MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

E起发 2.3.0.APK

APP名称:	E起发
包名:	com.eqf.share
域名线索:	11条
URL线索:	3条
邮箱线索:	0条
分析日期:	2022年1月20日 21:51

文件信息

文件名: eqifa.apk
文件大小: 12.49MB
MD5值: a4933e0d54dc2cbeb25ddaed0a3ef737
SHA1值: 5146e1c27ee39eea0bc73ce961112e891e8ba1ad
SHA256值: 0dc73e5fb7e8b24dc8f4369f7d16bac75cce34f7af490a48765d8ea144f1c61a

APP 信息

App名称: E起发
包名: com.eqf.share
主活动**Activity:** com.eqf.share.ui.SplashActivity
安卓版本名称: 2.3.0
安卓版本: 22

域名线索

域名	是否危险域名	服务器信息
d1.client.map.bdimg.com	good	**IP:** 221.194.182.35 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map

域名	是否危险域名	服务器信息
v.map.baidu.com	good	**IP:** 111.206.209.185 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
sv0.map.bdimg.com	good	**IP:** 111.206.209.186 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.map.baidu.com	good	**IP:** 111.206.208.72 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
client.map.baidu.com	good	**IP:** 111.206.209.119 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
itsmap3.baidu.com	good	**IP:** 153.37.235.49 所属国家: China 地区: Jiangsu 城市: Suzhou 纬度: 31.311390 经度: 120.618057 查看地图: Google Map
www.umeng.com	good	**IP:** 59.82.29.249 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
wp.map.baidu.com	good	**IP:** 111.206.209.185 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
vector0.map.bdimg.com	good	**IP:** 221.194.182.35 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map

域名	是否危险域名	服务器信息
sv.map.baidu.com	good	**IP:** 111.206.209.186 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
newvector.map.baidu.com	good	**IP:** 111.206.209.171 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

URL线索

URL信息	Url所在文件
www.umeng.com/social	Android String Resource
http://client.map.baidu.com/imap/sdk/tj?qt=vmap	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/statistics/v1/	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
https://v.map.baidu.com/low/	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
https://v.map.baidu.com/indoorinside/	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so

URL信息	Url所在文件
https://v.map.baidu.com/high/	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
https://newvector.map.baidu.com/grid_vc/	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
http://vector0.map.bdimg.com/vecdata/	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
https://itsmap3.baidu.com/its.php	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
http://wp.map.baidu.com/	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
http://api.map.baidu.com/sdkws/heatmap?	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
https://client.map.baidu.com/footmap/image.php?	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
https://sv.map.baidu.com/	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
http://sv0.map.bdimg.com/	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
https://client.map.baidu.com/phpui2/?	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
https://client.map.baidu.com/offline-search/?	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
http://d1.client.map.bdimg.com/offline-search/?	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
https://newvector.map.baidu.com/travel_vc/	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
https://newvector.map.baidu.com/inst_grid/	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
https://client.map.baidu.com/phpui2/	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so

URL信息	Url所在文件
https://client.map.baidu.com/?qt=rg&mmproxyver=1&url=	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=	lib/armeabi-v7a/libBaiduMapSDK_map_v4_2_0.so
http://client.map.baidu.com/imap/sdk/tj?qt=vmap	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/statistics/v1/	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
https://v.map.baidu.com/low/	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
https://v.map.baidu.com/indoorinside/	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
https://v.map.baidu.com/high/	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
https://newvector.map.baidu.com/grid_vc/	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
http://vector0.map.bdimg.com/vecdata/	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
https://itsmap3.baidu.com/its.php	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
http://wp.map.baidu.com/	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
http://api.map.baidu.com/sdkws/heatmap?	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
https://client.map.baidu.com/footmap/image.php?	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
https://sv.map.baidu.com/	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
http://sv0.map.bdimg.com/	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so

URL信息	Url所在文件
https://client.map.baidu.com/phpui2/?	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
https://client.map.baidu.com/offline-search/?	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
http://d1.client.map.bdimg.com/offline-search/?	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
https://newvector.map.baidu.com/travel_vc/	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
https://newvector.map.baidu.com/inst_grid/	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
https://client.map.baidu.com/phpui2/	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
https://client.map.baidu.com/?qt=rg&mmproxyver=1&url=	lib/armeabi/libBaiduMapSDK_map_v4_2_0.so
http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=	lib/armeabi/libBaiduMapSDK_map_v4_2_0.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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

向手机申请的权限	是否危险	类型	详细情况
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
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_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.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.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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.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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
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.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息

向手机申请的权限	是否危险	类型	详细情况
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
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
android.permission.SET_DEBUG_APP	危险	启用应用程序调试	允许一个应用程序打开另一个应用程序的调试。恶意应用程序可以使用它来杀死其他应用程序
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证令牌
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作
getui.permission.GetuiService.com.eqf.share	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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=US, O=Android, CN=Android Debug
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-09-02 06:05:03+00:00
Valid To: 2044-08-25 06:05:03+00:00
Issuer: C=US, O=Android, CN=Android Debug
Serial Number: 0x37a41347
Hash Algorithm: sha256
md5: a82164e7887fd73b0d742de73a0417f5
sha1: 151d67dede828a28e93c3b1687f6dd774c306a37
sha256: 12187093af2ab07812eb4bc14b4c7c1efac006628f44c20351a3ceaef4f27ff0
sha512: 46c6b3e255e81bb60c6e11375635854af27da18f4f73664219c7257562b032f2bdd53c326813b6130873685f9d6da7873655539e9201123a6dc33dd4acff9fc1

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent1105603711://,

加壳分析

文件列表	分析结果
APK包	壳列表 / 详细情况 打包 / Jiagu
classes.dex	壳列表 / 详细情况 编译器 / dexlib 2.x
