MoGua

None 3.6.0.APK 分析报告

APP名称:	None

包名:	kajfosz.antimatterdimensions
域名线索:	29条
URL线索:	23条
邮箱线索:	2条
分析日期:	2024年7月27日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: Antimatter Dimensions_3.6.0.apks
文件大小: 39.59MB
MD5值: 6f5c8ddcbb86d2673b0f4c32e6a2533f
SHA1值: 27617d67262b71ed73b3847ac799be41f8f2bca0
SHA256值: 86b5bfbff69b8759d15a68bfecd67662a085866d179414ca86c59d28f0169e20

APP 信息

App名称: None
包名: kajfosz.antimatterdimensions
主活动Activity: kajfosz.antimatterdimensions.MainActivity
安卓版本名称: 3.6.0
安卓版本: 30060000

域名线索

域名	服务器信息
support.google.com	**IP**: 172.217.163.46 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
en.wikipedia.org	**IP**: 199.16.158.8 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
schemas.android.com	没有服务器地理信息.
	IP: 185.199.109.153

aarextiaokhiao.github.io	**所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
kajfik.github.io	IP: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
accounts.google.com	IP: 108.177.97.84 **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: 69.171.234.48 **所属国家**: United States of America **地区**: California **城市**: Menlo Park **纬度**: 37.436935 **经度**: -122.193604
www.gfaq.com	IP: 3.130.204.160 **所属国家**: United States of America **地区**: Ohio **城市**: Columbus **纬度**: 39.961380 **经度**: -82.997749
www.youtube.com	IP: 108.160.165.11 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

www.google.com	IP: 31.13.94.49 **所属国家**: Argentina **地区**: Ciudad Autonoma de Buenos Aires **城市**: Buenos Aires **纬度**: -34.603600 **经度**: -58.381554
www.googleadservices.com	IP: 114.250.67.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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
twitter.com	IP: 108.160.165.212 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.thingiverse.com	IP: 104.19.147.91 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
	IP: 114.250.70.33 **所属国家**: China

app-measurement.com	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
en.m.wikipedia.org	**IP**: 199.59.148.229 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
goo.gl	**IP**: 142.251.43.14 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.googleapis.com	**IP**: 172.217.163.42 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
discord.gg	**IP**: 74.86.151.167 **所属国家**: United States of America **地区**: California **城市**: San Jose **纬度**: 37.339390 **经度**: -121.894958
firebase.google.com	**IP**: 142.251.43.14 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514

pagead2.googlesyndication.com	**IP**: 114.250.66.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
developer.android.com	**IP**: 142.251.43.14 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
ivark.github.io	**IP**: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
crowdin.com	**IP**: 34.237.215.176 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.039474 **经度**: -77.491806
imgur.com	**IP**: 69.171.247.32 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.713192 **经度**: -74.006065
phone.firebase	没有服务器地理信息.
	IP: 20.205.243.166 **所属国家**: Singapore

github.com	**地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
play.google.com	**IP**: 93.46.8.90 **所属国家**: Italy **地区**: Lombardia **城市**: Milan **纬度**: 45.464336 **经度**: 9.188547
www.reddit.com	**IP**: 108.160.166.137 **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://accounts.google.com/o/oauth2/revoke?token=	A2/d.java
http://schemas.android.com/apk/res/android	N/b.java
https://www.googleapis.com/auth/drive.file	N2/e.java
https://www.googleapis.com/auth/drive.appdata	N2/e.java
https://www.googleapis.com/auth/drive	N2/e.java
https://www.googleapis.com/auth/drive.apps	N2/e.java

https://support.google.com/dfp_premium/answer/7160685	O4/h.java
https://accounts.google.com	U2/f.java
https://www.facebook.com	U2/f.java
https://twitter.com	U2/f.java
https://github.com	U2/f.java
https://phone.firebase	U2/f.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	Y1/c.java
https://developer.android.com/training/articles/direct-boot	h1/RunnableC0607f.java
https://discord.gg/teaU8ZQ	kajfosz/antimatterdimensions/D.java
https://ivark.github.io	kajfosz/antimatterdimensions/D.java
https://www.reddit.com/r/AntimatterDimensions	kajfosz/antimatterdimensions/D.java
https://crowdin.com/project/antimatter-dimensions/invite?h=1dc8018ab3b1e4b0e89837f6ea2310ae1903434	kajfosz/antimatterdimensions/D.java
https://play.google.com/store/apps/details?id=kajfosz.antimatterdimensions	kajfosz/antimatterdimensions/D.java
https://kajfik.github.io/privacy_policy.html	kajfosz/antimatterdimensions/View$OnClickListenerC0731g.java
https://www.youtube.com/watch?v=dQw4w9WgXcQ	kajfosz/antimatterdimensions/news/NewsKt$aiNews$2.java
https://www.youtube.com/watch?v=dQw4w9WgXcQ	kajfosz/antimatterdimensions/news/NewsKt$normalNews$1.java
https://www.youtube.com/watch?v=dQw4w9WgXcQ	kajfosz/antimatterdimensions/news/NewsKt$aiNews$17.java

https://ivark.github.io	kajfosz/antimatterdimensions/news/NewsKt$normalNews$133.java
https://www.google.com/search?q=massive+car+spoiler&tbm=isch	kajfosz/antimatterdimensions/news/NewsKt$normalNews$146.java
https://discord.gg/teaU8ZQ	kajfosz/antimatterdimensions/news/NewsKt$normalNews$82.java
https://www.youtube.com/watch?v=dQw4w9WgXcQ	kajfosz/antimatterdimensions/news/a.java
http://en.wikipedia.org/wiki/Hevipelle)	kajfosz/antimatterdimensions/news/a.java
https://aarextiaokhiao.github.io/blob/master/docs/en.json	kajfosz/antimatterdimensions/news/a.java
https://en.m.wikipedia.org/wiki/Olli%27_Web	kajfosz/antimatterdimensions/news/a.java
http://imgur.com/E4261C7h)	kajfosz/antimatterdimensions/news/a.java
http://www.thingiverse.com/id:98109802713176601414569]]	kajfosz/antimatterdimensions/news/a.java
http://www.gfaq.com/gfaqs/this-game-faq-by-title]],	kajfosz/antimatterdimensions/news/a.java
http://www.gfaq.com/tug/this-game-faq-by-title]].	kajfosz/antimatterdimensions/news/a.java
http://www.gfaq.com/gfaqs/this-game-faq-by-name]]	kajfosz/antimatterdimensions/news/a.java
https://www.youtube.com/watch?v=lXMskKTw3Bs).	kajfosz/antimatterdimensions/news/a.java
https://www.youtube.com/watch?v=uCP44Q37YHAQ	kajfosz/antimatterdimensions/news/a.java
https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=	n3/D0.java
https://firebase.google.com/support/guides/disable-analytics	n3/C0910F.java
https://google.com/search?	n3/G0.java
https://app-measurement.com/a	n3/AbstractC0963u.java

https://www.google.com	n3/x1.java
https://goo.gl/NAOOOI.	n3/x1.java
https://goo.gl/NAOOOI	n3/x1.java
https://github.com/firebase/FirebaseUI-Android/releases/tag/6.2.0	o1/C0997c.java
https://github.com	q1/n.java
https://phone.firebase	q1/n.java
https://accounts.google.com	q1/n.java
https://twitter.com	q1/n.java
https://www.facebook.com	q1/n.java

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	C2/m.java
ntimatter.dimensions@gmail.com realhevi@antimatter.com	kajfosz/antimatterdimensions/news/a.java

手机线索

手机号	所在文件
15552000000	n3/C0972y0.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: 2019-01-19 14:01:05+00:00
有效期至: 2049-01-19 14:01:05+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xb7370972ac3b33ea42bf7c0d63082d9d6a20fee9
哈希算法: sha256
md5值: a89a57be67c5d9632050ceeb80cc6937
sha1值: 291096733a1132b5565b26a58bd7ada0f405938f
sha256值: 24c5158c0de5d472f018107476ca6e5fd8c1442b404c3fe49a26c2024dd1fd14
sha512值: cab0f17b29a66868019f95dc131c333ad2e10388cc6f31e2bae8506366fb658d5837558616807cb795db3c647cc13b2e0298ca9beafcb79e4c8bd958c90c6d40
公钥算法: rsa
密钥长度: 4096
指纹: 86ce1711a6bae1172888116c36b41bd87dff31a0f5866d32123f33629eaea4af

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆模板网站后查看	

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.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.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.DETECT_SCREEN_CAPTURE	未知	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	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。
kajfosz.antimatterdimensions.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.facebook.CustomTabActivity	Schemes: @string/facebook_login_protocol_scheme://,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,