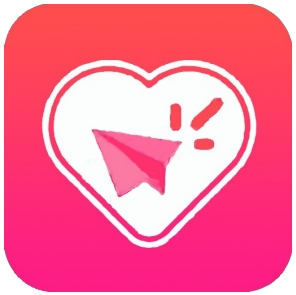
MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成



走心爱 1.0.0.APK

APP名称:	走心爱
包名:	com.tg.zhifj
域名线索:	12条
URL线索:	20条
邮箱线索:	1条
分析日期:	2022年1月28日 23:45

文件信息

文件名: zouxinai.apk
文件大小: 6.9MB
MD5值: d30c10f3b41ebb11856a3a163c4c0349
SHA1值: 14d55339313f4d59c74da7803466347e55329585
SHA256值: e50b418ca769e0fe9555105bbe3c0252fee071a50fcdd8fa24f1693b794a100d

APP 信息

App名称: 走心爱
包名: com.tg.zhifj
主活动**Activity:** com.yyjj.nnxx.nn_activity.NN_LaunchActivity
安卓版本名称: 1.0.0
安卓版本: 1

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

域名	是否危险域名	服务器信息
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
issuetracker.google.com	good	**IP:** 172.217.160.78 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
i.tddmp.com	good	**IP:** 116.196.71.30 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
me.xdrig.com	good	**IP:** 116.198.14.136 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
av1.xdrig.com	good	**IP:** 116.198.14.13 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
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
www.openssl.org	good	**IP:** 184.27.21.43 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map
cloud.xdrig.com	good	**IP:** 116.198.14.42 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:** 110.242.68.4 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
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
realm.io	good	**IP:** 65.9.42.110 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.606209 经度: -122.332069 查看地图: Google Map

URL线索

URL信息	Url所在文件
https://youyu-qinqin.oss-cn-shenzhen.aliyuncs.com/icon/1602487229333-200-61-1.jpg	com/yyjj/nnxx/nn_activity/NN_LaunchActivity.java

URL信息	Url所在文件
https://langu-ugirl.oss-cn-shenzhen.aliyuncs.com/icon/1602487229400-200-61-1.jpg	com/yyjj/nnxx/nn_activity/NN_LaunchActivity.java
https://www.baidu.com	cn/bingoogolapple/update/Engine.java
https://av1.xdrig.com/u/a/v1	c/b/a/f.java
https://cloud.xdrig.com/configcloud/rest/sdk/match	c/b/a/f.java
https://me.xdrig.com	c/b/a/i3.java
http://i.tddmp.com/a/	c/b/a/z3.java
www.talkingdata.net	c/b/a/p0.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	e/a/b0.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	e/a/s.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	e/a/l.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	e/a/c.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	e/a/k0.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	e/a/v0/f.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	e/a/v0/d.java
https://realm.io/docs/java/latest/#rxjava	io/realm/m0.java

URL信息	Url所在文件
https://realm.io/news/android-installation-change/	io/realm/g0.java
https://realm.io/docs/java/latest/#rxjava	io/realm/g0.java
https://issuetracker.google.com/issues/36918154	io/realm/c0.java
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/librealm-jni.so

邮箱线索

邮箱地址	所在文件
help@realm.io	lib/armeabi-v7a/librealm-jni.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.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.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。

向手机申请的权限	是否危险	类型	详细情况
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=111, ST=111, L=111, O=111, OU=111, CN=111
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-10-20 03:53:30+00:00
Valid To: 2045-10-14 03:53:30+00:00
Issuer: C=111, ST=111, L=111, O=111, OU=111, CN=111
Serial Number: 0x3274e887
Hash Algorithm: sha256
md5: cb473cb918a5a67b6de69d0bb88198a5
sha1: ed77b16d5f762099e3202d49e84f6b6131b1f986
sha256: 719f417c21f347fcfcbfb1c609373875959ed7519be8bb89badc3ce0e79f7792
sha512: a2df4654ae8fa884f14264beba48b2ad10c71f5db1babb51ab70990ccb7c7f289629f5c441e536dd3138a82952c45b5514eab6210c03317d150ddcf8f23507cf
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: e59daef51729b202066069dc59021e48fb6d6eca3c9c9c42587257d19875f8c5

Exodus威胁情报

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

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.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
Build.BRAND check
Build.DEVICE check
Build.PRODUCT check
possible Build.SERIAL check
SIM operator check
network operator name check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.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>