



MoGua

母狗园 2.2.8.APK 分析报告



APP名称:

母狗园

包名: com.androidjks.aw.d1732539192919205312

域名线索: 18条

URL线索: 32条

邮箱线索: 2条

分析日期: 2025年8月19日

分析平台: [摸瓜APK反编译平台](#)

文件名: 母狗园.apk
文件大小: 40.39MB
MD5值: b38673bd569f8182446e26d39c09b7d5
SHA1值: 5bd0c7e898553d9407f83c756b1f10d3f0fbd83d
SHA256值: a3ba890215060acc7c38198fdc5a637faf759c352eb0cb20e11a1f512fc8ddef

i APP 信息

App名称: 母狗园
包名: com.androidjks.aw.d1732539192919205312
主活动Activity: com.grass.mh.SplashActivity
安卓版本名称: 2.2.8
安卓版本: 228

🔍 域名线索

域名	服务器信息
schemas.android.com	没有服务器地理信息.
aw.vekqdyjy.xyz	IP: 104.21.55.248 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
cfg.flurry.com	IP: 69.147.80.12 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.731323 经度: -73.990089

data.flurry.com	IP: 98.136.147.16 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.731323 经度: -73.990089
aw.vkdzygl0.xyz	IP: 172.67.195.133 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
freemarker.org	IP: 192.64.119.217 所属国家: United States of America 地区: Georgia 城市: Atlanta 纬度: 33.727291 经度: -84.425377
clsp.fun	IP: 143.92.53.209 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
aw.vjgx0zd6.xyz	IP: 104.21.64.183 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700

	经度: -122.395203
playready.directtaps.net	IP: 104.45.231.79 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418
greenrobot.org	IP: 85.13.163.69 所属国家: Germany 地区: Thuringen 城市: Friedersdorf 纬度: 50.604919 经度: 11.035770
api.login.yahoo.com	IP: 74.6.160.138 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.731323 经度: -73.990089
schemas.microsoft.com	IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
www.example.com	IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052570 经度: -118.243904
	IP: 18.173.206.18 所属国家: United States of America 地区: Washington

dx0609tjkmfbm.cloudfront.net	城市: Seattle 纬度: 47.627499 经度: -122.346199
www.slf4j.org	IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790
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
freemarker.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

URL线索

URL信息	Url所在文件
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

https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/mp3cache/Pinger.java
http://%s:%d/%s	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
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java
http://www.example.com	com/flurry/sdk/ed.java
https://cfg.flurry.com/sdk/v1/config	com/flurry/sdk/cl.java
https://cfg.flurry.com/sdk/v1/config	com/flurry/sdk/by.java
https://data.flurry.com/v1/flr.do	com/flurry/sdk/br.java
https://api.login.yahoo.com/oauth2/device_session	com/flurry/sdk/ef.java
https://aw.vekdyjy.xyz	com/grass/mh/SplashActivity.java
https://aw.vjgx0zd6.xyz	com/grass/mh/SplashActivity.java
https://aw.vkdzygl0.xyz	com/grass/mh/SplashActivity.java

https://dx0609tjkmfbm.cloudfront.net/aw.json	com/grass/mh/SplashActivity.java
https://clsp.fun	com/grass/mh/databinding/ActivityShareLayoutBindingImpl.java
https://freemarker.apache.org/docs/ref_builtins.html ;	freemarker/core/BuiltIn.java
http://freemarker.org/docs/ref_directive_list.html).	freemarker/core/FMParserTokenManager.java
http://freemarker.org/docs/ref_directive_alphaidx.html ;	freemarker/core/FMParserTokenManager.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.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/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://schemas.android.com/apk/res/android	org/dsq/library/widget/tablayout/SlidingTabLayout.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
https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/database/DatabaseOpenHelper.java
http://www.slf4j.org/codes.html	org/slf4j/MDC.java
http://www.slf4j.org/codes.html	org/slf4j/LoggerFactory.java

http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.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

 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

 手机线索

手机号	所在文件
17179869185	freemarker/core/FMParserTokenManager.java
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

 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=86, ST=Hainan, L=Haikou, O=wujikeji, OU=CHN, CN=ChenXiaopeng
签名算法: rsassa_pkcs1v15
有效期自: 2024-07-08 03:53:48+00:00
有效期至: 2049-07-02 03:53:48+00:00
发行人: C=86, ST=Hainan, L=Haikou, O=wujikeji, OU=CHN, CN=ChenXiaopeng
序列号: 0x1d9272ce
哈希算法: sha256
md5值: 6611eaf74372fd774c2e0599ebb2c5b3
sha1值: a735159e80a7445642fd7f8f506780d21e50f4a4
sha256值: ec46082daea84aac1dd4c81bb2b30d5f42bf332edd75bf9a0e577b6371c39363
sha512值: d4323dd601f8b2d81906a885b2ea5aa0e8311a90e05426430ceb88b20dd440c979ad5872f742516359e635b2028079748dd697e97865dc3f78517d31520747b5
公钥算法: rsa
密钥长度: 2048
指纹: 9bd3fbcbf530ffe3d8d5456295aa7f20e1535a2e2bc53d729056f38ba85ad51a

 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.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

应用内通信