MoGua

双碳 1.0.0.APK 分析报告

APP名称:	双碳

包名:	com.st.stpro
域名线索:	16条
URL线索:	16条
邮箱线索:	2条
分析日期:	2024年9月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 2_base.apk
文件大小: 19.95MB
MD5值: da0d7918f408c789febfd4b535501df4
SHA1值: fa4d649c10e889ac858d3d920557f2c67450d338
SHA256值: dad71ac7362795cb4e834d2fb6d63db228086dc58e5e97b26013475b76db5680

APP 信息

App名称: 双碳
包名: com.st.stpro
主活动Activity: com.st.stpro.MainActivity
安卓版本名称: 1.0.0
安卓版本: 1

域名线索

域名	服务器信息
developer.android.com	**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
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
exoplayer.dev	**IP**: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania

	城市: California **纬度**: 40.065632 **经度**: -79.891708
www.ibm.com	**IP**: 23.2.140.161 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689507 **经度**: 139.691696
ns.adobe.com	没有服务器地理信息.
ea07618e922a4d67.natapp.cc	没有服务器地理信息.
www.w3.org	**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
journeyapps.com	**IP**: 13.224.141.49 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689507 **经度**: 139.691696
developer.apple.com	**IP**: 17.253.75.204 **所属国家**: Japan **地区**: Osaka **城市**: Osaka **纬度**: 34.693890 **经度**: 135.502213
aomedia.org	**IP**: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania

	城市: California **纬度**: 40.065632 **经度**: -79.891708
banshou311.oss-cn-hangzhou.aliyuncs.com	**IP**: 47.110.177.142 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
appupdate.shou01.cn	没有服务器地理信息.
geturl.shou01.cn	没有服务器地理信息.
github.com	**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
schemas.microsoft.com	**IP**: 13.107.213.49 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
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

URL线索

URL信息	Url所在文件
http://ns.adobe.com/xap/1.0/	b/d/a/a.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	c/d/a/a/e2.java
https://exoplayer.dev/issues/cleartext-not-permitted	c/d/a/a/e4/d0.java
https://aomedia.org/emsg/ID3	c/d/a/a/z3/j/a.java
https://developer.apple.com/streaming/emsg-id3	c/d/a/a/z3/j/a.java
http://ns.adobe.com/xap/1.0/	c/d/a/a/x3/i0/a.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	c/d/a/a/w3/l0.java
https://x	c/d/a/a/w3/k0.java
http://www.w3.org/ns/ttml#parameter	c/d/a/a/c4/t/c.java
https://github.com/flutter/flutter/issues/2897).It	io/flutter/plugin/platform/l.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/e.java
https://developer.android.com/reference/javax/net/ssl/SSLSocket	io/flutter/plugins/d/t.java
https://journeyapps.com/	Android String Resource
https://github.com/journeyapps/zxing-android-embedded	Android String Resource
http://www.w3.org/XML/1998/namespace	lib/armeabi-v7a/libflutter.so

http://www.w3.org/2000/xmlns/	lib/armeabi-v7a/libflutter.so
https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues.	lib/armeabi-v7a/libflutter.so
https://appupdate.shou01.cn/down/shuangtan/android/app-release.apk	lib/armeabi-v7a/libapp.so
https://geturl.shou01.cn/url.json	lib/armeabi-v7a/libapp.so
http://ea07618e922a4d67.natapp.cc:28081/register?code=	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html	lib/armeabi-v7a/libapp.so
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
http://www.w3.org/1998/Math/MathML	lib/armeabi-v7a/libapp.so
https://appupdate.shou01.cn/down/configure.json	lib/armeabi-v7a/libapp.so
http://www.w3.org/2000/svg	lib/armeabi-v7a/libapp.so
http://www.w3.org/2000/xmlns/	lib/armeabi-v7a/libapp.so
https://banshou311.oss-cn-hangzhou.aliyuncs.com/upload/1/index.mp4	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
http://ea07618e922a4d67.natapp.cc:28081/renren-api	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.	lib/armeabi-v7a/libapp.so
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
https://github.com/flutter/flutter/issues.	lib/arm64-v8a/libflutter.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so

邮箱线索

邮箱地址	所在文件
_httpparser@13463476.responsepa _double@0150898.fromintege ._future@4048458.immediate _growablelist@0150898._literal storationinformation@651124995.fromserial _link@14069316.fromrawpat c_growablelist@0150898.withcapaci _growablelist@0150898._literal6 _receiveportimpl@1026248.fromrawrec z_timer@1026248.periodic m_growablelist@0150898._literal2 g_bigintimpl@0150898.from _list@0150898.empty _directory@14069316.fromrawpat _casterror@0150898._create l_invocationmirror@0150898._withtype _growablelist@0150898._literal1 4_uri@0150898.file _growablelist@0150898._literal4 bb_growablelist@0150898._ofgrowabl x_growablelist@0150898.of 3_list@0150898._ofimmutab v_utf8encoder@9003594.withbuffer _growablelist@0150898._ofimmutab	

_cookie@13463476.fromsetcoo n_listconfig@806282418.frombuildm authenticationscheme@13463476.fromstring _list@0150898.of _growablelist@0150898._withdata _list@0150898.generate n_typeerror@0150898._create _list@0150898._ofgrowabl _list@0150898._ofefficie _growablelist@0150898._literal3 u_growablelist@0150898._ofother _list@0150898._oflist _timer@1026248._internal _growablelist@0150898._literal5 lectiontoolbarbutton@364113492.text _list@0150898._ofother eo_bytebuffer@7027147._new lectiontoolbarbutton@244392285.text ngstreamsubscription@4048458.zoned _assertionerror@0150898._create av_nativesocket@14069316.normal _uri@0150898.directory qd_growablelist@0150898._literal8 v_file@14069316.fromrawpat gh_growablelist@0150898.generate _uri@0150898.notsimple 7u_growablelist@0150898._literal7 __growablelist@0150898._ofefficie _future@4048458.immediatee m_growablelist@0150898._oflist	lib/armeabi-v7a/libapp.so
appro@openssl.org	lib/arm64-v8a/libflutter.so

手机线索

手机号	所在文件

17512775099	c/d/b/c/a.java

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: ST=shenzhen, L=shenzhen, O=no, OU=no, CN=wenzi
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-02-18 13:59:05+00:00
Valid To: 2047-02-12 13:59:05+00:00
Issuer: ST=shenzhen, L=shenzhen, O=no, OU=no, CN=wenzi
Serial Number: 0x3788fae1
Hash Algorithm: sha256
md5: 0ab733c40f6bd8dffdf4eca2501d273e
sha1: 49bb8386e34e8d61ef0294a875050b98481cee6f
sha256: bdf40b6c04af642e696d6a272ed93ef2104f255a61827a1311c9777056c665d7
sha512: c565654cbeaced7e14cadaced5015a1ba05ea5693e9ac9b4d7ffd43c5b42a517467bde325af5bfa0b23f9a6d187e76e34e6a00f3bcc00e1dbf9449eea6476af6
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: eb8177ecbddd8950a385834390ca46486218d3c7f3dda91c1a88685b6f13590b

硬编码敏感信息

可能的敏感信息
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

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.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.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
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.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。

应用内通信

报告由 **摸瓜**APK**反编译平台** 自动生成，并非包含所有检测结果，有疑问请联系管理员。