MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

冠准兼职 1.0.APK

APP名称:	冠准兼职
包名:	com.guanzhun.recruit.oppo
域名线索:	3条
URL线索:	10条
邮箱线索:	0条
分析日期:	2022年2月2日 20:01

文件信息

文件名: guanzhunjianzhi.apk
文件大小: 6.97MB
MD5值: 9703c794bc6979372fe745d4167adbb0
SHA1值: 71997c25af8253275d77ad2430cd92af48ef70c8
SHA256值: a7a41a697e7c55b6c48ddd3da3ac62626e5b165d89c15652edeea8591a94abf6

APP 信息

App名称: 冠准兼职
包名: com.guanzhun.recruit.oppo
主活动**Activity:** com.jianzhi.recruit.activity.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
2020.wicwuzhen.cn	good	**IP:** 203.107.36.9 **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
github.com	good	**IP:** 20.205.243.166 **所属国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看地图:** Google Map
guanzhun.jiusi.tech	good	**IP:** 116.62.125.242 **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
https://2020.wicwuzhen.cn/web20/news/szjj/202010/t20201027_21582605.shtml	com/jianzhi/recruit/activity/WebViewActivity.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://guanzhun.jiusi.tech:8000/appApi/app/	Android String Resource

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_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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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

向手机申请的权限	是否危险	类型	详细情况
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=NewYork, L=NewYork, O=Recruit, OU=Recruit_999, CN=guanzhun_oppo_2021_10_19_02_59
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-10-19 06:59:36+00:00
Valid To: 2031-10-17 06:59:36+00:00
Issuer: C=US, ST=NewYork, L=NewYork, O=Recruit, OU=Recruit_999, CN=guanzhun_oppo_2021_10_19_02_59
Serial Number: 0x55ac35b3
Hash Algorithm: sha256
md5: 84ff7b578dd1dfd8028a67df2f80f3f1
sha1: 14533f3edab26dfb000b2a948729f582c5fc81b5
sha256: efc408c02d48032d2453c43ad388933b133ba82b626cae9c506c14799d043b2e
sha512: c34c57276e86db83c7cec1bfb605c43c2727f7d89bded725039496438ef18b1285dfb3e8936b349c5e8dc6ffaa07f6c6dfe7667a32b7542bfd47318b64ae8a22
PublicKey Algorithm: rsa

Bit Size: 2048
Fingerprint: 15b6945dec5bf6f4d7d13433662521e1a2d4d337fdbe722f77d7531f0ac2b1b0

硬编码敏感信息

可能的敏感信息
"app_key" : "eSTl28QJ9x0myhF"
"company_authority" : "登记机关"
"input_password" : "请输入密码"
"login_by_password" : "已有账号，使用密码登录"
"setting_password" : "设置密码"

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.MANUFACTURER check 编译器 / r8 without marker (suspicious)