MoGua

月舞 6.10.17.1.APK 分析报告

APP名称:	月舞

包名:	com.zzjsi.lknwgwtwtgt2455412
域名线索:	33条
URL线索:	41条
邮箱线索:	1条
分析日期:	2024年11月7日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 1121.apk
文件大小: 37.79MB
MD5值: 2a4612b8eaaa9d04787c9c4cf52603e1
SHA1值: 96eb310b78f19ccfd1057c66e2f574594513bfba
SHA256值: b20c22ace9b27564042a5e857b7b5be0ab553a3da4a9d29aa10d11dbc1aa7636

APP 信息

App名称: 月舞
包名: com.zzjsi.lknwgwtwtgt2455412
主活动Activity: com.sevengms.myframe.ui.activity.start.CheckActivity
安卓版本名称: 6.10.17.1
安卓版本: 1174

域名线索

域名	服务器信息
notify.bugsnag.com	**IP**: 35.186.205.6 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
www.google.com	**IP**: 31.13.94.37 **所属国家**: Argentina **地区**: Ciudad Autonoma de Buenos Aires **城市**: Buenos Aires **纬度**: -34.603600 **经度**: -58.381554
ns.adobe.com	没有服务器地理信息.
	IP: 61.48.83.205

bato06.lllkkj.com	**所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
bato.sudataossob.com	**IP**: 154.23.178.170 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
exoplayer.dev	**IP**: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
schemas.android.com	没有服务器地理信息.
aomedia.org	**IP**: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
play.google.com	**IP**: 59.24.3.174 **所属国家**: Korea (Republic of) **地区**: Gyeonggi-do **城市**: Seongnam **纬度**: 37.420624 **经度**: 127.126717
console-k3mo.ks3-cn-shanghai.ksyuncs.com	**IP**: 120.72.43.84 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397102
schemas.microsoft.com	**IP**: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
cstaticdun.126.net	**IP**: 60.222.200.219 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
162.14.6.247	**IP**: 162.14.6.247 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
sessions.bugsnag.com	**IP**: 35.190.88.7 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
bugsnag.com	**IP**: 18.65.216.73 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322

developer.apple.com	**IP**: 17.253.87.198 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
bato.lllrrq.com	**IP**: 61.147.96.184 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221 **经度**: 119.435600
acstatic-dun.126.net	**IP**: 60.222.200.221 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
162.14.19.114	**IP**: 162.14.19.114 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
h.trace.qq.com	**IP**: 113.56.189.162 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170 **经度**: 115.077606
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
43.132.55.55	IP: 43.132.55.55 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
otlp.bugsnag.com	IP: 34.149.94.206 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
dashif.org	IP: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
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
api.ipify.org	IP: 172.67.74.152 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
	IP: 99.84.133.2 **所属国家**: Japan

docs.bugsnag.com	**地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
da.dun.163.com	**IP**: 59.111.211.178 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
direct.lc.chat	**IP**: 23.193.170.48 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
www.taobao.com	**IP**: 125.39.135.146 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
119.29.29.98	**IP**: 119.29.29.98 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
fh6api.77dbj8anka.com	**IP**: 38.181.21.140 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692

bato.sudataoss.com	**IP**: 154.23.176.234 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692

URL线索

URL信息	Url所在文件
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://43.132.55.55/conf?id=	com/tencent/msdk/dns/core/a.java
http://%s/d?%s&alg=des	com/tencent/msdk/dns/core/n/b/c.java
http://%s/d?%s&alg=aes	com/tencent/msdk/dns/core/n/a/c.java
https://h.trace.qq.com/kv?attaid=0ac00073068&token=9663669547&carrier=	com/tencent/msdk/dns/d/a.java

https://docs.bugsnag.com/platforms/android/anr-link-errors	com/bugsnag/android/AnrPlugin.java
https://docs.bugsnag.com/platforms/android/ndk-link-errors	com/bugsnag/android/NdkPlugin.java
https://da.dun.163.com/sn.gif?d=	com/netease/nis/captcha/h.java
http://acstatic-dun.126.net/tool.min.js	com/netease/nis/captcha/CaptchaWebView.java
http://cstaticdun.126.net/2.14.2/core.v2.14.2.min.js	com/netease/nis/captcha/CaptchaWebView.java
http://cstaticdun.126.net/2.14.2/light.v2.14.2.min.js	com/netease/nis/captcha/CaptchaWebView.java
http://cstaticdun.126.net//2.14.2/images/tipBg@2x.c7a9593.png	com/netease/nis/captcha/CaptchaWebView.java
http://cstaticdun.126.net//2.14.2/images/icon_light@2x.9386248.png	com/netease/nis/captcha/CaptchaWebView.java
http://schemas.android.com/apk/res/android	com/alimuzaffar/lib/pin/PinEntryEditText.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	ᵕ/C1299.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	⁚/C1423.java
https://www.google.com/	∀/AbstractC1686.java
https://www.taobao.com/help/getip.php	ŋ/AbstractC2620.java
https://api.ipify.org?format=json	ŋ/AbstractC2620.java
https://otlp.bugsnag.com/v1/traces	Ă/C2388.java
http://dashif.org/guidelines/trickmode	̏Ω/C2455.java
http://dashif.org/guidelines/last-segment-number	̏Ω/C2455.java
http://ns.adobe.com/xap/1.0/\u0000	ᵐ/C2625.java

https://notify.bugsnag.com	慨/C3575.java
https://sessions.bugsnag.com	慨/C3575.java
https://docs.bugsnag.com/platforms/android/	慨/C3534.java
https://bugsnag.com	慨/C3599.java
http://schemas.android.com/apk/res/android	痴/AbstractC4355.java
http://dashif.org/guidelines/trickmode	箙/C4568.java
http://schemas.android.com/apk/res/android	玓/C4223.java
https://exoplayer.dev/issues/cleartext-not-permitted	絽/C4653.java
https://x</LA_URL>	畷/C4313.java
https://x	畷/C4313.java
https://otlp.bugsnag.com/v1/traces	穬/C4512.java
http://ns.adobe.com/xap/1.0/	冢/C4523.java
https://aomedia.org/emsg/ID3	J/C0694.java
https://developer.apple.com/streaming/emsg-id3	J/C0694.java
http://play.google.com/store/apps/details?id=%2$s	摸瓜V1引擎
https://direct.lc.chat/11574053/	lib/armeabi-v7a/libnative-lib.so
https://bato06.lllkkj.com/06/error	lib/armeabi-v7a/libnative-lib.so

https://fh6api.77dbj8anka.com	lib/armeabi-v7a/libnative-lib.so
http://bato.sudataoss.com/06/error	lib/armeabi-v7a/libnative-lib.so
http://bato.sudataossob.com/06/error	lib/armeabi-v7a/libnative-lib.so
https://bato.lllrrq.com:7360/06/error	lib/armeabi-v7a/libnative-lib.so
https://console-k3mo.ks3-cn-shanghai.ksyuncs.com/06/error	lib/armeabi-v7a/libnative-lib.so
http://162.14.6.247/v4/ConfigGetSvc/GetOpenSSOIPList	lib/armeabi-v7a/libImSDK.so
http://119.29.29.98/d?id=39662	lib/armeabi-v7a/libImSDK.so
http://162.14.19.114/	lib/armeabi-v7a/libImSDK.so
https://direct.lc.chat/11574053/	lib/arm64-v8a/libnative-lib.so
https://bato06.lllkkj.com/06/error	lib/arm64-v8a/libnative-lib.so
https://fh6api.77dbj8anka.com	lib/arm64-v8a/libnative-lib.so
http://bato.sudataoss.com/06/error	lib/arm64-v8a/libnative-lib.so
http://bato.sudataossob.com/06/error	lib/arm64-v8a/libnative-lib.so
https://bato.lllrrq.com:7360/06/error	lib/arm64-v8a/libnative-lib.so
https://console-k3mo.ks3-cn-shanghai.ksyuncs.com/06/error	lib/arm64-v8a/libnative-lib.so
http://162.14.6.247/v4/ConfigGetSvc/GetOpenSSOIPList	lib/arm64-v8a/libImSDK.so
http://119.29.29.98/d?id=39662	lib/arm64-v8a/libImSDK.so
http://162.14.19.114/	lib/arm64-v8a/libImSDK.so

邮箱线索

邮箱地址	所在文件
tipbg@2x.c7a9593 icon_light@2x.9386248	com/netease/nis/captcha/CaptchaWebView.java

手机线索

手机号	所在文件
19222222222	镽/C3418.java
17512775099	瓦/AbstractC4274.java

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=63, ST=horizontal, L=horizontal, O=horizontal, OU=horizontal, CN=horizontal
签名算法: dsa
有效期自: 2024-11-06 02:03:54+00:00
有效期至: 2025-11-06 02:03:54+00:00
发行人: C=63, ST=horizontal, L=horizontal, O=horizontal, OU=horizontal, CN=horizontal
序列号: 0x4029727f
哈希算法: sha256

md5值: 0aac2c8d8d00539d5fc5f828abb016df
sha1值: 469c757357d7cc980c80b151115d95cb98e1604e
sha256值: ac4431c3a1482adc5710dc97444c3950dd0bb4fea3fe2a89f15f7d8567ed6ec9
sha512值: 5c48ae9b056ee1d813a01243d0ea5ce71a560728d41937d092f40d3d6d2643cc693ffb89f3c4ab643eda714570860f29c79a07babd93d61ae2ad09a069858364
公钥算法: dsa
密钥长度: 2048
指纹: 9516ed77f0d69e6b708e725925aa3e0644481c7e0a34665129b5ebc3a8892ac7

硬编码敏感信息

可能的敏感信息
"cjwt" : "常见问题"

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.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.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_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.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.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.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.READ_CLIPBOARD	未知	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_CONFIGURATION	系统需	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小

	要		
permission.WRITE_EXTERNAL_STORAGE	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.READ_PRIVILEGED_PHONE_STATE	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
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.sevengms.myframe.ui.activity.start.CheckActivity	Schemes: app7706://, xpjnmqws://, Hosts: *,
com.sevengms.myframe.ui.activity.login.LoginActivity	Schemes: xpjnmqws://,

---