MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

百汇达 1.0.APK

APP名称:	百汇达
包名:	com.baihui.home
域名线索:	32条
URL线索:	39条
邮箱线索:	0条
分析日期:	2022年1月25日 21:38

文件信息

文件名: baihuida.apk
文件大小: 4.54MB
MD5值: 91e9baa09c717f9823e24d1c6293ef53
SHA1值: d820d60f613f52794d0a82b6edcc27d3e438937e
SHA256值: a73b9871365eae11a4bd25740472a8fdfa4e0213f94d3878fc12a01df3487b29

APP 信息

App名称: 百汇达
包名: com.baihui.home
主活动**Activity:** com.hongbi.tech.SplashActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
adiu.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

域名	是否危险域名	服务器信息
dualstack.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
mobilegw.alipay.com	good	**IP:** 203.209.245.78 **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
app-router.leancloud.cn	good	**IP:** 106.75.81.168 **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
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
mst0d.is.autonavi.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
m.alipay.com	good	**IP:** 203.209.245.74 **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
mcgw.alipay.com	good	**IP:** 203.209.250.6 **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
apiinit.amap.com	good	**IP:** 203.119.175.194 **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
wb.amap.com	good	**IP:** 59.82.60.46 **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
webrd0d.is.autonavi.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
lbs.amap.com	good	**IP:** 59.82.31.203 **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
m5.amap.com	good	**IP:** 106.11.43.74 **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
dualstack-restapi.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
yuntuapi.amap.com	good	没有服务器地理信息.
aps.testing.amap.com	good	**IP:** 140.205.69.9 **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
www.yunyixaiou.com	good	没有服务器地理信息.
tm.amap.com	good	**IP:** 59.82.31.100 **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
www.jierankeji.com	good	**IP:** 103.59.145.167 **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
h5.m.taobao.com	good	**IP:** 60.21.152.107 **所属国家:** China **地区:** Liaoning **城市:** Dandong **纬度:** 40.129169 **经度:** 124.394722 **查看地图:** Google Map
hydra.alibaba.com	good	**IP:** 203.119.169.227 **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
grid.amap.com	good	**IP:** 140.205.172.75 **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
kaiyunli.com	good	没有服务器地理信息.
wprd0d.is.autonavi.com	good	没有服务器地理信息.
s.s.s	good	没有服务器地理信息.
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
restapi.amap.com	good	**IP:** 203.119.175.194 **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
upload.qiniu.com	good	**IP:** 180.101.136.32 **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

域名	是否危险域名	服务器信息
mobilegw.stable.alipay.net	good	没有服务器地理信息.
wap.amap.com	good	**IP:** 61.182.130.222 **所属国家:** China **地区:** Hebei **城市:** Shijiazhuang **纬度:** 38.041389 **经度:** 114.478607 **查看地图:** Google Map
xmlpull.org	good	**IP:** 74.50.61.58 **所属国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.814899 **经度:** -96.879204 **查看地图:** Google Map
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

URL线索

URL信息	Url所在文件
http://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
http://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/c.java
http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$&	com/alipay/sdk/data/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/security/mobile/module/a/a/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/face/APSecuritySdk.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/face/APSecuritySdk.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/face/APSecuritySdk.java
https://app-router.leancloud.cn/2/route?appId=	com/avos/avoscloud/AppRouterManager.java
http://upload.qiniu.com/bput/%s/%d	com/avos/avoscloud/upload/QiniuUploader.java
http://upload.qiniu.com/mkblk/%d	com/avos/avoscloud/upload/QiniuUploader.java
http://upload.qiniu.com	com/avos/avoscloud/upload/QiniuUploader.java
http://upload.qiniu.com/mkfile/%d/key/%s	com/avos/avoscloud/upload/QiniuUploader.java
http://upload.qiniu.com	com/avos/avoscloud/upload/QiniuAccessor.java
http://apilocate.amap.com/mobile/binary	com/loc/en.java

URL信息	Url所在文件
http://dualstack.apilocate.amap.com/mobile/binary	com/loc/en.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/en.java
http://restapi.amap.com	com/loc/s.java
https://adiu.amap.com/ws/device/adius	com/loc/av.java
http://dualstack-restapi.amap.com/v3/geocode/regeo	com/loc/ei.java
http://restapi.amap.com/v3/geocode/regeo	com/loc/ei.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/eg.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/er.java
https://restapi.amap.com/v3/iasdkauth	com/loc/l.java
http://restapi.amap.com/v3/iasdkauth	com/loc/l.java
http://aps.testing.amap.com/collection/collectData?src=baseCol&ver=v74&	com/loc/cf.java
http://restapi.amap.com/v3/place/text?	com/loc/a.java
http://restapi.amap.com/v3/place/around?	com/loc/a.java
http://restapi.amap.com/v3/config/district?	com/loc/a.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明	com/autonavi/amap/mapcore2d/Inner_3dMap_location.java

URL信息	Url所在文件
http://hydra.alibaba.com/	com/ta/utdid2/aid/AidRequester.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/XmlUtils.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/FastXmlSerializer.java
http://apiinit.amap.com/v3/log/init	com/amap/api/services/a/bh.java
http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0	com/amap/api/services/a/bb.java
http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0	com/amap/api/services/a/bb.java
http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0	com/amap/api/services/a/bb.java
http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0	com/amap/api/services/a/bb.java
https://restapi.amap.com/v3/iasdkauth	com/amap/api/services/a/bg.java
http://restapi.amap.com/v3/iasdkauth	com/amap/api/services/a/bg.java
https://adiu.amap.com/ws/device/adius	com/amap/api/services/a/dc.java
http://restapi.amap.com/v3	com/amap/api/services/a/i.java
https://restapi.amap.com/v3	com/amap/api/services/a/i.java
http://restapi.amap.com/v4	com/amap/api/services/a/i.java
https://restapi.amap.com/v4	com/amap/api/services/a/i.java

URL信息	Url所在文件
http://yuntuapi.amap.com	com/amap/api/services/a/i.java
https://yuntuapi.amap.com	com/amap/api/services/a/i.java
http://m5.amap.com/ws/mapapi/shortaddress/transform	com/amap/api/services/a/i.java
https://m5.amap.com/ws/mapapi/shortaddress/transform	com/amap/api/services/a/i.java
http://restapi.amap.com	com/amap/api/services/a/bn.java
http://restapi.amap.com	com/amap/api/mapcore2d/cy.java
http://tm.amap.com	com/amap/api/mapcore2d/ax.java
http://wprd0%d.is.autonavi.com	com/amap/api/mapcore2d/ax.java
http://webrd0%d.is.autonavi.com	com/amap/api/mapcore2d/ax.java
http://grid.amap.com/grid/%d/%d/%d?ds=	com/amap/api/mapcore2d/ax.java
http://mst0%d.is.autonavi.com	com/amap/api/mapcore2d/ax.java
https://adiu.amap.com/ws/device/adius	com/amap/api/mapcore2d/eq.java
http://apilocate.amap.com/mobile/binary	com/amap/api/mapcore2d/gu.java
http://apiinit.amap.com/v3/log/init	com/amap/api/mapcore2d/cs.java
https://restapi.amap.com/v3/iasdkauth	com/amap/api/mapcore2d/cr.java

URL信息	Url所在文件
http://restapi.amap.com/v3/iasdkauth	com/amap/api/mapcore2d/cr.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
http://wap.amap.com/	com/amap/api/maps2d/AMapUtils.java
https://kaiyunli.com/index/shen/xqys?id=16	com/hongbi/tech/WebViewActivity.java
https://www.jierankeji.com/h5/#/	com/hongbi/tech/WebViewActivity.java
https://www.jierankeji.com/h5/#/pages/index/allgoods	com/hongbi/tech/WebViewActivity.java
https://www.jierankeji.com/h5/#/pages/index/user	com/hongbi/tech/WebViewActivity.java
https://www.yunyixaiou.com	com/hongbi/tech/SplashActivity.java

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.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

向手机申请的权限	是否危险	类型	详细情况
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_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.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_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_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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=asf, ST=asfa, L=sf, O=asfasa, OU=afa, CN=adafa
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-06-08 04:30:32+00:00
Valid To: 2046-06-02 04:30:32+00:00
Issuer: C=asf, ST=asfa, L=sf, O=asfasa, OU=afa, CN=adafa

Serial Number: 0x184963d8
Hash Algorithm: sha256
md5: 8318a15be2dc5717730b4ea9677a15ec
sha1: f9b8d0ec3bc9d361e7fd5b36ac082040685b8437
sha256: 9cc73afce698fca8be278b14a7d9f5d42cd3684730e7808c6b8b32b672c96949
sha512: 60bea1441c34f6790038f08c977e256b03a2217b09283c195516f50f6ac1129b4f818af1c5bfa397bfaf37a5fc322a0ab25796c26691ad8a3d12a97bdb84acd2
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 6e7e0a2ac53441b628ffe71023b0cdd7c22e62de5e60906a44dce55f8a876f92

Exodus威胁情报

名称	分类	URL链接
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361

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.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
SIM operator check
network operator name check
device ID check
subscriber ID check
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>

报告由 摸瓜平台 自动生成，并非包含所有检测结果，有疑问请联系管理员。

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析