MoGua

Softsister 1.0.1.APK 分析报告

APP名称: Softsister

包名:	com.example.qhjci
域名线索:	7条
URL线索:	6条
邮箱线索:	5条
分析日期:	2024年11月7日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: base.apk
文件大小: 47.61MB
MD5值: f38546a0ecfea1bf4fa2666dc65369fe
SHA1值: 9e85f32d2b2ec4a4c1a3b268c2098fe3c89de205
SHA256值: b51b7eba343c83b7db4d3b42dc41596c6d766bd1ea6d81c52a84bc1f193ca8a8

APP 信息

App名称: Softsister
包名: com.example.qhjci
主活动Activity: com.example.qhjci.MainActivity
安卓版本名称: 1.0.1
安卓版本: 1

域名线索

域名	服务器信息
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
plus.google.com	**IP**: 199.59.148.7 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
api.flutter.dev	**IP**: 199.36.158.100 **所属国家**: United States of America **地区**: California

	城市: Mountain View **纬度**: 37.405991 **经度**: -122.078514
flutter.dev	**IP**: 199.36.158.100 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
softsister1026.s3.ap-northeast-3.amazonaws.com	**IP**: 52.95.181.17 **所属国家**: Japan **地区**: Osaka **城市**: Osaka **纬度**: 34.694218 **经度**: 135.502228
developer.android.com	**IP**: 142.251.211.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
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

URL线索

URL**信息**	Url**所在文件**

https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/c.java
https://plus.google.com/	a2/p1.java
https://github.com/flutter/flutter/issues.	lib/armeabi-v7a/libflutter.so
https://softsister1026.s3.ap-northeast-3.amazonaws.com/softsister	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues.	lib/x86_64/libflutter.so
https://github.com/flutter/flutter/issues.	lib/arm64-v8a/libflutter.so

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	x1/q.java
_cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring storationinformation@633124995.fromserial _list@0150898.of _httpparser@13463476.responsepa _typeerror@0150898._create _list@0150898._ofgrowabl _list@0150898._ofefficie	

_growablelist@0150898._ofarray _double@0150898.fromintege _growablelist@0150898._literal3 _future@4048458.immediate _growablelist@0150898._literal _growablelist@0150898._ofother _link@14069316.fromrawpat _growablelist@0150898.withcapaci _timer@1026248._internal _growablelist@0150898._literal6 _growablelist@0150898._literal5 _receiveportimpl@1026248.fromrawrec _list@0150898._ofarray _timer@1026248.periodic _growablelist@0150898._literal2 _bigintimpl@0150898.from _list@0150898.empty _list@0150898._ofother _bytebuffer@7027147._new _directory@14069316.fromrawpat _casterror@0150898._create _compressednode@240137193.single _invocationmirror@0150898._withtype ngstreamsubscription@4048458.zoned _assertionerror@0150898._create _nativesocket@14069316.normal _growablelist@0150898._literal1 _uri@0150898.file _uri@0150898.directory _growablelist@0150898._literal8 _file@14069316.fromrawpat _growablelist@0150898._literal4 _growablelist@0150898._ofgrowabl _growablelist@0150898.of _growablelist@0150898.generate _uri@0150898.notsimple _growablelist@0150898._literal7 _growablelist@0150898._ofefficie _hashcollisionnode@240137193.fromcollis _future@4048458.immediatee	lib/armeabi-v7a/libapp.so
_receiveportimpl@1026248.fromrawrec	lib/x86_64/libapp.so

appro@openssl.org	lib/arm64-v8a/libflutter.so
_receiveportimpl@1026248.fromrawrec	lib/arm64-v8a/libapp.so

手机线索

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=beijing, ST=beijing, L=beijing, O=ii1730714194394, OU=dp1730714194394, CN=grsx
签名算法: rsassa_pkcs1v15
有效期自: 2024-11-04 09:56:40+00:00
有效期至: 2074-10-23 09:56:40+00:00
发行人: C=beijing, ST=beijing, L=beijing, O=ii1730714194394, OU=dp1730714194394, CN=grsx
序列号: 0x63ef1931
哈希算法: sha512
md5值: ec906e6431c997911f00ed8865eb5234
sha1值: 703fb9aea3e9c02a28f5f0dde4220b2392a19e6b
sha256值: 0dd06b8c83563b4f6bd98655a005bc0ca84a9a56d1ced6c013abe1727306b1db
sha512值: 88350ab7aa2c5a60402587333d26e31cedf0f9d2a280012c0c966960c1242f6db215256d83b021203c484ff05231449421d4cb84587078b31ec32a1c8f45ec57
公钥算法: rsa
密钥长度: 4096
指纹: 5389264bc2a412c0c5f1768a1dc2f1024d2fd2d2c0b57fd8debee78af0b2ff36

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.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.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.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前

android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.READ_PHONE_NUMBERS	危险		允许到设备的读访问的电话号码。这是 READ_PHONE_STATE 授予的功能的一个子集,但对即时应用程序公开
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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
com.example.qhjci.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信