MoGua

DIYP影音 5.2.0.APK 分析报告

APP名称:	DIYP影音

包名:	com.player.diyp2020
域名线索:	17条
URL线索:	19条
邮箱线索:	4条
分析日期:	2025年7月4日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: DIYP影音0622内置台标美化版.apk
文件大小: 45.47MB
MD5值: c750ec8769e8475f9f8736ab62b391f7
SHA1值: 5850bc2a30837697250c2f210fd21000c50ef821
SHA256值: 76ad10fb2b3c1dec5f2331e26a47c0f66cfb9dc2b502bcf5319d97740709f1af

APP 信息

App名称: DIYP影音
包名: com.player.diyp2020
主活动Activity: com.player.activity.LoginActivity
安卓版本名称: 5.2.0
安卓版本: 21

域名线索

域名	服务器信息
sizzlejs.com	**IP**: 104.18.230.48 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
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
www.openssl.org	**IP**: 23.13.92.35 **所属国家**: Malaysia **地区**: Selangor

	城市: Cyberjaya **纬度**: 2.922500 **经度**: 101.654999
www.macromedia.com	**IP**: 23.193.96.121 **所属国家**: United States of America **地区**: Massachusetts **城市**: Cambridge **纬度**: 42.363598 **经度**: -71.085205
fb.me	**IP**: 157.240.3.35 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.606209 **经度**: -122.332069
jquery.com	**IP**: 104.18.212.12 **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**: 128.30.52.100 **所属国家**: United States of America **地区**: Massachusetts **城市**: Cambridge **纬度**: 42.365078 **经度**: -71.104523
schemas.xmlsoap.org	**IP**: 13.107.246.49 **所属国家**: Netherlands **地区**: Noord-Holland **城市**: Amsterdam **纬度**: 52.374031 **经度**: 4.889690
	IP: 20.205.243.166

github.com	**所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
playready.directtaps.net	**IP**: 40.70.71.156 **所属国家**: United States of America **地区**: Virginia **城市**: Boydton **纬度**: 36.667641 **经度**: -78.387497
stackoverflow.com	**IP**: 151.101.1.69 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
diyp.112114.xyz	**IP**: 172.67.128.242 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
jquery.org	**IP**: 104.17.20.100 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
feross.org	**IP**: 50.116.11.184 **所属国家**: United States of America **地区**: California **城市**: Fremont **纬度**: 37.548271

	经度: -121.988571
schemas.android.com	没有服务器地理信息.
facebook.github.io	**IP**: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065632 **经度**: -79.891708
schemas.microsoft.com	**IP**: 13.107.213.49 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903

URL线索

URL**信息**	Url**所在文件**
http://www.w3.org/ns/ttml	c/c/a/a/p0/j/c.java
http://playready.directtaps.net/pr/svc/rightsmanager.asmx	c/c/a/a/k0/m.java
http://127.0.0.1:	c/e/d/h.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	c/e/e/f/h/b/b.java
http://diyp.112114.xyz	setting/MySettings.java
http://127.0.0.1:	net/media/mpc.java

http://schemas.android.com/apk/res/android	b/b/k/k.java
http://jquery.com/	Mogua Engine V2
http://sizzlejs.com/	Mogua Engine V2
http://jquery.org/license	Mogua Engine V2
https://fb.me/react-spread-deprecation	Mogua Engine V2
http://facebook.github.io/react/docs/error-decoder.html?invariant=	Mogua Engine V2
https://fb.me/react-special-props)	Mogua Engine V2
https://github.com/facebook/react/issues/3236).	Mogua Engine V2
https://fb.me/react-legacyfactory	Mogua Engine V2
https://fb.me/react-warning-keys	Mogua Engine V2
https://fb.me/react-warning-dont-call-proptypes	Mogua Engine V2
https://fb.me/react-devtools	Mogua Engine V2
https://fb.me/react-minification	Mogua Engine V2
https://fb.me/react-warning-polyfills	Mogua Engine V2
https://fb.me/react-event-pooling	Mogua Engine V2
https://fb.me/react-refs-must-have-owner).	Mogua Engine V2
http://www.w3.org/1999/xhtml	Mogua Engine V2
http://www.w3.org/1998/Math/MathML	Mogua Engine V2

http://www.w3.org/2000/svg	Mogua Engine V2
https://fb.me/react-invariant-dangerously-set-inner-html	Mogua Engine V2
https://fb.me/react-controlled-components	Mogua Engine V2
http://www.w3.org/1999/xlink	Mogua Engine V2
http://www.w3.org/XML/1998/namespace	Mogua Engine V2
https://fb.me/react-unknown-prop%s	Mogua Engine V2
https://fb.me/invalid-aria-prop%s	Mogua Engine V2
https://github.com/zertosh/loose-envify)	Mogua Engine V2
http://stackoverflow.com/questions/30030031)	Mogua Engine V2
https://github.com/reactjs/react-redux/releases/tag/v2.0.0	Mogua Engine V2
http://feross.org>	Mogua Engine V2
http://%s/forcelive&begin=%d&count=%d/%s.ts	lib/armeabi-v7a/libp8p.so
http://127.0.0.1:%d/mpegts_live	lib/armeabi-v7a/libtvcore.so
http://127.0.0.1:%d/%lu/index.m3u8	lib/armeabi-v7a/libtvcore.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libtvcore.so
http://[fe80:	lib/armeabi-v7a/libtvcore.so
http://schemas.xmlsoap.org/soap/envelope/	lib/armeabi-v7a/libtvcore.so

http://schemas.xmlsoap.org/soap/encoding/	lib/armeabi-v7a/libtvcore.so
http://%s/forcelive&begin=%d&count=%d/%s.ts	lib/armeabi-v7a/libp9p.so
http://%s/forcelive&begin=%d&count=%d/%s.ts	lib/armeabi-v7a/libp7p.so
http://%s/forcelive&begin=%d&count=%d/%s.ts	lib/armeabi-v7a/libp6p.so
http://%s/forcelive&begin=%d&count=%d/%s.ts	lib/armeabi-v7a/libp5p.so
http://%s:%s%s	lib/armeabi-v7a/libmpc_jni.so
http://%s:%s	lib/armeabi-v7a/libmpc_jni.so
http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd	lib/armeabi-v7a/libmpc_jni.so
https://www.openssl.org/docs/faq.html	lib/armeabi-v7a/libmpc_jni.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so
http://%s/forcelive&begin=%d&count=%d/%s.ts	lib/armeabi-v7a/libp3p.so
http://%s/forcelive&begin=%d&count=%d/%s.ts	lib/armeabi-v7a/libp4p.so
http://%s/forcelive&begin=%d&count=%d/%s.ts	lib/armeabi-v7a/libp2p.so

邮箱线索

邮箱地址	所在文件
tvb@gmail.com	net/media/mpc.java

feross@feross.org	Mogua Engine V2
ftp@example.com	lib/armeabi-v7a/libtvcore.so
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2008-02-29 01:33:46+00:00
Valid To: 2035-07-17 01:33:46+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Serial Number: 0x936eacbe07f201df
Hash Algorithm: sha1
md5: e89b158e4bcf988ebd09eb83f5378e87
sha1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

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.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
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.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.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.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

应用内通信

报告由 **摸瓜**APK**反编译平台** 自动生成，并非包含所有检测结果，有疑问请联系管理员。