 | 特狗APP |
| 版本 | 3.2.2 |
| 包名 | com.ybyx.app.euun |
| 域名线索 | 80条 |
| URL线索 | 71条 |
| APP图标 |  |
| 分析日期 | 2025年6月27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 | 7f28c0e1d25e4f8db037acb6c9475c26.apk |
| 文件大小 | 49.33MB |
| MD5值 | 080f8ad61c4ac006191118a59ddda15f |
| SHA1值 | a1553b26f27a12b3832185a3136670769392f648 |
| SHA256值 | 7861a69d1a46882fce42ceeb55609cda09f771551114605ed97639e9616d367b |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 特狗APP |
| 包名 | com.ybyx.app.euun |
| 主活动Activity | com.ybyx.app.euun.MainActivity |
| 安卓版本名称 | 3.2.2 |
| 安卓版本 | 3202 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| alogus.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| p1-lm.adkwai.com | IP: 116.162.153.201 所属国家: China 地区: Hunan 城市: Loudi  |
| www.csjplatform.com | IP: 42.56.65.69 所属国家: China 地区: Liaoning 城市: Shenyang  |
| changemaker.hzsanjiaomao.com | IP: 82.157.26.175 所属国家: China 地区: Beijing 城市: Beijing  |
| api.spstmind.com | IP: 101.37.255.98 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| sf6-ttcdn-tos.pstatp.com | IP: 183.255.33.70 所属国家: China 地区: Hainan 城市: Haikou  |
| ouplog.umeng.com | IP: 47.246.110.93 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| adservice.sigmob.cn | IP: 101.200.125.221 所属国家: China 地区: Beijing 城市: Beijing  |
| webaddress.elided | 没有服务器地理信息.  |
| gist.github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| ulogs.umengcloud.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| ad.shunchangzhixing.com | IP: 123.249.106.132 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.iana.org | IP: 192.0.33.8 所属国家: United States of America 地区: California 城市: El Segundo  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| tdid.m.qq.com | IP: 60.29.240.40 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.ascc.net | IP: 140.109.4.18 所属国家: Taiwan (Province of China) 地区: Taipei 城市: Taipei  |
| curl.haxx.se | IP: 151.101.90.49 所属国家: United States of America 地区: California 城市: San Francisco  |
| plbslog.umeng.com | IP: 36.156.202.73 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| p2-lm.adkwai.com | IP: 221.194.162.229 所属国家: China 地区: Hebei 城市: Langfang  |
| sdk.beizi.biz | IP: 59.110.4.153 所属国家: China 地区: Beijing 城市: Beijing  |
| apps.bytesfield-b.com | IP: 116.196.143.222 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| apmplus.volces.com | IP: 101.26.38.241 所属国家: China 地区: Hebei 城市: Handan  |
| app.chuangjing.com | IP: 123.125.244.81 所属国家: China 地区: Beijing 城市: Beijing  |
| static.yximgs.com | IP: 221.194.162.225 所属国家: China 地区: Hebei 城市: Langfang  |
| play.google.com | IP: 59.24.3.174 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam  |
| cpro.baidustatic.com | IP: 101.72.203.38 所属国家: China 地区: Hebei 城市: Langfang  |
| apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| sdk.spstmind.com | IP: 61.48.83.230 所属国家: China 地区: Beijing 城市: Beijing  |
| www.oasis-open.org | IP: 172.99.100.168 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| js-ad.a.yximgs.com | IP: 221.195.228.1 所属国家: China 地区: Hebei 城市: Cangzhou  |
| schemas.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| purl.org | IP: 207.241.225.157 所属国家: United States of America 地区: California 城市: San Francisco  |
| c.tobidad.cn | IP: 39.96.185.90 所属国家: China 地区: Beijing 城市: Beijing  |
| relaxng.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.google.com | IP: 199.16.158.182 所属国家: United States of America 地区: California 城市: San Francisco  |
| cpu.baidu.com | IP: 153.3.238.225 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  |
| d.alipay.com | IP: 116.142.234.146 所属国家: China 地区: Beijing 城市: Beijing  |
| i.snssdk.com | IP: 111.202.5.199 所属国家: China 地区: Beijing 城市: Beijing  |
| passport.kuaishou.com | IP: 103.107.217.66 所属国家: China 地区: Beijing 城市: Beijing  |
| ulogs.umeng.com.gds.alibabadns.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| mobads-logs.baidu.com | IP: 153.3.237.160 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| apps.samsung.com | IP: 104.17.142.17 所属国家: United States of America 地区: California 城市: San Francisco  |
| p5-lm.adkwai.com | IP: 123.117.132.41 所属国家: China 地区: Beijing 城市: Beijing  |
| glassfish.dev.java.net | IP: 137.254.56.48 所属国家: United States of America 地区: California 城市: Belmont  |
| developer.umeng.com | IP: 59.82.31.95 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mobads.baidu.com | IP: 111.206.208.180 所属国家: China 地区: Beijing 城市: Beijing  |
| c.etoolads.cn | IP: 39.96.184.178 所属国家: China 地区: Beijing 城市: Beijing  |
| www.sec.co.kr | IP: 112.106.187.200 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul  |
| www.dbunit.org | IP: 74.220.199.51 所属国家: United States of America 地区: Utah 城市: Provo  |
| aaid.umeng.com | IP: 223.109.148.139 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| adxtool.sigmob.cn | IP: 39.106.166.112 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| gcc.gnu.org | IP: 8.43.85.97 所属国家: United States of America 地区: North Carolina 城市: Raleigh  |
| developer.android.com | IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| schemas.xmlsoap.org | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| www.rfc-editor.org | IP: 104.22.50.131 所属国家: United States of America 地区: California 城市: San Francisco  |
| style-browse-openapi.test.gifshow.com | IP: 103.102.202.41 所属国家: China 地区: Beijing 城市: Beijing  |
| purl.oclc.org | IP: 207.241.225.157 所属国家: United States of America 地区: California 城市: San Francisco  |
| msg.cmpassport.com | IP: 112.33.111.188 所属国家: China 地区: Anhui 城市: Hefei  |
| open.e.kuaishou.com | IP: 116.136.202.194 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| alogus.umeng.com.gds.alibabadns.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| n.sigmob.cn | IP: 116.196.144.147 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| dc.sigmob.cn | IP: 47.94.5.41 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mobads-pre-config.cdn.bcebos.com | IP: 123.117.132.38 所属国家: China 地区: Beijing 城市: Beijing  |
| pslog.umeng.com | IP: 59.82.112.112 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mobads-pre-config.bj.bcebos.com | IP: 113.200.2.111 所属国家: China 地区: Shaanxi 城市: Yulin  |
| www.samsungapps.com | IP: 52.31.24.56 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| api.ipify.org | IP: 104.26.13.205 所属国家: United States of America 地区: California 城市: San Francisco  |
| apps.bytesfield.com | IP: 175.19.126.232 所属国家: China 地区: Jilin 城市: Changchun  |
| ulogs.umeng.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| sdk.hzsanjiaomao.com | IP: 60.222.116.105 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| java.sun.com | IP: 23.214.168.202 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| union.baidu.com | IP: 111.206.208.169 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  |
| apps.oceanengine.com | IP: 60.222.11.201 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| inner.shunchangzhixing.com | IP: 120.46.3.232 所属国家: China 地区: Guangdong 城市: Guangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://d.alipay.com  | a2/a.java  |
| https://ad.shunchangzhixing.com  | cn/hzjizhun/admin/api/ApiManager.java  |
| https://inner.shunchangzhixing.com  | cn/hzjizhun/admin/api/ApiManager.java  |
| https://ad.shunchangzhixing.com/base/  | cn/hzjizhun/admin/api/ApiManager.java  |
| http://inner.shunchangzhixing.com  | cn/hzjizhun/admin/base/z.java  |
| https://cpro.baidustatic.com/cpro/logo/sdk/mob-adIcon\_2x.png  | com/baidu/mobads/sdk/api/XAdNativeResponse.java  |
| https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png  | com/baidu/mobads/sdk/api/XAdNativeResponse.java  |
| https://union.baidu.com/  | com/baidu/mobads/sdk/api/XAdNativeResponse.java  |
| https://cpro.baidustatic.com/cpro/logo/sdk/mob-adIcon\_2x.png  | com/baidu/mobads/sdk/api/XAdEntryResponse.java  |
| https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png  | com/baidu/mobads/sdk/api/XAdEntryResponse.java  |
| https://union.baidu.com/  | com/baidu/mobads/sdk/api/XAdEntryResponse.java  |
| https://union.baidu.com  | com/baidu/mobads/sdk/internal/ap.java  |
| https://i.snssdk.com/  | com/bytedance/sdk/openadsdk/downloadnew/core/AdBaseConstants.java  |
| https://dc.sigmob.cn/log  | com/czhj/sdk/common/models/Config.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_3.webp  | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_2.webp  | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_1.webp  | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_4.webp  | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_0.webp  | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_limit\_error.png  | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_video\_img.png  | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_error.png  | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_data\_img.png  | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/wallpaper/kwai\_wallpaper\_plugin\_1.4.apk  | com/kwad/components/ct/wallpaper/d/b.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/wallpaper/kwai\_wallpaper\_plugin\_1.5.apk  | com/kwad/components/ct/wallpaper/d/b.java  |
| https://js-ad.a.yximgs.com/kos/nlav10933/ksad\_profile\_header\_bg.png  | com/kwad/components/ct/profile/home/c/c.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_limit\_error.png  | com/kwad/components/ct/widget/KSPageLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_video\_img.png  | com/kwad/components/ct/widget/KSPageLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_error.png  | com/kwad/components/ct/widget/KSPageLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_data\_img.png  | com/kwad/components/ct/widget/KSPageLoadingView.java  |
| https://passport.kuaishou.com/account-h5/login?smallWebview=true&sid=kuaishou.unioncontent.wallpaper  | com/kwad/components/ct/c/a.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-webpArm64v8aRelease-3.3.9-e8fbb3a5f8-666.apk  | com/kwad/components/ct/b/c.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-webpArmeabiv7aRelease-3.3.9-e8fbb3a5f8-666.apk  | com/kwad/components/ct/b/c.java  |
| https://p5-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/tk/ks\_so-tachikomaNoSoRelease-3.3.76.2-6e49205f15-618.zip  | com/kwad/components/offline/d/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/d/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/d/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/d/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/d/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/c/b.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/adWaynePlayer/ks\_so-adWaynePlayerNoSoRelease-3.3.76-bab2e13fb8-62.zip  | com/kwad/components/offline/b/b.java  |
| https://p2-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adWaynePlayer/ks\_so-adWaynePlayerArm64v8aRelease-3.3.76-e8fbb3a5f8-666.apk  | com/kwad/components/offline/b/a/a.java  |
| https://p2-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adWaynePlayer/ks\_so-adWaynePlayerArmeabiv7aRelease-3.3.76-e8fbb3a5f8-666.apk  | com/kwad/components/offline/b/a/a.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/adLive/ks\_so-adLiveNoSoRelease-3.3.76-089e702802-65.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://msg.cmpassport.com/h5/uaidAdGetMobile  | com/kwad/sdk/h.java  |
| https://open.e.kuaishou.com/rest/e/v3/open/sdk2  | com/kwad/sdk/api/loader/v.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/ks\_so-kwaiPlayerArm64v8aRelease-3.3.44-e8fbb3a5f8-666.apk  | com/kwad/sdk/core/video/a/e.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/ks\_so-kwaiPlayerArmeabiv7aRelease-3.3.44-e8fbb3a5f8-666.apk  | com/kwad/sdk/core/video/a/e.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/e.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  |
| https://play.google.com/  | com/mbridge/msdk/foundation/tools/aj.java  |
| https://play.google.com/store/apps/details?id=  | com/mbridge/msdk/foundation/tools/aj.java  |
| https://play.google.com/store/apps/details?id=  | com/mbridge/msdk/foundation/webview/a.java  |
| http://whatwg.org/html/common-microsyntaxes.html  | com/mbridge/msdk/c/b/c.java  |
| http://whatwg.org/html/webappapis.html  | com/mbridge/msdk/c/b/c.java  |
| https://gist.github.com/atk/1020396\n  | com/mbridge/msdk/c/b/c.java  |
| http://whatwg.org/C  | com/mbridge/msdk/c/b/c.java  |
| https://play.google.com  | com/mbridge/msdk/mbsignalcommon/windvane/WindVaneWebView.java  |
| https://play.google.com/  | com/mbridge/msdk/click/b.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | com/mbridge/msdk/playercommon/exoplayer2/drm/HttpMediaDrmCallback.java  |
| https://c.etoolads.cn/s/config  | com/sigmob/sdk/base/l.java  |
| https://adservice.sigmob.cn/s/config  | com/sigmob/sdk/base/l.java  |
| https://adservice.sigmob.cn/s/config?  | com/sigmob/sdk/base/l.java  |
| https://adservice.sigmob.cn/extconfig?  | com/sigmob/sdk/base/l.java  |
| https://dc.sigmob.cn/log  | com/sigmob/sdk/base/l.java  |
| https://adxtool.sigmob.cn/debug/feedback  | com/sigmob/sdk/base/l.java  |
| https://adservice.sigmob.cn/ad/v4  | com/sigmob/sdk/base/l.java  |
| https://adservice.sigmob.cn/hb/v2/ad  | com/sigmob/sdk/base/l.java  |
| https://appassets/android\_asset/sig\_appelements.html  | com/sigmob/sdk/base/views/q.java  |
| http://%s:%d/%s  | com/sigmob/sdk/videocache/n.java  |
| http://%s:%d/%s  | com/sigmob/sdk/videocache/h.java  |
| https://www.samsungapps.com/appquery/appDetail.as?appId=  | com/ss/android/downloadlib/g/h.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://i.snssdk.com/  | com/ss/android/downloadad/api/constant/AdBaseConstants.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/j.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://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://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ouplog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://aaid.umeng.com/api/updateZdata  | com/umeng/umzid/ZIDManager.java  |
| https://aaid.umeng.com/api/postZdata  | com/umeng/umzid/ZIDManager.java  |
| https://adservice.sigmob.cn/w/config  | com/windmill/sdk/strategy/WMSdkConfig.java  |
| https://c.tobidad.cn/w/config  | com/windmill/sdk/strategy/WMSdkConfig.java  |
| https://adservice.sigmob.cn/extconfig?  | com/windmill/sdk/strategy/WMSdkConfig.java  |
| https://adservice.sigmob.cn/strategy/v6  | com/windmill/sdk/strategy/WMSdkConfig.java  |
| https://adservice.sigmob.cn/waterfall/v1  | com/windmill/sdk/strategy/WMSdkConfig.java  |
| https://dc.sigmob.cn/log  | com/windmill/sdk/strategy/WMSdkConfig.java  |
| https://c.tobidad.cn/w/config?  | com/windmill/sdk/strategy/WMSdkConfig.java  |
| https://adservice.sigmob.cn/w/config?  | com/windmill/sdk/strategy/WMSdkConfig.java  |
| http://purl.org/dc/elements/1.1/\  | com/xht/flutter/flutter\_dlna/screening/DLNAPlayer.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| http://api.spstmind.com/api/staEvent  | j2/d.java  |
| http://sdk.spstmind.com/sjmconfig/%s\_e.json  | m3/c.java  |
| http://schemas.xmlsoap.org/soap/envelope/  | org/fourthline/cling/transport/impl/o.java  |
| http://schemas.xmlsoap.org/soap/encoding/  | org/fourthline/cling/transport/impl/o.java  |
| http://www.dbunit.org/properties/datatypeFactory  | org/seamless/util/dbunit/H2DBUnitOperations.java  |
| http://xml.org/sax/features/external-general-entities  | org/seamless/xml/SAXParser.java  |
| http://xml.org/sax/features/external-parameter-entities  | org/seamless/xml/SAXParser.java  |
| http://apache.org/xml/features/disallow-doctype-decl  | org/seamless/xml/SAXParser.java  |
| https://d.alipay.com  | q3/b.java  |
| https://api.ipify.org  | w1/f.java  |
| http://xml.org/sax/features/external-general-entities  | n4/a.java  |
| http://xml.org/sax/features/external-parameter-entities  | n4/a.java  |
| http://www.sec.co.kr/dlna  | c6/d.java  |
| https://ad.shunchangzhixing.com  | i/c.java  |
| https://ad.shunchangzhixing.com/keenValue/  | i/c.java  |
| http://changemaker.hzsanjiaomao.com:6688/105009  | l1/a.java  |
| http://sdk.hzsanjiaomao.com/sspconfig/%s.txt  | l1/a.java  |
| http://www.google.com  | y1/a.java  |
| http://www.google.com?  | y1/a.java  |
| alogus.umeng.com  | 摸瓜V3引擎  |
| https://js-ad.a.yximgs.com/kos/nlav10933/ksad\_profile\_header\_bg.png  | 摸瓜V3引擎  |
| https://apmplus.volces.com/apm/collect/crash  | 摸瓜V3引擎  |
| http://gcc.gnu.org/bugs.html):  | 摸瓜V3引擎  |
| https://cpu.baidu.com/  | 摸瓜V3引擎  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/obiwan/ks\_so-obiwanNoSoRele  | 摸瓜V3引擎  |
| http://relaxng.org/ns/structure/1.0Memory  | 摸瓜V3引擎  |
| https://union.baidu.com/  | 摸瓜V3引擎  |
| https://mobads-logs.baidu.com/dz.zb?  | 摸瓜V3引擎  |
| https://p2-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adWaynePlayer/ks\_so-adWaynePlayerArm64v8aRelea  | 摸瓜V3引擎  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v7\_lite\_3358  | 摸瓜V3引擎  |
| https://dc.sigmob.cn/log  | 摸瓜V3引擎  |
| http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtd  | 摸瓜V3引擎  |
| https://p2-lm.adkwai.com/udata/pkg/81c04ed656cd492e93c19598d66f5be3.png  | 摸瓜V3引擎  |
| https://p2-lm.adkwai.com/bs2/adUnionVideo/98f7ff08d42d421b87ce6005117e4942.jpg  | 摸瓜V3引擎  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/adLive/ks\_so-adLiveNoSoRele  | 摸瓜V3引擎  |
| http://purl.oclc.org/dsdl/schematronhttp://www.ascc.net/xml/schematronFailed  | 摸瓜V3引擎  |
| http://purl.oclc.org/dsdl/schematron  | 摸瓜V3引擎  |
| sdk.beizi.biz  | 摸瓜V3引擎  |
| http://www.iana.org/assignments/language-subtag-registry  | 摸瓜V3引擎  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adLive/ks\_so-adLiveArmeabiv7aRelease-3.3.44.2-  | 摸瓜V3引擎  |
| https://tdid.m.qq.com?mc=2  | 摸瓜V3引擎  |
| https://p2-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adWaynePlayer/ks\_so-adWaynePlayerArmeabiv7aRel  | 摸瓜V3引擎  |
| https://p2-lm.adkwai.com/kos/nlav11213/hybrid/api-introduction/api-introduction-2a68416022.html?id  | 摸瓜V3引擎  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adLive/ks\_so-adLiveArm64v8aRelease-3.3.44.2-e8  | 摸瓜V3引擎  |
| https://n.sigmob.cn/mraid2  | 摸瓜V3引擎  |
| https://adservice.sigmob.cn/s/config?  | 摸瓜V3引擎  |
| http://schemas.android.com/aapt  | 摸瓜V3引擎  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-webpArm64v8aRelease-3.3.9-e8fbb3a5f8-66  | 摸瓜V3引擎  |
| https://mobads-pre-config.bj.bcebos.com/tools/toolsvideohor.mp4  | 摸瓜V3引擎  |
| https://www.csjplatform.com/supportcenter/5885  | 摸瓜V3引擎  |
| https://mobads.baidu.com/ad.html?url=%s&sn=%s&v=%s  | 摸瓜V3引擎  |
| https://cpu.baidu.com/block/app/  | 摸瓜V3引擎  |
| https://glassfish.dev.java.net/public/CDDL  | 摸瓜V3引擎  |
| https://curl.haxx.se/docs/http-cookies.html  | 摸瓜V3引擎  |
| https://ad.shunchangzhixing.com/base/  | 摸瓜V3引擎  |
| https://cpro.baidustatic.com/cpro/logo/sdk/mob-adIcon\_2x.png  | 摸瓜V3引擎  |
| http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtdurn:oasis:names:tc:entity:xmlns:x  | 摸瓜V3引擎  |
| http://inner.shunchangzhixing.com  | 摸瓜V3引擎  |
| HTTP://WEBADDRESS.ELIDED  | 摸瓜V3引擎  |
| https://apmplus.volces.com/monitor/collect/c/session  | 摸瓜V3引擎  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v7\_3358  | 摸瓜V3引擎  |
| https://inner.shunchangzhixing.com  | 摸瓜V3引擎  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v8\_3358  | 摸瓜V3引擎  |
| ulogs.umeng.com.gds.alibabadns.com  | 摸瓜V3引擎  |
| https://adservice.sigmob.cn/s/config  | 摸瓜V3引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V3引擎  |
| https://p2-lm.adkwai.com/bs2/ad-app/YWQtYXBwOmFkX2RzcF9hcHA6NDIzMDU3NTQ2MTpNRVJDSEFOVDpbQkA3ZWRjNjUw  | 摸瓜V3引擎  |
| http://java.sun.com/xml/ns/jaxb  | 摸瓜V3引擎  |
| https://mobads-pre-config.bj.bcebos.com/sdk/dynamicBarrage/bd\_barrage\_emoji  | 摸瓜V3引擎  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-webpArmeabiv7aRelease-3.3.9-e8fbb3a5f8-  | 摸瓜V3引擎  |
| https://mobads.baidu.com/query\_ad  | 摸瓜V3引擎  |
| https://mobads-pre-config.cdn.bcebos.com/tools/lp\_hor.jpg  | 摸瓜V3引擎  |
| https://adservice.sigmob.cn/ad/v4  | 摸瓜V3引擎  |
| http://www.sec.co.kr/dlna  | 摸瓜V3引擎  |
| https://ad.shunchangzhixing.com  | 摸瓜V3引擎  |
| https://c.etoolads.cn/s/config  | 摸瓜V3引擎  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v8\_lite\_3358  | 摸瓜V3引擎  |
| https://n.sigmob.cn/mraid2/prod/200010/200010.e774d0f0.css  | 摸瓜V3引擎  |
| https://adxtool.sigmob.cn/debug/feedback  | 摸瓜V3引擎  |
| https://d.alipay.com  | 摸瓜V3引擎  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/ks\_so-kwaiPlayerArmeabiv7aRelease-3.3.44-e8  | 摸瓜V3引擎  |
| https://adservice.sigmob.cn/strategy/v6  | 摸瓜V3引擎  |
| http://127.0.0.1  | 摸瓜V3引擎  |
| http://www.ascc.net/xml/schematron  | 摸瓜V3引擎  |
| https://mobads.baidu.com/cpro/ui/mads.php  | 摸瓜V3引擎  |
| https://adservice.sigmob.cn/waterfall/v1  | 摸瓜V3引擎  |
| alogus.umeng.com.gds.alibabadns.com  | 摸瓜V3引擎  |
| https://passport.kuaishou.com/account-h5/login?smallWebview=true&sid=kuaishou.unioncontent.wallpaper  | 摸瓜V3引擎  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/ks\_so-kwaiPlayerArm64v8aRelease-3.3.44-e8fb  | 摸瓜V3引擎  |
| http://httpsLavf/58.29.100  | 摸瓜V3引擎  |
| https://p2-lm.adkwai.com/s1/htmls/api-permissioninfo/api-permissioninfo-0a5006bbb1.html?id  | 摸瓜V3引擎  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/adWaynePlayer/ks\_so-adWayne  | 摸瓜V3引擎  |
| https://app.chuangjing.com/editor/preview?projectId  | 摸瓜V3引擎  |
| ulogs.umeng.com  | 摸瓜V3引擎  |
| http://developer.umeng.com/docs/66650/cate/66650  | 摸瓜V3引擎  |
| https://adservice.sigmob.cn/extconfig?  | 摸瓜V3引擎  |
| http://java.sun.com/xml/ns/javaee  | 摸瓜V3引擎  |
| https://adservice.sigmob.cn/hb/v2/ad  | 摸瓜V3引擎  |
| http://relaxng.org/ns/structure/1.0  | 摸瓜V3引擎  |
| https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| https://n.sigmob.cn/mraid2/prod/200010/200010.82ec19b8.js  | 摸瓜V3引擎  |
| http://www.rfc-editor.org/rfc/bcp/bcp47.txt  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| xxx@email.elided  | aegon/chrome/base/PiiElider.java  |
| danikula@gmail.com  | com/kwad/sdk/core/videocache/h.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | com/kwai/video/player/KsMediaMeta.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: CN=euun, OU=euun, O=euun, L=euun, ST=euun, C=euun 签名算法: rsassa\_pkcs1v15 有效期自: 2025-02-06 04:19:25+00:00 有效期至: 2125-01-13 04:19:25+00:00 发行人: CN=euun, OU=euun, O=euun, L=euun, ST=euun, C=euun 序列号: 0x1 哈希算法: sha256 md5值: 95987bc05967cbe7563b5f496f698f79 sha1值: 32aa7c2fa98fdf00821e9c3b28f95b364e74d877 sha256值: 0579236f8d9eb9e3181038da227e0519d1cb2d9f2806187dc5041b5ff61d86b8 sha512值: c0670f307ca724b5c201a0e5293c9f0c79c044df5b98d1177b70f52b63d1d67835ec5931b2e5697d3ebd32a7a2378458a62b2a6c4b75ace3b9e47a0ba31ad8b2 公钥算法: rsa 密钥长度: 2048 指纹: d3a56761abad54c1adfa0af6b18524d12fdfc2ebe64942808d174ca7a6f99b80**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "dyStrategy.privateAddress" : "privateAddress"  |
| "ksad\_ad\_default\_author" : "@可爱的广告君创造的原声"  |
| "ksad\_ad\_default\_username" : "@可爱的广告君"  |

## **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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.CHANGE\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收  | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| 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.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.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.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.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.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.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 |
| com.ybyx.app.euun.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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.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 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| com.ybyx.app.euun.openadsdk.permission.TT\_PANGOLIN | 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.permissio.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 |
| com.ybyx.app.euun.permission.KW\_SDK\_BROADCAST | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| 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 |

## **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。**