MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Chat Journal 1.8.0.APK

APP名称:	Chat Journal
包名:	com.agiletelescope.chatjournal
域名线索:	12条
URL线索:	13条
邮箱线索:	2条
分析日期:	2022年2月2日 22:36

文件信息

文件名: sjxrj.apk
文件大小: 9.21MB
MD5值: cef6e4f2641e3909908ff140290c4897
SHA1值: bd2a2006858e5391bbeaab896cfff90ef883cda8
SHA256值: bd2cbfd38cfe46996689877f899fcf1ccbf3846048769de921114ad8e68f82d5

APP 信息

App名称: Chat Journal
包名: com.agiletelescope.chatjournal
主活动**Activity:** com.example.cj_provider.MainActivity
安卓版本名称: 1.8.0
安卓版本: 59

域名线索

域名	是否危险域名	服务器信息
app-measurement.com	good	**IP:** 220.181.174.97 **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
firebase.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
goo.gl	good	**IP:** 142.251.43.14 **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
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
pagead2.googlesyndication.com	good	**IP:** 220.181.174.166 **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.google.com	good	**IP:** 199.16.156.11 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.773968 **经度:** -122.410446 **查看地图:** Google Map
google.com	good	**IP:** 142.251.43.14 **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
plus.google.com	good	**IP:** 108.160.163.112 **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
accounts.google.com	good	**IP:** 142.251.43.13 **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

域名	是否危险域名	服务器信息
chatjournalreal.firebaseio.com	good	**IP:** 35.201.97.85 **所属国家:** United States of America **地区:** Missouri **城市:** Kansas City **纬度:** 39.099731 **经度:** -94.578568 **查看地图:** Google Map
www.googleadservices.com	good	**IP:** 220.181.174.166 **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

URL线索

URL信息	Url所在文件
https://accounts.google.com/o/oauth2/revoke?token=	c/d/a/a/b/e/f/e/f.java

URL信息	Url所在文件
www.google.com	c/d/a/a/h/b/ca.java
https://www.google.com	c/d/a/a/h/b/ca.java
https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s	c/d/a/a/h/b/ca.java
https://goo.gl/NAOOOI.	c/d/a/a/h/b/ca.java
https://goo.gl/NAOOOI	c/d/a/a/h/b/ca.java
https://google.com/search?	c/d/a/a/h/b/j7.java
https://firebase.google.com/support/guides/disable-analytics	c/d/a/a/h/b/d4.java
https://app-measurement.com/a	c/d/a/a/h/b/q.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	c/d/a/a/a/a/b.java
https://plus.google.com/	c/d/a/a/d/p/o0.java
https://goo.gl/J1sWQy	c/d/a/a/g/g/ld.java
https://app-measurement.com/a	c/d/a/a/g/g/s8.java
https://github.com/flutter/flutter/issues/2897).It	io/flutter/plugin/platform/PlatformViewsController.java
https://github.com/flutter/flutter/issues/37025	io/flutter/view/FlutterView.java
https://chatjournalreal.firebaseio.com	Android String Resource

URL信息	Url所在文件
http://www.w3.org/XML/1998/namespace	lib/arm64-v8a/libflutter.so
http://www.w3.org/2000/xmlns/	lib/arm64-v8a/libflutter.so
https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).	lib/arm64-v8a/libflutter.so

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	c/d/a/a/d/e0.java
appro@openssl.org	lib/arm64-v8a/libflutter.so

数据库线索

FIREBASE链接地址	详细信息
https://chatjournalreal.firebaseio.com	info App talks to a Firebase Database.

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.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
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.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.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.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.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。

向手机申请的权限	是否危险	类型	详细情况
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-10-07 11:51:43+00:00
Valid To: 2048-10-07 11:51:43+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x5de9a5be5b1cb131ac6d6a49b0eb633418248afa
Hash Algorithm: sha256
md5: 4fe3c0f20a0577b88468f4a89fce5270
sha1: d3493b654e9abe09ec1232bb9a4df016e96b89cb
sha256: 10a341d86306a7daec1c0a645e271ebd4acf6c0d8e634a0bad03891a08172cd0
sha512: 2b851e49065e876fa9929f3b524b941bd31a9a024a85fdd8ac88056c4ede4ac5bc73f9c0d3af3b3deca37f674319c3fd829e3ace4b00e415d3a4df01308c9d5c
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: a3ae801dbe10849a08213176bbed249c253d15a393440fb0b8f174c48bfdddc0

Exodus威胁情报

名称	分类	URL链接
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

硬编码敏感信息

可能的敏感信息
"firebase_database_url" : "https://chatjournalreal.firebaseio.com"
"google_api_key" : "AIzaSyDN56JJETLRDZz2zTv35iNxSvw72OyGm7M"
"google_crash_reporting_api_key" : "AIzaSyDN56JJETLRDZz2zTv35iNxSvw72OyGm7M"

加壳分析

文件列表	分析结果

<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.MANUFACTURER check
Build.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>编译器</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>
