MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

锤锤 0.1.APK

APP名称:	锤锤
包名:	com.jrsen.android.rimet
域名线索:	6条
URL线索:	8条
邮箱线索:	0条
分析日期:	2022年2月2日 19:28

文件信息

文件名: cc.apk
文件大小: 1.28MB
MD5值: f299583f8a54928a9c5e393c495180d5
SHA1值: 9dcda5d56b01bcc2f8946c516806457a37dec3b3
SHA256值: 2d909778b61be249bc114f87a56d71c1b8c4ce9780b762e85f8a3ef84961dbc2

APP 信息

App名称: 锤锤
包名: com.jrsen.android.rimet
主活动**Activity:** com.jrsen.android.rimet.MainActivity
安卓版本名称: 0.1
安卓版本: 1

域名线索

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

域名	是否危险域名	服务器信息
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
apilocatesrc.amap.com	good	IP: 59.82.31.183 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
lbs.amap.com	good	IP: 59.82.29.156 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
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
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

URL线索

URL信息	Url所在文件
http://abroad.apilocate.amap.com/mobile/binary	com/b/cn.java
https://adiu.amap.com/ws/device/adius	com/b/aj.java
http://abroad.apilocate.amap.com/mobile/binary	com/b/cc.java
http://apilocatesrc.amap.com/mobile/binary	com/b/cc.java
https://restapi.amap.com/v3/iasdkauth	com/b/da.java
http://restapi.amap.com/v3/iasdkauth	com/b/da.java
http://apilocate.amap.com/mobile/binary	com/b/ci.java
http://abroad.apilocate.amap.com/mobile/binary	com/b/ci.java

URL信息	Url所在文件
http://restapi.amap.com	com/b/dg.java
http://restapi.amap.com/v3/geocode/regeo	com/b/cd.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明	com/amap/api/location/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.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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

向手机申请的权限	是否危险	类型	详细情况
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.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。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=BeiJing, L=HaiDian, O=BeiJingHaiDian Jrsen.LTD, OU=JrsenUnit, CN=Jrsen
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-07-05 14:35:07+00:00
Valid To: 2039-06-29 14:35:07+00:00
Issuer: C=CN, ST=BeiJing, L=HaiDian, O=BeiJingHaiDian Jrsen.LTD, OU=JrsenUnit, CN=Jrsen
Serial Number: 0x785b2bf1
Hash Algorithm: sha256
md5: 560606180833fa3a30fa082436092ecc
sha1: 44043c466a9768ffc161aa48ddea5ccaf2a39ed5
sha256: 9766f346f08d94664b81839d2c36a20aeaac73945db70bed0c9600180324f310
sha512: afcf30879c2a8079fec66969d5415754e570279587e5e98e512b17351c20acac9537e193446bc9d69557d571d87826f75d3246c370bdeed26adc58c7abaa3f76
PublicKey Algorithm: rsa

Bit Size: 2048
Fingerprint: 9d8dcec48f911621a85f009bbfbe990dad5766be7ffd163a463932f335227df0

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
classes.dex	壳列表 / 详细情况 反虚拟机: Build.MANUFACTURER check possible Build.SERIAL check SIM operator check network operator name check subscriber ID check 编译器: dx

---