MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

一起陪玩 1.0.8.APK

APP名称:	一起陪玩
包名:	com.feijing.yypeiwan
域名线索:	30条
URL线索:	33条
邮箱线索:	0条
分析日期:	2022年1月29日 00:17

文件信息

文件名: yiqianpeiwan.apk
文件大小: 4.89MB
MD5值: cb0b16b947568d64750850952973647d
SHA1值: a8a37baa9c6ee92dde289be7d4c3d0e0ef67b4b5
SHA256值: 308905bd8eb2875838c1de0356c7ca46fc913f9689134d0864df0560a6990348

APP 信息

App名称: 一起陪玩
包名: com.feijing.yypeiwan
主活动**Activity:** com.lt.app.MainActivity
安卓版本名称: 1.0.8
安卓版本: 108

域名线索

域名	是否危险域名	服务器信息
ulogs.umengcloud.com	good	**IP:** 106.11.43.144 **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
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
register.xmpush.global.xiaomi.com	good	**IP:** 47.88.199.5 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
errlog.umeng.com	good	**IP:** 106.8.130.60 **所属国家:** China **地区:** Hebei **城市:** Zhangjiakou **纬度:** 40.810001 **经度:** 114.879440 **查看地图:** Google Map
long.open.weixin.qq.com	good	**IP:** 109.244.217.35 **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
api.xmpush.xiaomi.com	good	**IP:** 117.48.116.220 **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
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
ouplog.umeng.com	good	**IP:** 47.74.172.6 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
cn.register.xmpush.xiaomi.com	good	**IP:** 203.100.92.32 **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
pslog.umeng.com	good	**IP:** 59.82.60.43 **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
plbslog.umeng.com	good	**IP:** 59.82.43.171 **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
resolver.msg.xiaomi.net	good	**IP:** 183.84.5.221 **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
ulogs.umeng.com	good	**IP:** 106.11.43.229 **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
idmb.register.xmpush.global.xiaomi.com	good	**IP:** 15.206.99.29 **所属国家:** India **地区:** Maharashtra **城市:** Mumbai **纬度:** 19.014410 **经度:** 72.847939 **查看地图:** Google Map
alogsus.umeng.com	good	**IP:** 203.119.145.194 **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
api-push.in.meizu.com	good	**IP:** 206.161.233.191 **所属国家:** United States of America **地区:** Virginia **城市:** Herndon **纬度:** 38.978210 **经度:** -77.386993 **查看地图:** Google Map
www.jivesoftware.com	good	**IP:** 35.238.7.255 **所属国家:** United States of America **地区:** Iowa **城市:** Council Bluffs **纬度:** 41.261940 **经度:** -95.860832 **查看地图:** Google Map

域名	是否危险域名	服务器信息
api-push.meizu.com	good	**IP:** 125.94.213.129 **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
new.api.ad.xiaomi.com	good	没有服务器地理信息.
aaid.umeng.com	good	**IP:** 116.132.190.27 **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
xmlpull.org	good	**IP:** 74.50.61.58 **所属国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.814899 **经度:** -96.879204 **查看地图:** Google Map
schemas.android.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
play.google.com	good	**IP:** 142.251.42.238 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map
developer.umeng.com	good	**IP:** 59.82.31.210 **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
ru.register.xmpush.global.xiaomi.com	good	**IP:** 107.155.52.56 **所属国家:** Russian Federation **地区:** Moskva **城市:** Moscow **纬度:** 55.752220 **经度:** 37.615559 **查看地图:** Google Map
errlogos.umeng.com	good	**IP:** 47.246.110.18 **所属国家:** Hong Kong **地区:** Hong Kong **城市:** Hong Kong **纬度:** 22.285521 **经度:** 114.157692 **查看地图:** Google Map

域名	是否危险域名	服务器信息
appgallery.cloud.huawei.com	good	**IP:** 117.78.15.51 **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
alogus.umeng.com	good	**IP:** 106.11.86.78 **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
norma-external-collect.meizu.com	good	**IP:** 113.106.27.98 **所属国家:** China **地区:** Guangdong **城市:** Zhongshan **纬度:** 22.520580 **经度:** 113.382317 **查看地图:** Google Map
fr.register.xmpush.global.xiaomi.com	good	**IP:** 18.185.221.188 **所属国家:** Germany **地区:** Hessen **城市:** Frankfurt am Main **纬度:** 50.115520 **经度:** 8.684170 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/i.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java

URL信息	Url所在文件
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
http://schemas.android.com/apk/res/android	com/baidu/techain/h/d.java
https://api-push.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/a/a.java
https://api-push.in.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/a/a.java
https://api-push.meizu.com/garcia/api/client/log/upload	com/meizu/cloud/pushsdk/platform/a/a.java
https://api-push.meizu.com/garcia/api/server/getPublicKey	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.in.meizu.com	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.meizu.com	com/meizu/cloud/pushsdk/constants/PushConstants.java
http://norma-external-collect.meizu.com/android/exchange/getpublickey.do	com/meizu/cloud/pushsdk/constants/PushConstants.java
http://norma-external-collect.meizu.com/push/android/external/add.do	com/meizu/cloud/pushsdk/constants/PushConstants.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/gv.java
http://new.api.ad.xiaomi.com/logNotificationAdActions	com/xiaomi/push/ct.java
http://www.jivesoftware.com/xmlns/xmpp/properties	com/xiaomi/push/gn.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/gu.java

URL信息	Url所在文件
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/fs.java
http://%1$s/gslb/?ver=4.0	com/xiaomi/push/dc.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/gc.java
http://resolver.msg.xiaomi.net/psc/?t=a	com/xiaomi/push/service/bg.java
https://cn.register.xmpush.xiaomi.com	com/xiaomi/push/service/l.java
https://register.xmpush.global.xiaomi.com	com/xiaomi/push/service/l.java
https://fr.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/l.java
https://ru.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/l.java
https://idmb.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/l.java
www.baidu.com:80	com/xiaomi/push/service/ae.java
https://api.xmpush.xiaomi.com/upload/xmsf_log?file=	com/xiaomi/mipush/sdk/u.java
https://api.xmpush.xiaomi.com/upload/app_log?file=	com/xiaomi/mipush/sdk/u.java
https://api.xmpush.xiaomi.com/upload/crash_log?file=	com/xiaomi/mipush/sdk/w.java
https://errlogos.umeng.com/upload	com/uc/crashsdk/e.java
https://errlog.umeng.com/upload	com/uc/crashsdk/e.java

URL信息	Url所在文件
https://errlog.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
https://errlogos.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
https://errlog.umeng.com	com/uc/crashsdk/a/d.java
https://errlogos.umeng.com	com/uc/crashsdk/a/d.java
https://play.google.com/store	Android String Resource
https://appgallery.cloud.huawei.com/app/	Android String Resource
https://play.google.com/store/apps/details?id=	Android String Resource
https://appgallery.cloud.huawei.com	Android String Resource
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlog.umeng.com	lib/arm64-v8a/libcrashsdk.so

URL信息	Url所在文件
https://errlogos.umeng.com	lib/arm64-v8a/libcrashsdk.so

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_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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

向手机申请的权限	是否危险	类型	详细情况
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.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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.feijing.yypeiwan.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.feijing.yypeiwan.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.feijing.yypeiwan.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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
com.feijing.yypeiwan.permission.techain.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.feijing.yypeiwan.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.feijing.yypeiwan.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference
com.feijing.yypeiwan.permission.YM_APP	未知	Unknown permission	Unknown permission from android reference
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.RECORD_VIDEO	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=BG, ST=BG, L=BG, O=BG, OU=BGUH, CN=BG
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-04-28 08:53:39+00:00
Valid To: 2121-04-04 08:53:39+00:00
Issuer: C=BG, ST=BG, L=BG, O=BG, OU=BGUH, CN=BG
Serial Number: 0x6c01d02e
Hash Algorithm: sha256
md5: d6d740c52c0f9fce7922236441ddc991
sha1: 686b943a53c4a204b526c7b1e30c07aab1d7c8be
sha256: e579298e9f9bd1f7b053f3620302b02d50cd6d95c62edcdc8f497105295b9c53
sha512: 6c9da2ab275bc8e59cc0f89fcc84c609766b063ede29bad9f9463680e0b6d7a0a1988800874a357dc7b9d58c610bcc4522da3a8939b5e0447a8d67f3b7314657
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 15ccf8634d2ee92ce427573001dd2a0403cf5f7c89c8aa596d01997f0ffe3adc

Exodus威胁情报

名称	分类	URL链接
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

🔑 硬编码敏感信息

可能的敏感信息
"p_ht_appkey" : "700006169"
"p_ht_mz_appkey" : ""
"p_ht_op_appkey" : ""
"p_ht_op_appsecret" : ""
"p_ht_vv_appkey" : ""
"p_ht_xm_appkey" : ""
"p_rcpush_mzAppKey" : ""
"p_rcpush_opAppKey" : ""
"p_rcpush_opAppSecret" : ""
"p_rcpush_vvAppKey" : ""

可能的敏感信息
"p_rcpush_xmAppKey" : ""
"p_u_appkey" : "60892294f00c2e19b93e8613"
"p_weibo_appkey" : ""

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.lt.app.JumpActivity	Schemes: ltapp261507://,

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 SIM operator check network operator name check</td></tr><tr><td>编译器</td><td>r8</td></tr><tr><td>模糊器</td><td>unreadable field names unreadable method names</td></tr></table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>lib/arm64-v8a/libtechain.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version 3.4</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi-v7a/libtechain.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version 3.4</td></tr>
</table>
</td></tr>
</table>
