MoGua

None 3.3.7.0.APK 分析报告

APP名称:	None

包名:	com.ytheekshana.deviceinfo
域名线索:	25条
URL线索:	23条
邮箱线索:	2条
分析日期:	2024年11月7日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.ytheekshana.deviceinfo.apk
文件大小: 6.62MB
MD5值: ee80bb196c6fc1984accf912574bb336
SHA1值: 29988a817b41cc00a72dc3f3789caec472622baa
SHA256值: 39b0cf34ed3a2ac93e68461ca0137aba2aafb62073d9dd72727b85238ba86e2f

APP 信息

App名称: None
包名: com.ytheekshana.deviceinfo
主活动Activity: com.ytheekshana.deviceinfo.SplashActivity
安卓版本名称: 3.3.7.0
安卓版本: 258

域名线索

域名	服务器信息
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
www.google.com	**IP**: 31.13.88.26 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
ns.adobe.com	没有服务器地理信息.

google.com	**IP**: 59.24.3.174 **所属国家**: Korea (Republic of) **地区**: Gyeonggi-do **城市**: Seongnam **纬度**: 37.420624 **经度**: 127.126717
developer.android.com	**IP**: 142.251.33.78 **所属国家**: Canada **地区**: Ontario **城市**: Toronto **纬度**: 43.653660 **经度**: -79.382927
support.google.com	**IP**: 142.251.33.78 **所属国家**: Canada **地区**: Ontario **城市**: Toronto **纬度**: 43.653660 **经度**: -79.382927
api.seeip.org	**IP**: 23.128.64.156 **所属国家**: United States of America **地区**: Oregon **城市**: Clackamas **纬度**: 45.415646 **经度**: -122.524277
schemas.android.com	没有服务器地理信息.
play.google.com	**IP**: 46.82.174.69 **所属国家**: Germany **地区**: Niedersachsen **城市**: Braunschweig **纬度**: 52.266121 **经度**: 10.526730
	IP: 114.250.64.38 **所属国家**: China **地区**: Beijing

www.googleadservices.com	**城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
deviceinfo.oneskyapp.com	**IP**: 54.86.7.121 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.039474 **经度**: -77.491806
issuetracker.google.com	**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
www.linkedin.com	**IP**: 52.130.75.155 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
fundingchoicesmessages.google.com	**IP**: 142.251.33.78 **所属国家**: Canada **地区**: Ontario **城市**: Toronto **纬度**: 43.653660 **经度**: -79.382927
firebaseinstallations.googleapis.com	**IP**: 142.251.215.234 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514

firebase.google.com	**IP**: 142.250.69.206 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
goo.gl	**IP**: 142.251.215.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.deviceinfo.app	**IP**: 104.152.222.128 **所属国家**: United States of America **地区**: Oregon **城市**: Bend **纬度**: 44.058170 **经度**: -121.315308
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
twitter.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
firebase-settings.crashlytics.com	**IP**: 114.250.65.34 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501

	经度: 116.397102
forum.xda-developers.com	**IP**: 52.5.96.96 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.039474 **经度**: -77.491806
t.me	**IP**: 149.154.167.99 **所属国家**: United Kingdom of Great Britain and Northern Ireland **地区**: England **城市**: Warrington **纬度**: 52.184460 **经度**: -0.687590
googlemobileadssdk.page.link	**IP**: 142.250.69.193 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.facebook.com	**IP**: 199.16.158.182 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446

URL线索

URL**信息**	Url**所在文件**
https://googlemobileadssdk.page.link/admob-android-update-manifest	E2/F0.java

https://googlemobileadssdk.page.link/ad-manager-android-update-manifest.	E2/F0.java
http://schemas.android.com/apk/res/android	K/b.java
https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/	A3/t.java
https://firebase.google.com/docs/crashlytics/get-started?platform=android	A3/t.java
https://firebase.google.com/support/privacy/init-options.	O4/d.java
https://support.google.com/dfp_premium/answer/7160685	H2/DialogInterface$OnClickListenerC0096f.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	B2/c.java
https://www.deviceinfo.app/web-services/get-details.php	com/ytheekshana/deviceinfo/MainActivity.java
https://www.facebook.com/deviceinfoapp	com/ytheekshana/deviceinfo/AboutActivity.java
https://twitter.com/deviceinfoapp	com/ytheekshana/deviceinfo/AboutActivity.java
https://t.me/DeviceInfoDiscussion	com/ytheekshana/deviceinfo/AboutActivity.java
https://deviceinfo.oneskyapp.com/mobile	com/ytheekshana/deviceinfo/AboutActivity.java
https://www.linkedin.com/company/deviceinfo	com/ytheekshana/deviceinfo/AboutActivity.java
https://www.deviceinfo.app	com/ytheekshana/deviceinfo/AboutActivity.java
https://forum.xda-developers.com/android/apps-games/app-device-info-hardware-software-t3844060	com/ytheekshana/deviceinfo/AboutActivity.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	S5/r.java
https://play.google.com/store/apps/details?id=com.ytheekshana.deviceinfo	c5/C0423w.java
https://api.seeip.org/geoip	h5/F.java

https://play.google.com/store/apps/details?id=	h5/C3315x.java
https://play.google.com/store/apps/details?id=com.ytheekshana.deviceinfo	h5/H.java
https://fundingchoicesmessages.google.com/a/consent	m3/C3447c.java
https://developer.android.com/training/articles/direct-boot	m1/g.java
https://app-measurement.com/a	q3/AbstractC3738w.java
https://app-measurement.com/s	q3/AbstractC3738w.java
https://www.google.com	q3/p1.java
https://goo.gl/NAOOOI.	q3/p1.java
https://goo.gl/NAOOOI	q3/p1.java
https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=	q3/A0.java
https://firebase.google.com/support/guides/disable-analytics	q3/C3681I.java
https://google.com/search?	q3/D0.java
http://ns.adobe.com/xap/1.0/\u0000	o0/g.java
https://firebaseinstallations.googleapis.com/v1/	Q4/c.java
https://play.google.com/store/apps/details?id=com.ytheekshana.deviceinfo	m5/C3469d.java
https://www.deviceinfo.app/privacy-policy/	m5/C3469d.java

邮箱线索

邮箱地址	所在文件
support@deviceinfo.app	com/ytheekshana/deviceinfo/AboutActivity.java
u0013android@android.com0 u0013android@android.com	X2/m.java

手机线索

手机号	所在文件
14222222222	h5/C3291k0.java
13222222222	h5/C3291k0.java
15552000000	q3/C3737v0.java

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=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2018-09-17 14:21:38+00:00
有效期至: 2048-09-17 14:21:38+00:00

发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x88b7796b358ef44520504474dcbe9a5aa7e45211
哈希算法: sha256
md5值: 87c639a929a9a2e9d0c24c42b0faad97
sha1值: 256c81f8130408f385cb0903faf0179b2d634e22
sha256值: 59233d4ee84151879a9171301aa8708dd654d76feb9e9cf23115f76431f53aaa
sha512值: 86605030ad5d9444dc210c50c17cc9afc0054ce75b29d585c269ee7870c2174f7a22e1e62ab255e7f8cf3c908fe63b40ab876de737330d01305343147f9742ca
公钥算法: rsa
密钥长度: 4096
指纹: 95f0c6d10307c2699f11bf9ded3c22dd7fba4112be6596b84bad52c62b86b8f0

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

	是		

向手机申请的权限	否危险	类型	详细情况
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
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.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
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.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference

android.permission.ACCESS_ADSERVICES_AD_ID	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ADSERVICES_TOPICS	未知	Unknown permission	Unknown permission from android reference
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
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.ytheekshana.deviceinfo.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信