MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

惠 收银台

惠米米 5.2.APK

APP名称:	惠米米
包名:	com.corefiretec.huimimi
域名线索:	15条
URL线索:	11条
邮箱线索:	1条
分析日期:	2022年2月2日 20:09

文件信息

文件名: huimimi537141.apk
文件大小: 5.38MB
MD5值: bab5503a250c8ed912f047e66057ae17
SHA1值: 600346ffcafe32c7cf072d717a304a938c4237da
SHA256值: 4beca3e8d920910bd8aeeeb3d5cc7a21c635c74d8338058d4fcd4f43a8a2abec

APP 信息

App名称: 惠米米
包名: com.corefiretec.huimimi
主活动**Activity:** com.corefiretec.mbupay.terminal.controller.WelcomeActivity
安卓版本名称: 5.2
安卓版本: 502

域名线索

域名	是否危险域名	服务器信息
s-gt.getui.com	good	**IP:** 183.131.7.107 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
fqr.mbupay.com	good	IP: 106.14.33.237 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
d.gt.igexin.com	good	IP: 183.134.98.71 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.mbupay.com	good	IP: 106.15.75.137 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
cmnsguider.yunos.com	good	IP: 203.119.169.224 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
uop.umeng.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
www.corefiretec.com	good	IP: 121.43.239.74 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
sdk.open.lbs.igexin.com	good	IP: 121.52.255.89 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
yzf.api.54ceo.com	good	IP: 119.23.146.167 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
c-hzgt2.getui.com	good	IP: 124.160.127.198 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
alog.umengcloud.com	good	IP: 106.11.40.44 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
log.umsns.com	good	IP: 59.82.31.154 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
sdk.open.phone.igexin.com	good	IP: 183.131.7.98 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
alog.umeng.com	good	IP: 59.82.29.246 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.baidu.com	good	IP: 110.242.68.3 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
http://alog.umeng.com/app_logs	com/umeng/analytics/a.java
http://alog.umengcloud.com/app_logs	com/umeng/analytics/a.java
https://uop.umeng.com	com/umeng/analytics/a.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/analytics/pro/an.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/e.java
http://log.umsns.com/	com/umeng/analytics/social/d.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/d.java
https://www.baidu.com	com/corefiretec/mbupay/terminal/http/RequestGenerator.java

URL信息	Url所在文件
https://app.mbupay.com/	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://fqr.mbupay.com/	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/aliMicroPay	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/aliPreCreate	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/orderClose	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/orderQuery	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/orderReverse	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://fqr.mbupay.com/app/pushClientClose	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://fqr.mbupay.com/app/pushClientOpen	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://fqr.mbupay.com/app/pushClientUpload	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/queryDayReport	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/queryDayReport2	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/queryOrderList	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/queryOrderTotal	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/queryOrderTotal2	com/corefiretec/mbupay/terminal/http/CommonUrl.java

URL信息	Url所在文件
https://app.mbupay.com/app/queryRefundList	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/refund	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/refundQuery	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/storeQrCode	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/syyLogin	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/syyUpdPwd	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/unifPayNative	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/unifPayQuery	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/unionPayMicroPay	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/version	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/wxMicroPay	com/corefiretec/mbupay/terminal/http/CommonUrl.java
https://app.mbupay.com/app/wxUnifiedOrder	com/corefiretec/mbupay/terminal/http/CommonUrl.java
http://www.corefiretec.com/skw_voice_manual.php	com/corefiretec/mbupay/terminal/controller/more/voice/VoiceManualActivity.java
http://www.corefiretec.com/ios_agreement.html	com/corefiretec/mbupay/terminal/controller/login/AgreementActivity.java
http://yzf.api.54ceo.com/api/v1/report_order/report.do?	com/huiyi/ypos/usdk/data/DSYPPara.java

URL信息	Url所在文件
http://sdk.open.phone.igexin.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://c-hzgt2.getui.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://sdk.open.lbs.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
http://d.gt.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
http://s-gt.getui.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://bi.	com/igexin/push/config/p.java
http://config.	com/igexin/push/config/p.java
http://stat.	com/igexin/push/config/p.java
http://log.	com/igexin/push/config/p.java
http://lbs.	com/igexin/push/config/p.java

邮箱线索

邮箱地址	所在文件
service@citicbankpay.com	com/corefiretec/mbupay/terminal/controller/more/AboutActivity.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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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

向手机申请的权限	是否危险	类型	详细情况
android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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.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.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。

向手机申请的权限	是否危险	类型	详细情况
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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
getui.permission.GetuiService.com.corefiretec.huimimi	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=86, ST=bj, L=bj, O=corefiretec, OU=corefiretec, CN=litang
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-08-13 08:30:31+00:00
Valid To: 2046-08-07 08:30:31+00:00
Issuer: C=86, ST=bj, L=bj, O=corefiretec, OU=corefiretec, CN=litang
Serial Number: 0x640bad18
Hash Algorithm: sha256
md5: f981ae9ac00c70e4ce6e6127352b6c62
sha1: 0b8c9cdfc4d23dda12bfa39cfe68393d8506e3e7
sha256: 2ad73135834a42e037a524c620ba7329614b662a1d583ba2e2acd6989109c7a5
sha512: 880039e5c795195f9f6cff955729f38a850855136d62c761d77c0b1b0ed4de70b87522c8884d2c7df48ca410f6e642c136a14be46503694d2ce43e53aebdda06
PublicKey Algorithm: rsa
Bit Size: 2048

Fingerprint: 384ecc4c09091442b935350cfbf41353db1248a13e0e89687571ab723647514e

Exodus威胁情报

名称	分类	URL链接
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

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 Build.BOARD check possible Build.SERIAL check network operator name check subscriber ID check 编译器: r8