MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Grupo Cine 3.0.1662.APK

APP名称:	Grupo Cine
包名:	br.com.velox.grupocine
域名线索:	20条
URL线索:	22条
邮箱线索:	1条
分析日期:	2022年1月25日 22:02

文件信息

文件名: grupocine567636.apk
文件大小: 5.07MB
MD5值: 9316273079f6b664e82035ce02c8adbb
SHA1值: 00c7eeec85d383f2472a84cb917e8c70c49fa3d6
SHA256值: 4b561c337ecd09263c62eef48bf8865d87a8f11542f70eabec1f84e889f2609d

APP 信息

App名称: Grupo Cine
包名: br.com.velox.grupocine
主活动**Activity:** br.com.velox.grupocine.MainActivity
安卓版本名称: 3.0.1662
安卓版本: 1662

域名线索

域名	是否危险域名	服务器信息
www.facebook.com	good	**IP:** 199.59.148.222 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.773968 **经度:** -122.410446 **查看地图:** Google Map

域名	是否危险域名	服务器信息
login.live.com	good	**IP:** 40.126.35.80 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
www.example.com	good	**IP:** 93.184.216.34 **所属国家:** United States of America **地区:** Virginia **城市:** Ashburn **纬度:** 39.043720 **经度:** -77.487488 **查看地图:** Google Map
teste-master.veloxtix.com	good	**IP:** 172.67.189.189 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看地图:** Google Map
onesignal.com	good	**IP:** 104.18.225.52 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.googleapis.com	good	**IP:** 172.217.160.106 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map
plus.google.com	good	**IP:** 128.242.245.93 **所属国家:** United States of America **地区:** California **城市:** Milpitas **纬度:** 37.428268 **经度:** -121.906616 **查看地图:** Google Map
www.youtube.com	good	**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 **查看地图:** Google Map
play.google.com	good	**IP:** 142.251.42.238 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.linkedin.com	good	**IP:** 106.3.34.145 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
login.yahoo.com	good	**IP:** 74.6.160.138 **所属国家:** United States of America **地区:** New York **城市:** New York City **纬度:** 40.731323 **经度:** -73.990089 **查看地图:** Google Map
fidapi.veloxtickets.com	good	**IP:** 104.26.13.192 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看地图:** Google Map
api.veloxtickets.com	good	**IP:** 172.67.72.186 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看地图:** Google Map

域名	是否危险域名	服务器信息
veloxtickets.com	good	**IP:** 104.26.13.192 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看地图:** Google Map
accounts.google.com	good	**IP:** 142.251.42.237 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map
pagead2.googlesyndication.com	good	**IP:** 220.181.174.38 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
schemas.android.com	good	没有服务器地理信息.
teste-master-fidapi.veloxtix.com	good	**IP:** 104.21.49.104 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.paypal.com	good	**IP:** 23.10.3.27 **所属国家:** Japan **地区:** Tokyo **城市:** Tokyo **纬度:** 35.689507 **经度:** 139.691696 **查看地图:** Google Map
twitter.com	good	**IP:** 75.126.150.210 **所属国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.939491 **经度:** -96.838730 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	e/k/d/i/h.java
https://www.example.com	e/f/b/e.java
https://play.google.com/store/apps/details?id=	f/a/a/a/l1.java
https://teste-	f/a/a/a/k1.java
https://veloxtickets.com	f/a/a/a/s1/a.java

URL信息	Url所在文件
https://teste-master.veloxtix.com	f/a/a/a/s1/a.java
https://fidapi.veloxtickets.com/	f/a/a/a/s1/a.java
https://teste-master-fidapi.veloxtix.com/	f/a/a/a/s1/a.java
https://api.veloxtickets.com/WebView/	f/a/a/a/s1/a.java
https://play.google.com/store/apps/details?id=com.picpay	f/a/a/a/m1/t/z.java
http://schemas.android.com/apk/res-auto	g/b/a/b/j/b.java
http://schemas.android.com/apk/res/android	g/b/a/b/j/a.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	g/b/a/a/b/a/b.java
https://www.googleapis.com/auth/games.firstparty	g/b/a/a/f/f.java
https://www.googleapis.com/auth/fitness.oxygen_saturation.write	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.body_temperature.read	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.body_temperature.write	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.reproductive_health.read	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.reproductive_health.write	g/b/a/a/f/p.java
https://www.googleapis.com/auth/plus.login	g/b/a/a/f/p.java

URL信息	Url所在文件
https://www.googleapis.com/auth/plus.me	g/b/a/a/f/p.java
https://www.googleapis.com/auth/games	g/b/a/a/f/p.java
https://www.googleapis.com/auth/games_lite	g/b/a/a/f/p.java
https://www.googleapis.com/auth/datastoremobile	g/b/a/a/f/p.java
https://www.googleapis.com/auth/appstate	g/b/a/a/f/p.java
https://www.googleapis.com/auth/drive.file	g/b/a/a/f/p.java
https://www.googleapis.com/auth/drive.appdata	g/b/a/a/f/p.java
https://www.googleapis.com/auth/drive	g/b/a/a/f/p.java
https://www.googleapis.com/auth/drive.apps	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.activity.read	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.activity.write	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.location.read	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.location.write	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.body.read	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.body.write	g/b/a/a/f/p.java

URL信息	Url所在文件
https://www.googleapis.com/auth/fitness.nutrition.read	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.nutrition.write	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.blood_pressure.read	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.blood_pressure.write	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.blood_glucose.read	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.blood_glucose.write	g/b/a/a/f/p.java
https://www.googleapis.com/auth/fitness.oxygen_saturation.read	g/b/a/a/f/p.java
https://plus.google.com/	g/b/a/a/f/y/o1.java
https://www.facebook.com	g/b/a/a/d/l/f/h.java
https://accounts.google.com	g/b/a/a/d/l/f/h.java
https://www.linkedin.com	g/b/a/a/d/l/f/h.java
https://login.live.com	g/b/a/a/d/l/f/h.java
https://www.paypal.com	g/b/a/a/d/l/f/h.java
https://twitter.com	g/b/a/a/d/l/f/h.java
https://login.yahoo.com	g/b/a/a/d/l/f/h.java

URL信息	Url所在文件
https://accounts.google.com/o/oauth2/revoke?token=	g/b/a/a/d/l/i/g/f.java
http://www.youtube.com/watch?v=	g/e/a/c/b/a.java
https://www.youtube.com	g/e/a/c/a/e/a.java
https://onesignal.com/android_frame.html	g/d/p1.java
https://onesignal.com/api/v1/	g/d/w1.java

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	g/b/a/a/f/q0.java

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

向手机申请的权限	是否危险	类型	详细情况
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_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
br.com.velox.grupocine.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	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
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。

向手机申请的权限	是否危险	类型	详细情况
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
com.huawei.android.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
android.permission.READ_APP_BADGE	正常	显示应用程序通知	允许应用程序显示应用程序图标徽章
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。

向手机申请的权限	是否危险	类型	详细情况
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-10-08 17:53:57+00:00
Valid To: 2050-10-08 17:53:57+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xf88f76647cfe8d694320571d9c3e260f0aaf01c2
Hash Algorithm: sha256
md5: 7167b1eb1dafa9b10f3c7bbf84361595
sha1: bef1b9af18c7784157c120156dd28161b619ce6c
sha256: 173657653c1527364481a14e26624d5ec8b5cb8b1dfa07a175f178b71bb2159c
sha512: a43bd4cfd5813cdbdadc77a576e9d2485f255a1abeb0db8fff79877bc2e626b35ae263c887e0190e31d9ef1891f3ddcade777b493b4771a14b926bea1e4a4fd5
PublicKey Algorithm: rsa
Bit Size: 4096

Fingerprint: 34f8c4e71d1e40e5f39675765e9dd2508a1922686a328eef0440dc1f3e3b4877

Exodus威胁情报

名称	分类	URL链接
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

应用内通信

活动(ACTIVITY)	通信(INTENT)
br.com.velox.grupocine.MainActivity	Schemes: grupocine://,

加壳分析

文件列表	分析结果

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
