MoGua

Fox null.APK 分析报告

APP名称:	Fox

包名:	odb.gbznzvd1.nat
域名线索:	2条
URL线索:	2条
邮箱线索:	1条
分析日期:	2025年6月15日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: Fox-JiMB4uxNWDqpQAC2.apk
文件大小: 21.53MB
MD5值: 8c43e686c743aa0e61cf3a1f70ffe00f
SHA1值: 1b9e06b49e44bcf00d405abd9d8b3465185bc640
SHA256值: 8500bdeafa0f66d036f4d1e52fc31ff866b57a769e319971d69c4cce8d66de27

APP 信息

App名称: Fox
包名: odb.gbznzvd1.nat
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**: 142.250.107.113 **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**: 198.44.185.131 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904

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=ajazvomonpyrodi, ST=rndupjcjkcxkwzp, L=ipwalgfydfgkajj, O=ube1749773231803, OU=ugf1749773231803, CN=Xvjf1749773231803
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-13 00:07:11+00:00
有效期至: 2075-06-01 00:07:11+00:00
发行人: C=ajazvomonpyrodi, ST=rndupjcjkcxkwzp, L=ipwalgfydfgkajj, O=ube1749773231803, OU=ugf1749773231803, CN=Xvjf1749773231803
序列号: 0x539c4a3a
哈希算法: sha1
md5值: 727fde930fa323048f476d716c56233e
sha1值: cba98eaee7863eb54246eb52bdfd6270358dd4dd

sha256值: 84c64027d70a665172e977fc08b47aaeb0ae1a786a041863ffeb934d6d165b76
sha512值: 10f42b77223ec52f3dd90a4a8704cbcd4b704acba6527b07b3937d2be291ea2e32a15fa9c25ffc026f916dffe15262beb80db6b827d921691a6eda6f6702341a
公钥算法: rsa
密钥长度: 1024
指纹: 1da8b47510ba07887b7be8c3e61f54fff2712faf63a37fbce421e095dc9f4e27

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
		Unknown	

odb.gbznzvd1.nat.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	permission	Unknown permission from android reference

应用内通信
