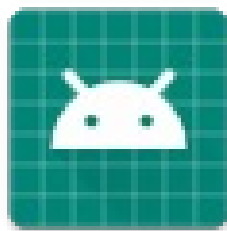




MoGua

e充电 1.0.APK 分析报告



APP名称:

e充电

包名:

域名线索:

28条

URL线索:

8条

邮箱线索:

2条

分析日期:

2025年6月18日

分析平台:

[摸瓜APK反编译平台](#)



文件信息

文件名: e充电.apk

文件大小: 94.47MB
MD5值: 8126998d87691ba2e4654fe429ada393
SHA1值: 7b3c02f6b3d9d2424c24ec420d91ef20471e10e9
SHA256值: fe345fc17d0b74271a85485391dc9f32e676fa73074fbbc634e7f2b8e2d54bb0

i APP 信息

App名称: e充电
包名:
主活动Activity: []
安卓版本名称: 1.0
安卓版本: []

🔍 域名线索

域名	服务器信息
www.95516.com	IP: 123.125.46.38 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
h5pay.jd.com	IP: 111.206.228.124 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
maps.testing.amap.com	IP: 59.82.57.204 所属国家: China 地区: Beijing 城市: Beijing

	纬度: 39.907501 经度: 116.397102
dev.dcloud.net.cn	IP: 123.125.244.81 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
data-drru.push.dbankcloud.com	IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
m5.amap.com	IP: 106.11.35.98 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
grs.dbankcloud.eu	没有服务器地理信息.
metrics5.dt.dbankcloud.ru	IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499

layer.layui.com	没有服务器地理信息.
grs.dbankcloud.asia	IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
tsapi.amap.com	IP: 106.11.43.116 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
grs.platform.dbankcloud.ru	没有服务器地理信息.
metrics1.data.hicloud.com	IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
data-dre.push.dbankcloud.com	IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
shareyxcdapp.echargenet.com	没有服务器地理信息.
data-drcn.push.dbankcloud.com	IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou

	纬度: 23.127361 经度: 113.264572
restsdk.amap.com	IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
metrics2.data.hicloud.com	IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
grs.dbankcloud.cn	IP: 124.70.116.153 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
www.echargenet.com	IP: 140.207.47.33 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
mpsapi.amap.com	IP: 59.82.113.71 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
	IP: 119.8.163.189

data-dra.push.dbankcloud.com	所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
metrics5.data.hicloud.com	IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
192.168.102.196	IP: 192.168.102.196 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
mps.amap.com	IP: 59.82.113.71 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
grs.dbankcloud.com	IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
restapi.amap.com	IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650

 URL线索

URL信息	Url所在文件
https://h5pay.jd.com/degrade?	摸瓜V1引擎
https://www.95516.com/portal/open/init.do?entry=open	摸瓜V1引擎
http://www.echargenet.com/views/index.html	摸瓜V1引擎
https://data-drcn.push.dbankcloud.com	摸瓜V2引擎
https://data-dra.push.dbankcloud.com	摸瓜V2引擎
https://data-dre.push.dbankcloud.com	摸瓜V2引擎
https://data-drru.push.dbankcloud.com	摸瓜V2引擎
https://metrics1.data.hicloud.com:6447	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics2.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.dt.dbankcloud.ru:6447	摸瓜V2引擎
https://grs.dbankcloud.com	摸瓜V2引擎

https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://grs.platform.dbankcloud.ru	摸瓜V2引擎
https://grs.dbankcloud.eu	摸瓜V2引擎
http://192.168.102.196:8080/yxcdApp/baseinfo/userinfo	摸瓜V2引擎
https://restapi.amap.com/v3/assistant/coordinate/convert?key=fb9dda259bfd7ba0652ea30e4725974d&locations=\$	摸瓜V2引擎
https://shareyxcdapp.echargenet.com/yxcdApp/stationInfo/getStationInfo	摸瓜V2引擎
http://192.168.102.196:8080/yxcdApp/stationInfo/getStationInfo	摸瓜V2引擎
https://shareyxcdapp.echargenet.com/yxcdApp/stationInfo/getStationChargePortList	摸瓜V2引擎
http://192.168.102.196:8080/yxcdApp/stationInfo/getStationChargePortList	摸瓜V2引擎
https://shareyxcdapp.echargenet.com/yxcdApp/orderlyCharge/page/charge/setChargingParamPage.html?stakeNo=	摸瓜V2引擎
https://shareyxcdapp.echargenet.com/yxcdApp/userInfo/getUsinguserInfo	摸瓜V2引擎
https://shareyxcdapp.echargenet.com/yxcdApp/stakeInfo/reservationStakeList	摸瓜V2引擎
https://shareyxcdapp.echargenet.com/yxcdApp/orderlyCharge/page/reservation/chargeEquipmentReservationInput.html	摸瓜V2引擎
https://shareyxcdapp.echargenet.com/yxcdApp/orderlyCharge/page/charge/personalStakeDetail.html	摸瓜V2引擎
https://shareyxcdapp.echargenet.com/yxcdApp/baseinfo/getAccountBalance',	摸瓜V2引擎
http://layer.layui.com/mobile	摸瓜V2引擎
http://dev.dcloud.net.cn/mui)	摸瓜V2引擎

http://restsdk.amap.com/rest/lbs	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://restsdk.amap.com/v4	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://tsapi.amap.com/v1	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://restsdk.amap.com/v3	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://restsdk.amap.com/rest	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
https://tsapi.amap.com/v1/route/intercept	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://restsdk.amap.com/opennavi	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://m5.amap.com	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://maps.testing.amap.com/ws/shield/motor-route/etatrafficupdate	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://maps.testing.amap.com/ws/shield/motor-route/cross	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://maps.testing.amap.com/ws/shield/navigation/motor_traffic_report	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://maps.testing.amap.com/ws/shield/navigation/motor_off_route_report	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://maps.testing.amap.com/ws/shield/open_di/jiache_deepinfo/	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://m5.amap.com/ws/shield/elevated/downloadData	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://m5.amap.com/ws/shield/rdr/log/upload	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://m5.amap.com/ws/shield/mainsideroad/downloadData	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://mpsapi.amap.com/ws/mps/vmap/	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so

http://mpsapi.amap.com/ws/mps/rtt/	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://mpsapi.amap.com/ws/mps/smap	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://m5.amap.com/ws/transfer/auth/map/indoor_maps	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://mpsapi.amap.com/ws/mps/lyrdata/ugc/	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
http://mpsapi.amap.com/	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
https://mps.amap.com/ws/mps/rtt	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
https://mps.amap.com/ws/mps/vmap	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
https://maps.testing.amap.com/ws/transfer/auth/map/indoor_maps	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
https://mps.amap.com/ws/mps/smap	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
https://mps.amap.com/ws/mps/spot	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so
https://mps.amap.com/ws/mps/hot	lib/arm64-v8a/libAMapSDK_NAVI_v9_8_2.so

 邮箱线索

邮箱地址	所在文件
o@8.l15ri	摸瓜V2引擎
houfeng@dcloud.io	摸瓜V2引擎

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=86, ST=Beijing, L=Beijing, O=State Grid, OU=State Grid, CN=State Grid
签名算法: rsassa_pkcs1v15
有效期自: 2016-04-26 08:11:44+00:00
有效期至: 2041-04-20 08:11:44+00:00
发行人: C=86, ST=Beijing, L=Beijing, O=State Grid, OU=State Grid, CN=State Grid
序列号: 0x571f22c0
哈希算法: sha1
md5值: c28fef2e558a4fd00b190f4dd194bb83
sha1值: 0afc56ac420b3ad9d4a1349d41972d9df8e28007
sha256值: 43b575a9b1c258d782ba3d71277d3ffb439ca55849a7d16aa6548f5b124d4a4e
sha512值: 88d85249970bf345e8b66fc0c2d29ccc75e83c43c1d0ffce8af878f8496132346212cefad4c119a135c4c0afd43648ed63b4869ecb8e6467ce654e14d3162fb3
公钥算法: rsa
密钥长度: 1024
指纹: 96311e61189488181c71030ddb41995ed0c5a668493a71f4e1f16dd9db50282a

硬编码敏感信息

可能的敏感信息
"common_token_expired": "登录已过期，请重新登录"
"echarge_enterprise_pay_password": "手机号或者企业账号"
"enterprise_pay_password": "手机号或者企业账号"

"err_auth_dented" : "认证被否决"
"forget_pwd" : "忘记密码"
"input_password" : "请输入有效的密码"
"input_username" : "请输入您的用户名"
"login_forget_password" : "忘记密码？ "
"pos_pwd_display_yiqianbao" : "请输入壹钱包支付密码:"
"ppplugin_dialog_purse_not_get_pwdinfo_yiqianbao" : "壹钱包密码键盘无密文信息返回"
"ppplugin_forgetpwd_prompt" : "忘记密码"
"ppplugin_input_cardinfo_cardpwd_prompt" : "确认密码"
"ppplugin_inputpaypwd_pos_prompt" : "请输入6位全民付移动支付密码"
"ppplugin_inputpaypwd_prompt" : "请输入6位支付密码"
"ppplugin_inputpwddialog_accbalance_prompt" : "账户余额"
"ppplugin_inputpwddialog_coupon_prompt" : "优惠券"
"ppplugin_microfreepwd_amount_prompt" : "免密金额"
"ppplugin_microfreepwd_pay_prompt" : "小额免密支付"
"ppplugin_microfreepwd_prompt" : "小额免密"
"ppplugin_microfreepwd_switchoff" : "关闭"
"ppplugin_microfreepwd_switchon" : "已开户"

ppplugin_microfreepwd_switchon : 已开启
"ppplugin_microfreepwd_use_prompt": "超过免密额度时，需要验证支付密码，并且系统会移除可疑交易。"
"ppplugin_modifypaypwd_ok": "支付密码修改成功"
"ppplugin_modifypwd_prompt": "修改支付密码"
"ppplugin_resetpaypwd_ok": "支付密码重置成功"
"ppplugin_session_timeout_prompt": "由于您长时间未操作，请重新登录"
"ppplugin_set_pwd_prompt": "设置密码"
"protocal_private": "隐私声明"
"session_timeout": "会话超时,请重新登录"
"station_private": "不对外开放"
"str_input_password": "请输入密码"
"str_name_no_authou": "未实名认证"
"tip_authority": "本功能仅对已实名认证用户开放"
"tip_authority_fail": "实名认证审核失败，请你重新提交"
"tips_amount_free_pwd": "已为您开启200元额度小额免密，可在右上角设置"
"tips_input_password": "为了您的账号安全请输入支付密码"
"user_name": "昵称"
"user_up_noPwd_recharge": "开通免密码充电"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

应用内通信