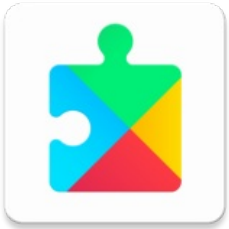
MoGua

Google Play Service 1.0.APK 分析报告



APP名称: Google Play Service

包名:	ahmyth.mine.king.ahmyth
域名线索:	2条
URL线索:	2条
邮箱线索:	0条
分析日期:	2025年8月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: Ahmyth-aligned-debugSigned.apk
文件大小: 0.29MB
MD5值: f17de2cc3857d0ab116b619c3ee4df3b
SHA1值: a9759cb532fc6704f8c9f43c2e6ddb8074157032
SHA256值: 04636305e098f4a9336eb5b66c7718fd17af1ce19e6b043aa9a4b148bc81491d

APP 信息

App名称: Google Play Service
包名: ahmyth.mine.king.ahmyth
主活动Activity: ahmyth.mine.king.ahmyth.MainActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	服务器信息
play.google.com	**IP**: 8.7.198.46 **所属国家**: United States of America **地区**: Louisiana **城市**: Monroe **纬度**: 32.548328 **经度**: -92.045235
192.168.163.137	**IP**: 192.168.163.137 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000

URL线索

URL信息	Url所在文件
https://play.google.com/store/apps	ahmyth/mine/king/ahmyth/MainActivity.java
http://192.168.163.137:4444?model=	ahmyth/mine/king/ahmyth/e.java

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=US, ST=US, L=US, O=US, OU=Android, CN=Android Debug
签名算法: rsassa_pkcs1v15
有效期自: 2016-10-23 20:10:05+00:00
有效期至: 2044-03-10 20:10:05+00:00
发行人: C=US, ST=US, L=US, O=US, OU=Android, CN=Android Debug
序列号: 0x56c1a15
哈希算法: sha256
md5值: ffd6314a83f267ac4f9407fd2e5a0480
sha1值: 5d08264b44e0e53fbccc70b4f016474cc6c5ab5c
sha256值: 1e08a903aef9c3a721510b64ec764d01d3d094eb954161b62544ea8f187b5953
sha512值: 428b549823a4f3010218b270db81b8dea32f9115edcf58898a38839826ed3a5ece86fe792c4e0db47aab7c940e3968220bb16dfcca36052070d6e6ab2c482b96
公钥算法: rsa
密钥长度: 2048
指纹: 5ae9c127f99536cc5371c0a638c92ffcd60c770d30ddc58bd1721fba7e0d321f

硬编码敏感信息

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.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
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.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
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.WRITE_SECURE_SETTINGS	系统需要	修改安全系统设置	允许应用程序修改系统固定好设置数据。不供普通应用程序使用
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.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息
	正		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

android.permission.RECEIVE_BOOT_COMPLETED	常	开机时自动启动	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
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_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.PROCESS_OUTGOING_CALLS	危险	拦截拨出电话	允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.REQUEST_IGNORE_BATTERY_OPTIMISATIONS	未知	Unknown permission	Unknown permission from android reference

应用内通信