MoGua

Fox null.APK 分析报告

APP名称: Fox

包名:	jeehberhhr.sgegeheh.dudhrbr
域名线索:	2条
URL线索:	2条
邮箱线索:	1条
分析日期:	2025年7月7日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 196475.apk
文件大小: 21.74MB
MD5值: d145c68399449075efd6f347bd5a6bf1
SHA1值: b27812f5f4d36d64dc66014de6791806ae21c7d6
SHA256值: 28f4fd9c490ea2b832c3308234f73a6d2e34fed0b63fea76e0d2997e2470cd3f

APP 信息

App名称: Fox
包名: jeehberhhr.sgegeheh.dudhrbr
主活动Activity: com.dgdg2024.app.dfdg_app.MainActivity
安卓版本名称: null
安卓版本:

域名线索

域名	服务器信息
developer.android.com	**IP**: 142.250.73.78 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
plus.google.com	**IP**: 108.160.165.189 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

URL线索

URL信息	Url所在文件
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/h.java
https://plus.google.com/	s1/j1.java

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	p1/v.java

手机线索

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=vlyoixeuryooiqh, ST=jfuoicpokofpobe, L=roocexjufljneus, O=bay1751783675036, OU=pgr1751783675036, CN=Xcuu1751783675036
签名算法: rsassa_pkcs1v15
有效期自: 2025-07-06 06:34:35+00:00
有效期至: 2075-06-24 06:34:35+00:00
发行人: C=vlyoixeuryooiqh, ST=jfuoicpokofpobe, L=roocexjufljneus, O=bay1751783675036, OU=pgr1751783675036, CN=Xcuu1751783675036
序列号: 0x743fef40
哈希算法: sha1
md5值: 535825e970c02f37d9a4141b5f86cd0a
sha1值: 4a1f2e60ef7175fc8e8b98948ee78e78064703ac

sha256值: 48d37b24a916dfa87d451ef540a8a5bdcc3f01c88c828f1f0d4b8e5a7f5b56fc
sha512值: dd48824399219c1fa16696a3a9abbd6034f9c3d68187072437fdacd7e40c679d70951a8aa3fcec215bc691f0f6c5e852398fe1758e9ba62048d4bbb0e205a8aa
公钥算法: rsa
密钥长度: 1024
指纹: 1c63fc1334be68bb92579c25bd4b486610b4ee3e47095af6647a29b516cfb8ff

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.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_PHONE_NUMBERS	危险		允许到设备的读访问的电话号码。这是 READ_PHONE_STATE 授予的功能的一个子集,但对即时应用程序公开
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
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_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_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
jeehberhhr.sgegeheh.dudhrbr.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信
