MoGua

天涯社区 2.0.APK 分析报告

APP名称: 天涯社区

包名:	com.jbzd.media.tianya
域名线索:	18条
URL线索:	19条
邮箱线索:	1条
分析日期:	2025年8月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: tysq_ozss1tysq_2.0.apk
文件大小: 15.39MB
MD5值: 5c391637e88a6faf3437587ad5125ea0
SHA1值: 8c93153ce085af985bc38077b2bdd24395cabcd3
SHA256值: ceb66cf271e51427b96385072116996b471ec8d2939b1c24d4f9ec1521e0c2d0

APP 信息

App名称: 天涯社区
包名: com.jbzd.media.tianya
主活动Activity: com.jbzd.media.mbjqapp.ui.splash.SplashActivity
安卓版本名称: 2.0
安卓版本: 20

域名线索

域名	服务器信息
m.alipay.com	**IP**: 203.209.245.120 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
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
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
mcgw.alipay.com	IP: 123.125.216.192 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mobilegw.alipay.com	IP: 203.209.255.248 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
schemas.android.com	没有服务器地理信息.
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
loggw-exsdk.alipay.com	IP: 203.209.238.2 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
tmapi.tmsangewg.com	没有服务器地理信息.
mobilegw.aaa.alipay.net	没有服务器地理信息.

h5.m.taobao.com	**IP**: 111.19.135.197 **所属国家**: China **地区**: Shaanxi **城市**: Xianyang **纬度**: 34.337780 **经度**: 108.702606
mobilegw.stable.alipay.net	没有服务器地理信息.
wappaygw.alipay.com	**IP**: 123.125.216.192 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
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
api.buzhidaoxiesha.com	没有服务器地理信息.
mclient.alipay.com	**IP**: 125.39.135.57 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181

	经度: 117.176102

URL线索

URL**信息**	Url**所在文件**
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java

http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
http://m.alipay.com/?action=h5quit	g/a/b/j/h.java
https://h5.m.taobao.com/mlapp/olist.html	g/a/b/c/a.java
https://mobilegw.alipay.com/mgw.htm	g/a/b/c/d.java
https://mobilegw.alipay.com/mgw.htm	g/a/b/f/c.java
https://mcgw.alipay.com/sdklog.do	g/a/b/f/d/c.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	g/a/b/f/d/d.java
https://github.com/danikula/AndroidVideoCache/issues/88.	g/e/a/i.java
https://github.com/danikula/AndroidVideoCache/issues/43.	g/e/a/i.java
https://github.com/danikula/AndroidVideoCache/issues.	g/e/a/i.java
http://%s:%d/%s	g/e/a/l.java
http://%s:%d/%s	g/e/a/g.java
https://github.com/danikula/AndroidVideoCache/issues/134.	g/e/a/g.java
http://dashif.org/guidelines/last-segment-number	g/h/a/a/k1/l0/k/c.java
http://api.buzhidaoxiesha.com/cxapi/	g/m/a/a/i/l.java

http://tmapi.tmsangewg.com/cxapi/	g/m/a/a/i/l.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	i/b/a/c/d.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	i/b/a/c/b.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	g/e/a/i.java

手机线索

手机号	所在文件
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: True

找到 1 个唯一证书
主题: C=y, ST=g, L=g, O=g, OU=g, CN=we
签名算法: rsassa_pkcs1v15
有效期自: 2024-01-11 14:03:07+00:00
有效期至: 2078-10-14 14:03:07+00:00
发行人: C=y, ST=g, L=g, O=g, OU=g, CN=we
序列号: 0xc53371840bc03b41
哈希算法: sha256
md5值: 79a223dcdc339b0b0ffc4d0b8ee30b8d
sha1值: b88f9fc916bce88dfe3c9679291396177b56be41
sha256值: 1861e5889f65fc1ecb6d3fe820d54d1450f193ec4e280ef0abd1459aabbe3dd1
sha512值: a2bc3baf05e27699ecdaf305b4569d209754fd70686553d933a47da9277bf248ec19f3d0bf35ad762a069d129c9aa543c9ac4691e403ed261168cec71c11f10f
公钥算法: rsa
密钥长度: 2048
指纹: 48d6b178a446fc9d624284c8bd2049b39375e931498249d9fef1b35290176051

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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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_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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低

android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

应用内通信
