MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

超级准指南针 3.2.4.APK

APP名称:	超级准指南针
包名:	com.bee.scompass
域名线索:	29条
URL线索:	41条
邮箱线索:	0条
分析日期:	2022年1月26日 18:46

文件信息

文件名: cjzznz.apk
文件大小: 6.34MB
MD5值: 5ceeb1fd7db326ef86b08bf6fdffd0dd
SHA1值: 1897e284c6a1041568a18e5e05c444c9bc7e0d2d
SHA256值: ab3901d75bc40bd141253bf66d9040e8e131dadee58b8900b63c90bf73c39ab8

APP 信息

App名称: 超级准指南针
包名: com.bee.scompass
主活动**Activity:** com.bee.scompass.SplashActivity
安卓版本名称: 3.2.4
安卓版本: 30204

域名线索

域名	是否危险域名	服务器信息
dualstack-arestapi.amap.com	good	**IP:** 39.98.22.142 **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

域名	是否危险域名	服务器信息
gwtools.redbeeai.com	good	**IP:** 101.132.188.145 **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
ulogs.umeng.com	good	**IP:** 106.11.43.142 **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
tianqi.redbeeai.com	good	**IP:** 139.224.63.151 **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
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

域名	是否危险域名	服务器信息
aaid.umeng.com	good	**IP:** 111.225.159.27 **所属国家:** China **地区:** Hebei **城市:** Zhangjiakou **纬度:** 40.810001 **经度:** 114.879440 **查看地图:** Google Map
apilocate.amap.com	good	**IP:** 59.82.60.15 **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
errlog.umeng.com	good	**IP:** 106.8.130.60 **所属国家:** China **地区:** Hebei **城市:** Zhangjiakou **纬度:** 40.810001 **经度:** 114.879440 **查看地图:** Google Map
astat.bugly.cros.wr.pvp.net	good	**IP:** 170.106.135.32 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.774929 **经度:** -122.419418 **查看地图:** Google Map

域名	是否危险域名	服务器信息
android.bugly.qq.com	good	**IP:** 109.244.244.137 **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
alogus.umeng.com	good	**IP:** 106.11.43.144 **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
ouplog.umeng.com	good	**IP:** 47.74.172.218 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
alogsus.umeng.com	good	**IP:** 106.11.86.76 **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

域名	是否危险域名	服务器信息
pslog.umeng.com	good	**IP:** 59.82.31.92 **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
data.redbeeai.com	good	**IP:** 139.196.7.170 **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
ns.adobe.com	good	没有服务器地理信息.
restsdk.amap.com	good	**IP:** 106.11.43.113 **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
ulogs.umengcloud.com	good	**IP:** 203.119.174.133 **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
abroad.apilocate.amap.com	good	**IP:** 59.82.39.53 **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
cgicol.amap.com	good	**IP:** 59.82.31.104 **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
feedback.redbeeai.com	good	**IP:** 47.102.147.84 **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
schemas.android.com	good	没有服务器地理信息.
errlogos.umeng.com	good	**IP:** 47.246.110.18 **所属国家:** Hong Kong **地区:** Hong Kong **城市:** Hong Kong **纬度:** 22.285521 **经度:** 114.157692 **查看地图:** Google Map

域名	是否危险域名	服务器信息
dualstack-a.apilocate.amap.com	good	**IP:** 106.11.40.50 **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
astat.bugly.qcloud.com	good	**IP:** 150.109.29.135 **所属国家:** Korea (Republic of) **地区:** Seoul-teukbyeolsi **城市:** Seoul **纬度:** 37.568260 **经度:** 126.977829 **查看地图:** Google Map
lbs.amap.com	good	**IP:** 59.82.31.202 **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
developer.umeng.com	good	**IP:** 59.82.31.95 **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
plbslog.umeng.com	good	**IP:** 59.82.43.171 **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
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

URL线索

URL信息	Url所在文件
https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/a/i/c.java
https://errlogos.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/a/d/a.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/a/d/a.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java

URL信息	Url所在文件
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/i.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/c.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/c.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明	com/amap/api/location/AMapLocation.java

URL信息	Url所在文件
https://www.baidu.com	com/kit/func/FunctionKit.java
https://tianqi.redbeeai.com/Api/common/Earthquake	com/kit/func/http/IFuncKitService.java
https://data.redbeeai.com/	com/kit/func/http/ApiService.java
https://errlogos.umeng.com/upload	com/uc/crashsdk/e.java
https://errlog.umeng.com/upload	com/uc/crashsdk/e.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
https://errlogos.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
https://errlog.umeng.com	com/uc/crashsdk/a/d.java
https://errlogos.umeng.com	com/uc/crashsdk/a/d.java
http://gwtools.redbeeai.com/supercompass/html/agreeandprivate/private.html	b/b/a/e/a.java
http://gwtools.redbeeai.com/supercompass/html/agreeandprivate/agree.html	b/b/a/e/a.java
http://schemas.android.com/apk/res-auto	b/e/a/a/k/a.java
http://apilocate.amap.com/mobile/binary	b/i/o3.java
http://dualstack-a.apilocate.amap.com/mobile/binary	b/i/o3.java
http://abroad.apilocate.amap.com/mobile/binary	b/i/o3.java

URL信息	Url所在文件
http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&	b/i/e1.java
http://dualstack-arestapi.amap.com/v3/geocode/regeo	b/i/j3.java
http://restsdk.amap.com/v3/geocode/regeo	b/i/j3.java
https://restsdk.amap.com/v3/iasdkauth	b/i/d4.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	b/i/d4.java
http://abroad.apilocate.amap.com/mobile/binary	b/i/h3.java
http://abroad.apilocate.amap.com/mobile/binary	b/i/s3.java
http://restsdk.amap.com	b/i/k4.java
http://restsdk.amap.com/v3/place/text?	b/i/a.java
http://restsdk.amap.com/v3/config/district?	b/i/a.java
http://restsdk.amap.com/v3/place/around?	b/i/a.java
http://feedback.redbeeai.com	b/d/a/g/b.java
https://feedback.redbeeai.com	b/d/a/g/b.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	c/a/z.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	c/a/i0.java

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/Plugins	c/a/j.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	c/a/q.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	c/a/a.java
http://schemas.android.com/apk/res/android	a/j/c/l/i.java
http://ns.adobe.com/xap/1.0/	a/p/a/a.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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。
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.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
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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=chif
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-11-24 03:03:46+00:00
Valid To: 2120-10-31 03:03:46+00:00
Issuer: CN=chif
Serial Number: 0xb0372bc
Hash Algorithm: sha256
md5: d16fee776451e070a695289af952531d
sha1: 35638a41c2c5dedcb4419e9e3032911dc27dbc40
sha256: 471f209d7c513653c69b5b3674928d4ec9757e971f826d66cd6b6ff13d730bd7
sha512: 544cf97ab91dfa616cb982c60d565154a80f6b6d84f71e4e59a38e0cac5e5cfb3fb555e509af3bda4decf6b1624c7756b5336f5b6541eb580418a69d2197ef92
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 91eab2d2985d4642cb68eaeb2ead22e1d7d280bd54ffb788c42193f348ee0f6b

Exodus威胁情报

名称	分类	URL链接
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

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.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
subscriber ID check
emulator file 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>
