



MoGua

照妖镜1.8 1.0.APK 分析报告



APP名称:

照妖镜1.8

包名:	com.android.ftpeasys
域名线索:	68条
URL线索:	24条
邮箱线索:	2条
分析日期:	2025年10月2日
分析平台:	摸瓜APK反编译平台

文件名: zhaoyaoad321.apk
文件大小: 12.31MB
MD5值: 5eb549e856013128b1c00959e68fa3d3
SHA1值: 24d7ee1975644cf46c516d6ca3010ee13295af73
SHA256值: 44fd2dc2c9ae9ae31defa816ca26298969d34de062df8edbdcc227cb14d72adf3

i APP 信息

App名称: 照妖镜1.8
包名: com.android.ftpeasys
主活动Activity: a.more.box.ui.activity.SplashActivity
安卓版本名称: 1.0
安卓版本: 1

🔍 域名线索

域名	服务器信息
cpucdn.baidu.com	IP: 221.204.49.35 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
hmma.baidu.com	IP: 110.242.68.196 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
render-server.cdn.bcebos.com	IP: 221.204.61.38 所属国家: China 地区: Shanxi

	城市: Taiyuan 纬度: 37.869438 经度: 112.561508
cpu-openapi.baidu.com	IP: 110.242.68.91 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
m.baidu.com	IP: 110.242.68.10 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
multi-az-ad.kuaishou.com	IP: 103.102.202.80 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
gcc.gnu.org	IP: 8.43.85.97 所属国家: United States of America 地区: North Carolina 城市: Raleigh 纬度: 35.773994 经度: -78.632759
211.151.146.65	IP: 211.151.146.65 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

cpro.baidustatic.com	IP: 101.72.203.38 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
cpucdn.baidu.com.a.bdydns.com	IP: 221.204.49.35 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
bes-mtj.baidu.com	IP: 103.211.221.124 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
opencdnbaiduwm.jomodns.com	IP: 101.72.203.35 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
lh3-dz.googleusercontent.com	IP: 142.251.215.225 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
lupic.cdn.bcebos.com	IP: 123.117.133.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501

	经度: 116.397102
p2-lm.adukwai.com	IP: 60.222.11.135 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
mobads-logs.e.shifen.com	IP: 153.3.237.160 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
gdfp.gifshow.com	IP: 116.136.162.62 所属国家: China 地区: Nei Mongol 城市: Hohhot 纬度: 40.810650 经度: 111.650665
apps.samsung.com	IP: 139.215.225.97 所属国家: China 地区: Jilin 城市: Changchun 纬度: 43.880001 经度: 125.322777
ulogs.umeng.com	IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
	IP: 223.109.148.139 所属国家: China

utoken.umeng.com	地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
gcp-anycast.sg.kwaionline.com	IP: 8.219.118.134 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
p1-lm.adkwai.com.cdn.dnsv1.com	IP: 39.91.181.47 所属国家: China 地区: Shandong 城市: Linyi 纬度: 35.063061 经度: 118.342781
pslog.umeng.com	IP: 59.82.60.43 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
multi-az-ulong.gifshow.com	IP: 103.107.217.28 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
developer.umeng.com	IP: 59.82.112.112 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583

ulogs.umengcloud.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
p3-ad.adukwai.com	IP: 42.56.77.2 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
lupic.cdn.bcebos.com.a.bdydns.com	IP: 123.117.133.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
mobads.baidu.com	IP: 111.206.208.180 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
alogsus.umeng.com	IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
opencdnsslglobal.jomodns.com	IP: 221.204.49.35 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438

	经度: 112.561508
p1-lm.adkwai.com	IP: 39.91.181.47 所属国家: China 地区: Shandong 城市: Linyi 纬度: 35.063061 经度: 118.342781
mobads-logs.baidu.com	IP: 153.3.237.160 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
lh3.googleusercontent.com	IP: 142.251.215.225 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
c.tenor.com	IP: 185.45.7.97 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London 纬度: 51.508530 经度: -0.125740
encrypted-tbn0.gstatic.com	IP: 142.251.215.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
	IP: 67.228.102.32 所属国家: United States of America

media.tenor.com	地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958
gcp-anycast-nq.sg.kwaionline.com	IP: 8.219.118.134 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
p4-ad.adukwai.com	IP: 60.6.3.120 所属国家: China 地区: Hebei 城市: Xingtai 纬度: 37.062309 经度: 114.494209
tx.a.kspkg.com	IP: 221.204.73.105 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
cpu.baidu.com	IP: 110.242.68.91 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
plbslog.umeng.com	IP: 36.156.202.68 所属国家: China 地区: Jiangsu 城市: Yangzhou 纬度: 32.397221 经度: 119.435600

open.e.kuaishou.com	IP: 116.136.202.194 所属国家: China 地区: Nei Mongol 城市: Hohhot 纬度: 40.810650 经度: 111.650665
w1.kskwai.com	IP: 123.125.244.44 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
lqlq6pqu.ovslegodl.sched.ovscdns.com	IP: 43.152.24.53 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
static.yximgs.com	IP: 60.222.11.128 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
edgedl.me.gvt1.com	IP: 34.104.35.123 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore

	纬度: 1.289987 经度: 103.850281
alogus.umeng.com	IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
p2-ad.adukwai.com	IP: 60.222.11.138 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
cpro.baidustatic.com.a.bdydns.com	IP: 101.72.203.38 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
p5-ad.adukwai.com	IP: 123.117.133.41 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
w1.kskwai.com.cdn.dns.v1.com	IP: 123.125.244.23 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 111.206.209.29 所属国家: China

haokan.baidu.com	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
zt.gifshow.com	IP: 103.102.202.120 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
mobads-pre-config.cdn.bcebos.com	IP: 221.204.61.38 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
a11agcf1.ovslegodl.sched.ovscdns.com	IP: 203.205.136.188 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
aden.baidu.com	IP: 110.242.68.230 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
union.baidu.com	IP: 111.206.208.169 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

tx.a.kspkg.com.cdn.dnsv1.com	IP: 221.204.72.196 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
d9cqj2xz.sched.kslego-dk.tdnsstic1.cn	IP: 221.204.72.196 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
googlehosted.l.googleusercontent.com	IP: 142.251.215.225 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
adjs-default-scd.e.kuaishou.com	IP: 116.136.202.194 所属国家: China 地区: Nei Mongol 城市: Hohhot 纬度: 40.810650 经度: 111.650665
opencdnglobal.gshifen.com	IP: 103.235.45.242 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong

	纬度: 22.285521 经度: 114.157692
opencdnssl6.jomodns.com	IP: 123.117.133.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
uilog-sdk.gifshow.com	IP: 103.102.202.158 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
mobads.e.shifen.com	IP: 111.206.208.180 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

 URL线索

URL信息	Url所在文件
https://cpro.baidustatic.com/cpro/logo/sdk/mob-adlcon_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
http://union.baidu.com/	com/baidu/mobads/sdk/api/XAdNativeResponse.java

https://cpro.baidustatic.com/cpro/logo/sdk/mob-adlcon_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
http://union.baidu.com/	com/baidu/mobads/sdk/api/XAdEntryResponse.java
http://211.151.146.65:8080/wlantest/shanghai_sun/mock_ad_server_interstitial_video.json	com/baidu/mobads/sdk/internal/dp.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/tk/ks_so-tachikomaNoSoRelease-3.3.55-ab4730d57f-416.zip	com/kwad/components/offline/c/c.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/ks_tk_so_v8_lite_3334	com/kwad/components/offline/c/b/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/ks_tk_so_v8_3334	com/kwad/components/offline/c/b/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/ks_tk_so_v7_lite_3334	com/kwad/components/offline/c/b/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/ks_tk_so_v7_3334	com/kwad/components/offline/c/b/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/obiwan/ks_so-obiwanNoSoRelease-3.3.44-d884574fc8-340.zip	com/kwad/components/offline/b/b.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/adLive/ks_so-adLiveNoSoRelease-3.3.54-6a9edb7f47-422.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://open.e.kuaishou.com/rest/e/v3/open/sdk2	com/kwad/sdk/api/loader/u.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/202305301754/ks_so-exceptionArm64v8aRelease-3.3.47-e8fbb3a5f8-666.apk	com/kwad/sdk/crash/g.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/so/exception/202305301754/ks_so-exceptionArmeabiv7aRelease-3.3.47-e8fbb3a5f8-666.apk	com/kwad/sdk/crash/g.java
http://apps.samsung.com/appquery/appDetail.as?appId=	com/kwad/sdk/utlis/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://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.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/119267/detail/182050	com/umeng/commonsdk/debug/UMLogCommon.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.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://utoken.umeng.com/api/postZdata/v4	com/umeng/umzid/ZIDManager.java
https://utoken.umeng.com/api/updateZdata/v4	com/umeng/umzid/ZIDManager.java
cpro.baidustatic.com	摸瓜V3引擎
https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png	摸瓜V3引擎
https://aden.baidu.com/	摸瓜V3引擎
https://mobads.baidu.com/ads/preload.php	摸瓜V3引擎
https://lupic.cdn.bcebos.com/static/aden_sdk_cache.b647449.css	摸瓜V3引擎
p1-lm.adkwai.com.cdn.dnsv1.com	摸瓜V3引擎
https://mobads-pre-config.cdn.bcebos.com/sdk/splash/mix_interact_black_arc.json	摸瓜V3引擎
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-appStatusArmeabiv7aRelease-3.3.14.apk	摸瓜V3引擎
p3-ad.adukwai.com	摸瓜V3引擎
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/so/exception/202305301754/ks_so-exceptionArm64	摸瓜V3引擎

play.googleapis.com	摸瓜V3引擎
http://aden.baidu.com/	摸瓜V3引擎
mobads-logs.baidu.com	摸瓜V3引擎
c.tenor.com	摸瓜V3引擎
https://bes-mtj.baidu.com/auto.gif	摸瓜V3引擎
http://gcc.gnu.org/bugs.html):	摸瓜V3引擎
encrypted-tbn0.gstatic.com	摸瓜V3引擎
tx.a.kspkg.com	摸瓜V3引擎
https://cpro.baidustatic.com/cpro/logo/sdk/mob-adlcon_2x.png	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
lqlq6pqu.ovslegodl.sched.ovscdns.com	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎
edgedl.me.gvt1.com	摸瓜V3引擎
tx.a.kspkg.com.cdn.dnsv1.com	摸瓜V3引擎
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/ks_tk_so_v8_3334	摸瓜V3引擎
https://mobads-pre-config.cdn.bcebos.com/sdk/feed/slide_finger.png	摸瓜V3引擎
opencdnssl6.jomodns.com	摸瓜V3引擎
https://cpucdn.baidu.com/static/assets/sdk-cache.cache-lottie.94178d47.chunk.js	摸瓜V3引擎

http://cpu-openapi.baidu.com/api/v2/aggregation/channels	摸瓜V3引擎
https://hmma.baidu.com/app.gif	摸瓜V3引擎
cpucdn.baidu.com	摸瓜V3引擎
https://haokan.baidu.com/activity/h5/chaihongbao?productid=2&inviteCode=736CCC5X010&pd=lu&tab=guide&	摸瓜V3引擎
http://mobads-pre-config.cdn.bcebos.com/sdk/iadex/full_iadex.php	摸瓜V3引擎
https://cpu-openapi.baidu.com/api/v2/aggregation/channels	摸瓜V3引擎
http://m.baidu.com/baidu.php?sc	摸瓜V3引擎
opencdnbaiduwm.jomodns.com	摸瓜V3引擎
https://cpu.baidu.com/	摸瓜V3引擎
http://%s:%d/%s?timestamp=%s&cachefactor=%.2f&sign=%s	摸瓜V3引擎
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/kmac/ks_kmac32	摸瓜V3引擎
gdfp.gifshow.com	摸瓜V3引擎
gcp-anycast.sg.kwaionline.com	摸瓜V3引擎
multi-az-ulog.gifshow.com	摸瓜V3引擎
mobads.baidu.com	摸瓜V3引擎
opencdnsslglobal.jomodns.com	摸瓜V3引擎
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/so/exception/202305301754/ks_so-exceptionArmea	摸瓜V3引擎

media.tenor.com	摸瓜V3引擎
p4-ad.adukwai.com	摸瓜V3引擎
https://mobads-logs.baidu.com/dz.zb?type=425	摸瓜V3引擎
https://m.baidu.com/baidu.php?sc	摸瓜V3引擎
http://hmma.baidu.com/app.gif	摸瓜V3引擎
https://cpu.baidu.com/block/app/	摸瓜V3引擎
http://127.0.0.1	摸瓜V3引擎
p2-ad.adukwai.com	摸瓜V3引擎
https://mobads-logs.baidu.com/dz.zb?	摸瓜V3引擎
https://union.baidu.com	摸瓜V3引擎
https://mobads-pre-config.cdn.bcebos.com/sdk/splash/mix_interact_shake.json	摸瓜V3引擎
https://utoken.umeng.com/api/updateZdata/v4	摸瓜V3引擎
http://apps.samsung.com/appquery/appDetail.as?appId=	摸瓜V3引擎
https://github.com/danikula/AndroidVideoCache/issues.	摸瓜V3引擎
d9cqj2xz.sched.kslego-dk.tdnsstic1.cn	摸瓜V3引擎
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/ks_tk_so_v7_3334	摸瓜V3引擎
googlehosted.l.googleusercontent.com	摸瓜V3引擎
http://cpu-openapi.baidu.com/api/v2/data/list	摸瓜V3引擎

https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/ks_tk_so_v8_lite_3334	摸瓜V3引擎
uilog-sdk.gifshow.com	摸瓜V3引擎
mobads.e.shifen.com	摸瓜V3引擎
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/ks_tk_so_v7_lite_3334	摸瓜V3引擎
cpucdn.baidu.com.a.bdydns.com	摸瓜V3引擎
http://mobads.baidu.com/query_ad	摸瓜V3引擎
lh3-dz.googleusercontent.com	摸瓜V3引擎
lupic.cdn.bcebos.com	摸瓜V3引擎
p2-lm.adukwai.com	摸瓜V3引擎
mobads-logs.e.shifen.com	摸瓜V3引擎
https://mobads-pre-config.cdn.bcebos.com/sdk/cpu/cpu_drama_playing.json	摸瓜V3引擎
https://github.com/danikula/AndroidVideoCache/issues/88	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
http://cpu-openapi.baidu.com/api/v2/data/detailwithconfig	摸瓜V3引擎
gcp-anycast-nq.sg.kwaionline.com	摸瓜V3引擎
http://mobads.baidu.com/ads/index.htm	摸瓜V3引擎
https://mobads.baidu.com/ad.html?url=%s&sn=%s&v=%s	摸瓜V3引擎

http://developer.umeng.com/docs/66650/cate/66650	摸瓜V3引擎
open.e.kuaishou.com	摸瓜V3引擎
w1.kskwai.com	摸瓜V3引擎
https://mobads-pre-config.cdn.bcebos.com/sdk/splash/mix_interact_slide.json	摸瓜V3引擎
https://mobads-pre-config.cdn.bcebos.com/sdk/splash/bd_splash_shake_lottie_red_package_common.json	摸瓜V3引擎
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/kmac/ks_kmac64	摸瓜V3引擎
https://lupic.cdn.bcebos.com/static/aden_sdk_cache_iconhand.74457e7.png	摸瓜V3引擎
clientservices.googleapis.com	摸瓜V3引擎
cpro.baidustatic.com.a.bdydns.com	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://cpu-openapi.baidu.com/api/v2/data/list	摸瓜V3引擎
http://mobads.baidu.com/	摸瓜V3引擎
https://utoken.umeng.com/api/postZdata/v4	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
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-appStatusArm64v8aRelease-3.3.14.apk	摸瓜V3引擎
zt.gifshow.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

a11agcf1.ovslegodl.sched.ovscdns.com	摸瓜V3引擎
https://lupic.cdn.bcebos.com/static/aden_sdk_cache_larkplayer.1ed5e92.js	摸瓜V3引擎
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/tk/ks_so-tachikomaNoSoRelea	摸瓜V3引擎
adjs-default-scd.e.kuaishou.com	摸瓜V3引擎
opencdnglobal.gshifen.com	摸瓜V3引擎
https://open.e.kuaishou.com/rest/e/v3/open/sdk2	摸瓜V3引擎
multi-az-ad.kuaishou.com	摸瓜V3引擎
http://union.baidu.com/	摸瓜V3引擎
https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties	摸瓜V3引擎
https://cpucdn.baidu.com/static/assets/sdk-cache.cache-packages.3d231ecb.chunk.js	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
https://mobads-pre-config.cdn.bcebos.com/sdk/feed/slide_cycle.json	摸瓜V3引擎
http://m.baidu.com	摸瓜V3引擎
http://211.151.146.65:8080/wlantest/shanghai_sun/mock_ad_server_intersitial_video.json	摸瓜V3引擎
http://mobads.baidu.com/ads/pa/8/gray/__pasys_remote_banner.php	摸瓜V3引擎
https://github.com/danikula/AndroidVideoCache/issues/43.	摸瓜V3引擎
https://cpu-openapi.baidu.com/api/v2/data/playlet/detail/ads	摸瓜V3引擎

lupic.cdn.bcebos.com.a.bdydns.com	摸瓜V3引擎
https://lupic.cdn.bcebos.com/static/aden_sdk_cache.e4623d8.js	摸瓜V3引擎
p1-lm.adkwai.com	摸瓜V3引擎
lh3.googleusercontent.com	摸瓜V3引擎
https://cpu-openapi.baidu.com/api/bes/s	摸瓜V3引擎
https://cpu-openapi.baidu.com/api/v2/data/detailwithconfig	摸瓜V3引擎
https://render-server.cdn.bcebos.com/static/images/20201231/zhongcao.png	摸瓜V3引擎
http://cpu-openapi.baidu.com/api/v2/data/novel/detail/ads	摸瓜V3引擎
https://cpu-openapi.baidu.com/api/v2/data/ads	摸瓜V3引擎
p5-ad.adukwai.com	摸瓜V3引擎
w1.kskwai.com.cdn.dns1.com	摸瓜V3引擎
http://cpu-openapi.baidu.com/api/v2/data/playlet/detail/ads	摸瓜V3引擎
https://developer.umeng.com/docs/66632/detail/	摸瓜V3引擎
https://mobads-pre-config.cdn.bcebos.com/sdk/splash/mix_interact_progress.json	摸瓜V3引擎
http://mobads.baidu.com/cpro/ui/mads.php	摸瓜V3引擎
https://developer.umeng.com/docs/119267/detail/182050	摸瓜V3引擎

邮箱地址	所在文件
danikula@gmail.com	com/kwad/sdk/core/video/cache/h.java
.apk@classes.dex	com/kuaishou/weapon/p0/ac.java

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: CN=null, OU=null, O=null, L=null, ST=null, C=null
签名算法: rsassa_pkcs1v15
有效期自: 2023-03-13 05:39:06+00:00
有效期至: 2048-03-06 05:39:06+00:00
发行人: CN=null, OU=null, O=null, L=null, ST=null, C=null
序列号: 0x1
哈希算法: sha256
md5值: 3f174f045db1cca96c224a78f723de78
sha1值: 43ec84f5258490dddb46191964234dfe1100e43c
sha256值: 4276cf49530eff26205127c1cd5acf3422b943862a3f944e5b1b34382d23a424
sha512值: 8edb5a66bd17141bfc884efc2d9d5a2cd6995528e0bb5ac5b42fab851280b33f448fd42f6da0e5dd2186c110c3c3fbf352e4830b827cf5b41fdd5151a8f10620
公钥算法: rsa
密钥长度: 2048
指纹: 5a4ef851f2efe993297da5d9511d4460950f3c062fafcbc9c3dd9ea6801ffa02

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.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_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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
com.zyfb.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信