MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

花姬视频 1.0.8.APK

APP名称:	花姬视频
包名:	com.huaji.shqx
域名线索:	39条
URL线索:	45条
邮箱线索:	1条
分析日期:	2022年1月28日 22:21

文件信息

文件名: huajiship.apk
文件大小: 13.77MB
MD5值: ad15162885e16b4b2980588a139f2e91
SHA1值: e1835c7f7917437d6ebcba6aea62025e29399b64
SHA256值: e890a568a6aea4ea95faf91ff2179cffacaf6122e34d378fb75fe93021aa51b6

APP 信息

App名称: 花姬视频
包名: com.huaji.shqx
主活动**Activity:** com.huaji.shqx.activity.WelcomeActivity
安卓版本名称: 1.0.8
安卓版本: 8

域名线索

域名	是否危险域名	服务器信息
www.talkingdata.net	good	**IP:** 116.196.122.26 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
mobilegw.aaa.alipay.net	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
open.weixin.qq.com	good	**IP:** 175.24.209.30 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
loggw-exsdk.alipay.com	good	**IP:** 110.75.130.122 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
appsupport.qq.com	good	**IP:** 183.2.144.86 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map
long.open.weixin.qq.com	good	**IP:** 109.244.216.15 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
www.baidu.com	good	**IP:** 110.242.68.3 **所属国家:** China **地区:** Hebei **城市:** Baoding **纬度:** 38.851109 **经度:** 115.490280 **查看地图:** Google Map
fusion.qq.com	good	**IP:** 121.51.36.15 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
yun.tim.qq.com	good	**IP:** 175.27.14.43 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
github.com	good	**IP:** 20.205.243.166 **所属国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看地图:** Google Map
mobilegw.stable.alipay.net	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
youyu-qinqin.oss-cn-shenzhen.aliyuncs.com	good	**IP:** 113.96.63.209 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
cgi.connect.qq.com	good	**IP:** 183.2.144.86 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map
www.w3.org	good	**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 查看地图: Google Map
xml.apache.org	good	**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 查看地图: Google Map

域名	是否危险域名	服务器信息
freemarker.apache.org	good	**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 查看地图: Google Map
wappaygw.alipay.com	good	**IP:** 203.209.250.50 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
mcgw.alipay.com	good	**IP:** 203.209.250.50 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
me.cpatrk.net	good	**IP:** 116.198.14.165 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
ap.cpatrk.net	good	**IP:** 116.198.14.40 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
purpyrlbe.bkt.clouddn.com	good	**IP:** 183.136.232.59 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
api.weixin.qq.com	good	**IP:** 109.244.145.152 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
freemarker.org	good	**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 查看地图: Google Map

域名	是否危险域名	服务器信息
m.alipay.com	good	**IP:** 203.209.245.120 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
openmobile.qq.com	good	**IP:** 113.96.208.233 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
cloud.xdrig.com	good	**IP:** 116.198.14.45 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
login.imgcache.qq.com	good	**IP:** 182.254.48.231 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map

域名	是否危险域名	服务器信息
langu-ugirl.oss-cn-shenzhen.aliyuncs.com	good	**IP:** 120.77.166.77 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
mclient.alipay.com	good	**IP:** 203.209.245.120 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
ping.huatuo.qq.com	good	**IP:** 121.51.191.216 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
mobilegw.alipay.com	good	**IP:** 203.209.255.238 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map

域名	是否危险域名	服务器信息
greenrobot.org	good	**IP:** 85.13.129.145 所属国家: Germany 地区: Thuringen 城市: Friedersdorf 纬度: 50.604919 经度: 11.035770 查看地图: Google Map
huatuocode.huatuo.qq.com	good	没有服务器地理信息.
mobilegw.alipaydev.com	good	**IP:** 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
render.alipay.com	good	**IP:** 150.138.144.195 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941 查看地图: Google Map
182.254.116.116	good	**IP:** 182.254.116.116 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map

域名	是否危险域名	服务器信息
cgi.qplus.com	good	**IP:** 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
h5.m.taobao.com	good	**IP:** 59.47.225.232 所属国家: China 地区: Liaoning 城市: Benxi 纬度: 41.288609 经度: 123.764999 查看地图: Google Map

URL线索

URL信息	Url所在文件
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.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

URL信息	Url所在文件
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
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/cons/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
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

URL信息	Url所在文件
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://ap.cpatrk.net/u/a/v1	com/tendcloud/tenddata/aa.java
https://cloud.xdrig.com/configcloud/rest/sdk/match	com/tendcloud/tenddata/aa.java
https://cloud.xdrig.com/configcloud/rest/sdk/gdprCheck	com/tendcloud/tenddata/aa.java
www.talkingdata.net	com/tendcloud/tenddata/u.java
https://me.cpatrk.net	com/tendcloud/tenddata/a.java
http://purpyrlbe.bkt.clouddn.com//subpackage/	com/dasc/base_self_innovate/model/vo/LoadDataVo.java
https://youyu-qinqin.oss-cn-shenzhen.aliyuncs.com/icon/1603243801685-400-1-1.png	com/dasc/base_self_innovate/base_/Constant.java
https://langu-ugirl.oss-cn-shenzhen.aliyuncs.com/icon/1603243802090-400-1-1.png	com/dasc/base_self_innovate/base_/Constant.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
https://openmobile.qq.com/oauth2.0/me	com/tencent/connect/UnionInfo.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1	com/tencent/connect/share/QQShare.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1	com/tencent/connect/share/QzoneShare.java
https://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/connect/auth/AuthAgent.java

URL信息	Url所在文件
https://openmobile.qq.com/user/user_login_statis	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/v3/user/get_info	com/tencent/connect/auth/AuthAgent.java
https://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	com/tencent/connect/auth/AuthAgent.java
https://login.imgcache.qq.com/ptlogin/static/qzsjump.html?	com/tencent/connect/auth/a.java
https://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/connect/common/BaseApi.java
https://login.imgcache.qq.com/ptlogin/static/qzsjump.html?	com/tencent/connect/common/BaseApi.java
https://login.imgcache.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApiIml.java
https://login.imgcache.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/SocialApiIml.java
https://login.imgcache.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/SocialApiIml.java
https://login.imgcache.qq.com	com/tencent/open/SocialApiIml.java
https://openmobile.qq.com/cgi-bin/qunopensdk/unbind	com/tencent/open/SocialOperation.java
https://openmobile.qq.com/cgi-bin/qunopensdk/check_group	com/tencent/open/SocialOperation.java
https://huatuocode.huatuo.qq.com	com/tencent/open/a/d.java
http://cgi.qplus.com/report/report	com/tencent/open/utils/k.java
https://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utils/f.java

URL信息	Url所在文件
https://www.baidu.com	com/up/update/Net.java
https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code	com/huaji/shqx/wxapi/WXEntryActivity.java
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s	com/huaji/shqx/wxapi/WXEntryActivity.java
http://xml.apache.org/xslt}indent-amount	com/orhanobut/logger/LoggerPrinter.java
https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/database/DatabaseOpenHelper.java
https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code	art/jqxcm/yrkr/wxapi/WXEntryActivity.java
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s	art/jqxcm/yrkr/wxapi/WXEntryActivity.java
http://www.w3.org/XML/1998/namespace	freemarker/ext/xml/Namespaces.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/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://yun.tim.qq.com/v4/im_cos_sign_svr/cos	lib/armeabi-v7a/libImSDK.so
https://yun.tim.qq.com/v4/imopenstat/im_sdk_report	lib/armeabi-v7a/libImSDK.so
https://ping.huatuo.qq.com/yun.tim.qq.com	lib/armeabi-v7a/libImSDK.so
http://182.254.116.116/d?dn=login.tim.qq.com	lib/armeabi-v7a/libImSDK.so
https://yun.tim.qq.com/v4/im_cos_sign_svr/cos	lib/arm64-v8a/libImSDK.so
https://yun.tim.qq.com/v4/imopenstat/im_sdk_report	lib/arm64-v8a/libImSDK.so
https://ping.huatuo.qq.com/yun.tim.qq.com	lib/arm64-v8a/libImSDK.so
http://182.254.116.116/d?dn=login.tim.qq.com	lib/arm64-v8a/libImSDK.so

邮箱线索

邮箱地址	所在文件
601653444@qq.com	com/dasc/base_self_innovate/model/ContactVo.java

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.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.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.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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=f4a65d4f6a4sdf, ST=fa4s65d4f65sd, L=adf464asd6f4s, O=s4df654s6df46q, OU=d564f65s4d6, CN=da4f564sd6f5
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-10-14 08:20:30+00:00
Valid To: 2045-10-08 08:20:30+00:00
Issuer: C=f4a65d4f6a4sdf, ST=fa4s65d4f65sd, L=adf464asd6f4s, O=s4df654s6df46q, OU=d564f65s4d6, CN=da4f564sd6f5
Serial Number: 0x77d6a59d
Hash Algorithm: sha256
md5: 05699ae64d43d91e3ee54681a45fe414
sha1: 381ebc97f245f448322208c9051641ace06891af
sha256: 72f5d817e73dbf82cd9aacd6dadb1d498af18ded7b7cfe24d0c04215147da0ce
sha512: 45d3e26ae0d33a94d77541ac04605263e838a0a4821df0cf3adf358e62dd842503b6dff2871562e2af68697e5d0ca4ea17986adbf0840566910bf38cb6e96a8e
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 642571ab2ea3bef1acd9480beda4083bfe6592c41afbd2b428ff77bfef6ae206

Exodus威胁情报

名称	分类	URL链接
TalkingData	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/293

硬编码敏感信息

可能的敏感信息
"one_key_login" : "一键登录"

可能的敏感信息
"unlimited_private" : "私聊无限制"
"unlimited_private_tip" : "无限制与其他用户聊天，想聊就聊"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent1109597284://,

加壳分析

文件列表	分析结果

文件列表	分析结果
classes.dex	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check device ID check subscriber ID check ro.product.device check ro.kernel.qemu check emulator file check</td></tr><tr><td>编译器</td><td>r8</td></tr></table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
subscriber ID check
possible ro.secure check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
