MoGua

狗急加速 0.28.1.APK 分析报告

APP名称:	狗急加速

包名:	cloud.centaur.goj
域名线索:	9条
URL线索:	11条
邮箱线索:	5条
分析日期:	2024年10月30日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: goj-v0.28.1-release-gif3.apk
文件大小: 46.15MB
MD5值: ed0590ebc60877b54f7965769b951ea8
SHA1值: 55ce5b34555f8a0191716604bf594418eed5ddfd
SHA256值: 9fc855bd963eff1b98ea7d5ab148649bc192d3dfcc59538447108c7cf8763c4b

APP 信息

App名称: 狗急加速
包名: cloud.centaur.goj
主活动Activity: cloud.centaur.goj.MainActivity
安卓版本名称: 0.28.1
安卓版本: 281

域名线索

域名	服务器信息
www.w3.org	**IP**: 104.18.22.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.coolapk.com	**IP**: 221.204.43.199 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
d.alipay.com	**IP**: 39.91.185.199 **所属国家**: China **地区**: Shandong

	城市: Linyi **纬度**: 35.063061 **经度**: 118.342781
goo.gl	IP: 142.250.217.78 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
github.com	IP: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
goj-app.firebaseio.com	IP: 34.120.206.254 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
app-measurement.com	IP: 114.250.65.33 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
pagead2.googlesyndication.com	IP: 114.250.65.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 103.224.212.211

forbest.site	**所属国家**: Australia **地区**: Victoria **城市**: Beaumaris **纬度**: -37.982201 **经度**: 145.038940

URL线索

URL信息	Url所在文件
https://app-measurement.com/a	c/c/a/a/e/e/x8.java
https://goo.gl/J1sWQy	c/c/a/a/e/e/d.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	c/c/a/a/a/a/b.java
https://github.com/flutter/flutter/issues/2897).It	io/flutter/plugin/platform/PlatformViewsController.java
https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects	io/flutter/view/FlutterView.java
https://d.alipay.com	cloud/centaur/goj/model/Global2pay.java
https://goj-app.firebaseio.com	摸瓜V1引擎
https://www.coolapk.com/apk/com.goplaycn.googleinstall	摸瓜V2引擎
http://forbest.site/goj/apks/v0.28.0/goj-v0.28.0-release-official.apk	摸瓜V2引擎
http://forbest.site/goj/app/index.html	摸瓜V2引擎
http://forbest.site/goj/app/shared.html	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	c/c/a/a/c/x.java
appro@openssl.org	lib/arm64-v8a/libflutter.so
go-tun2socks@v1.16	lib/arm64-v8a/libgojni.so
go-tun2socks@v1.16	lib/armeabi-v7a/libgojni.so
go-tun2socks@v1.16	lib/x86/libgojni.so

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=01, ST=California, L=San Francisco, O=Centaur Cloud, OU=Centaur, CN=Centaur Alpha
签名算法: rsassa_pkcs1v15
有效期自: 2020-02-16 07:23:07+00:00
有效期至: 2045-02-09 07:23:07+00:00
发行人: C=01, ST=California, L=San Francisco, O=Centaur Cloud, OU=Centaur, CN=Centaur Alpha
序列号: 0x60970d60
哈希算法: sha256
md5值: e8692db64932ec47fad414fafa15bd1d

sha1值: 64a4b2ec5920838f0de03acfb57fbd5e474021b3
sha256值: 06d7f14b3084fbe24ea30e0a02285670f5e6467eaacf7175cf4c8d53c5ddd9f4
sha512值: 6aa2c6ef79db3488405bfa7d99decb78589726c8b21d6dabb01d022ba64bf7a29e543df0ef800f44a25dcc46dcf4b6a1ea47a2d2e2a0c19fb40f066a2031ea36
公钥算法: rsa
密钥长度: 2048
指纹: 3552c303747a0c231beab239ecd0085403fbb6b160b667d9dcba714e572ee51c

硬编码敏感信息

可能的敏感信息
"firebase_database_url" : "https://goj-app.firebaseio.com"
"google_api_key" : "AIzaSyBhpokf8ERcR9LGo5KrT8M27NPIuFXb4pM"
"google_crash_reporting_api_key" : "AIzaSyBhpokf8ERcR9LGo5KrT8M27NPIuFXb4pM"

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

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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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.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_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.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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
cloud.centaur.goj.MainActivity	Schemes: cpdh4h://,
