MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

拆氪 1.0.8.APK

APP名称:	拆氪
包名:	chaiduoduo.top
域名线索:	22条
URL线索:	20条
邮箱线索:	0条
分析日期:	2022年1月18日 23:13

文件信息

文件名: de4df8a8675e90db7f9575ce9b7c7582.apk
文件大小: 7.0MB
MD5值: de4df8a8675e90db7f9575ce9b7c7582
SHA1值: d0ab0d6b9dc141e8805439420f703ae9e8c0830b
SHA256值: 9686f77f6d089c5c789e5d2fd8669d9842a6e15fe9d43e69d020967899be1ca6

APP 信息

App名称: 拆氪
包名: chaiduoduo.top
主活动**Activity:** chaiduoduo.top.StartPageActivity
安卓版本名称: 1.0.8
安卓版本: 10002

域名线索

域名	是否危险域名	服务器信息
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
pingma.qq.com	good	**IP:** 119.45.78.184 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
mobilegw.aaa.alipay.net	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
bjuser.jpush.cn	good	**IP:** 122.9.9.94 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
www.chaike.shop	good	**IP:** 47.100.92.151 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
ce3e75d5.jpush.cn	good	**IP:** 183.232.58.243 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map
mobilegw.alipaydev.com	good	**IP:** 110.75.132.131 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
h5.m.taobao.com	good	IP: 219.147.75.137 所属国家: China 地区: Heilongjiang 城市: Harbin 纬度: 45.750000 经度: 126.650002 查看地图: Google Map
xmlpull.org	good	IP: 74.50.62.60 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
mobilegw.stable.alipay.net	good	没有服务器地理信息.
wappaygw.alipay.com	good	IP: 203.209.250.50 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
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

域名	是否危险域名	服务器信息
mobilegw.alipay.com	good	IP: 203.209.255.238 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: 203.209.250.50 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
tsis.jpush.cn	good	IP: 121.36.74.75 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map
mta.qq.com	good	IP: 111.161.14.94 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map

域名	是否危险域名	服务器信息
mclient.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
sandcash.mixienet.com.cn	good	IP: 183.131.200.249 所属国家: China 地区: Zhejiang 城市: Jinhua 纬度: 30.013470 经度: 120.288658 查看地图: Google Map
open.weixin.qq.com	good	IP: 175.24.209.30 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
mta.oa.com	good	IP: 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690 查看地图: Google Map

域名	是否危险域名	服务器信息
long.open.weixin.qq.com	good	IP: 109.244.216.15 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
182.92.20.189	good	IP: 182.92.20.189 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
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java

URL信息	Url所在文件
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/d.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
http://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/b/a/e.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/b/a/a.java
https://sandcash.mixienet.com.cn/h5/?	com/pay/paytypelibrary/PayUtil.java
http://www.chaike.shop/#/private?ver=	chaiduoduo/top/WebViewActivity.java

URL信息	Url所在文件
http://www.chaike.shop/#/terms?ver=	chaiduoduo/top/WebViewActivity.java
http://www.chaike.shop/index.html?ver=	chaiduoduo/top/MainActivity.java
https://bjuser.jpush.cn/v2/appawake/status	cn/jiguang/ai/b.java
https://tsis.jpush.cn	cn/jiguang/ao/i.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/aj/d.java
http://182.92.20.189:9099/	cn/jiguang/r/a.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.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

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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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
com.huawei.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
android.permission.DELETE_CACHE_FILES	系统需要	删除其他应用程序缓存	允许应用程序删除缓存文件
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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=20000, ST=上海, L=上海, O=上海彩兜兜网络科技有限公司, OU=上海彩兜兜网络科技有限公司, CN=彩兜兜
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-07-20 08:47:03+00:00
Valid To: 2046-07-14 08:47:03+00:00
Issuer: C=20000, ST=上海, L=上海, O=上海彩兜兜网络科技有限公司, OU=上海彩兜兜网络科技有限公司, CN=彩兜兜
Serial Number: 0xd645bb0
Hash Algorithm: sha256
md5: f799c27d05380e7bef8d24a20ba5a5b3
sha1: c2a3f8150314fd17c54caab24111fba51d90a131
sha256: 57f2e8f6c82e0006fab653d8a6d75f80f9fe0bac730259818ed67474239d9e10
sha512: 7c62ab842833802f8ceb28cce5f8e7c247af89e54a58048cb1b029a882ca3a45cb2120455068a724fe95ad1f2a0f54ec6e82a013494c4311b402f45a591165f8
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c9ec1f66d9b78178657003e73b5938ae1be58b4c61fa3c9d33014bab9849cf5d

Exodus威胁情报

名称	分类	URL链接
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116

应用内通信

活动(ACTIVITY)	通信(INTENT)
chaiduoduo.top.MainActivity	Schemes: chaiduoduo://, Hosts: cdd,

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 反虚拟机: 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 device ID check subscriber ID check ro.product.device check ro.kernel.qemu check emulator file check 反调试: Debug.isDebuggerConnected() check 编译器: r8