MoGua

Pikashow 10.8.2.APK 分析报告

APP名称:	Pikashow

包名:	com.offshore.pikachu
域名线索:	28条
URL线索:	38条
邮箱线索:	1条
分析日期:	2025年1月31日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: Pikashow.APK
文件大小: 16.38MB
MD5值: 39513824abe081261fc6f7b29c311aaa
SHA1值: 01c8720dd45154520e7ab922a0ab3b0c191dd529
SHA256值: 39eeb95059edadedd820a58ee53599d93e21b8f683521df26369dd64fa7285f2

APP 信息

App名称: Pikashow
包名: com.offshore.pikachu
主活动Activity: com.offshore.pikachu.view.Splash
安卓版本名称: 10.8.2
安卓版本: 82

域名线索

域名	服务器信息
issuetracker.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
play.google.com	**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
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
plus.google.com	**IP**: 69.63.180.173 **所属国家**: United States of America **地区**: California **城市**: Menlo Park **纬度**: 37.436935 **经度**: -122.193604
ns.adobe.com	没有服务器地理信息.
offshore1play.firebaseio.com	**IP**: 34.120.206.254 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
schemas.android.com	没有服务器地理信息.
www.w3.org	**IP**: 104.18.22.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
awsindstream.com	**IP**: 213.183.62.122 **所属国家**: Bulgaria **地区**: Sofia (stolitsa) **城市**: Sofia **纬度**: 42.697510 **经度**: 23.324150
www.google.com	**IP**: 59.188.250.54 **所属国家**: Hong Kong **地区**: Hong Kong

	城市: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
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
uptostream.com	IP: 104.26.11.35 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
exoplayer.dev	IP: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
firebase-settings.crashlytics.com	IP: 58.254.149.226 **所属国家**: China **地区**: Guangdong **城市**: Yunfu **纬度**: 22.930559 **经度**: 112.037300
www.dailymotion.com	IP: 157.240.17.41 **所属国家**: Switzerland **地区**: Zurich **城市**: Zurich **纬度**: 47.366825 **经度**: 8.549790

app-measurement.com	IP: 58.254.137.161 **所属国家**: China **地区**: Guangdong **城市**: Yunfu **纬度**: 22.930559 **经度**: 112.037300
goo.gl	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
www.googleadservices.com	IP: 58.254.137.166 **所属国家**: China **地区**: Guangdong **城市**: Yunfu **纬度**: 22.930559 **经度**: 112.037300
onesignal.com	IP: 104.18.214.59 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
dashif.org	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
rest.opensubtitles.org	IP: 172.64.193.8 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700

	经度: -122.395203
aomedia.org	IP: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
schemas.microsoft.com	IP: 13.107.213.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
api.onesignal.com	IP: 104.18.215.59 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
developer.apple.com	IP: 17.253.85.203 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
pagead2.googlesyndication.com	IP: 58.254.149.166 **所属国家**: China **地区**: Guangdong **城市**: Yunfu **纬度**: 22.930559 **经度**: 112.037300
	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
pro.ip-api.com	**IP**: 18.162.49.53 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692

URL线索

URL信息	Url所在文件
https://aomedia.org/emsg/ID3	defpackage/ab0.java
https://developer.apple.com/streaming/emsg-id3	defpackage/ab0.java
https://firebase.google.com/support/privacy/init-options.	defpackage/aj0.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	defpackage/b04.java
http://ns.adobe.com/xap/1.0/	defpackage/d31.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	defpackage/ef3.java
https://uptostream.com/api/streaming/source/get?token=&file_code=	defpackage/eg3.java
http://ns.adobe.com/xap/1.0/\u0000	defpackage/ec0.java
http://www.w3.org/ns/ttml	defpackage/fc3.java

https://app-measurement.com/a	defpackage/hl4.java
http://.	defpackage/ij2.java
https://exoplayer.dev/issues/cleartext-not-permitted	defpackage/iu0.java
https://google.com/search?	defpackage/kz4.java
https://www.dailymotion.com/embed/video/	defpackage/mr.java
https://app-measurement.com/a	defpackage/ng5.java
http://schemas.android.com/apk/res/android	defpackage/oe3.java
https://play.google.com/store/apps/details?id=	defpackage/ow0.java
https://goo.gl/J1sWQy	defpackage/pl4.java
http://dashif.org/guidelines/last-segment-number	defpackage/qr.java
http://dashif.org/guidelines/trickmode	defpackage/qr.java
https://www.google.com	defpackage/qz4.java
https://pro.ip-api.com/json?fields=2181826&key=bfZaACAMusWJuJJ	defpackage/sq3.java
https://goo.gl/NAOOOI.	defpackage/ta5.java
https://goo.gl/NAOOOI	defpackage/ta5.java
https://www.googleadservices.com/pagead/conversion/app/deeplink? id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s	defpackage/ta5.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	defpackage/td0.java

https://firebase.google.com/support/guides/disable-analytics	defpackage/tl4.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	defpackage/tu0.java
https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	defpackage/tu2.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	defpackage/tw2.java
https://google.com	defpackage/vf0.java
https://plus.google.com/	defpackage/wq5.java
https://issuetracker.google.com/issues/new?component=413107&template=1096568	defpackage/y3.java
https://x</LA_URL>	defpackage/ym0.java
https://x	defpackage/ym0.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	defpackage/zw1.java
https://rest.opensubtitles.org/search	com/masterwok/opensubtitlesandroid/OpenSubtitlesUrlBuilder.java
https://awsindstream.com	com/offshore/pikachu/view/Embed.java
https://onesignal.com/android_frame.html	com/onesignal/Kkkkkkkkkkkkk.java
https://api.onesignal.com/	com/onesignal/Kkkkkkkkk.java
http://%s:%d%s	com/p2pengine/sdk/AbsProxy.java
https://offshore1play.firebaseio.com	Mogua Engine V1

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	defpackage/cz4.java

手机线索

手机号	所在文件
17512775099	defpackage/b9.java
15552000000	defpackage/tz4.java

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=44, ST=London, L=UK, O=Android, OU=Android, CN=Sam Jeo
签名算法: rsassa_pkcs1v15
有效期自: 2021-05-22 12:52:33+00:00
有效期至: 2046-05-16 12:52:33+00:00
发行人: C=44, ST=London, L=UK, O=Android, OU=Android, CN=Sam Jeo
序列号: 0x2ac58556
哈希算法: sha256
md5值: 0f2607dd87141a1429c1926d76427aa0
sha1值: 290636e9063ad03b85d043ffddec37cf714e9121
sha256值: 1c6462e89bf1f6545535e437948d8ea78c9714ab1fe03f1ac9ce0ef36f334cce
sha512值: 9261ca88029138e290a24a0d0c8b8af4e435ff5fca538793ea625b9209c8a218dc19c957476073b1f081002d454c53274ab9ce167b0cb1f58db1da8ca2b81b99
公钥算法: rsa
密钥长度: 2048

指纹: 6ac17028eca038cee9be68a965a439d9b9838d4e500784f36e9fc4feeb4eab29

硬编码敏感信息

可能的敏感信息
"firebase_database_url" : "https://offshore1play.firebaseio.com"
"google_api_key" : "AIzaSyAprP6BLafKpKrmCu5kOv_Ttky0oYS3-Hs"
"google_crash_reporting_api_key" : "AIzaSyAprP6BLafKpKrmCu5kOv_Ttky0oYS3-Hs"

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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
android.permission.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.ACCESS_NOTIFICATION_POLICY	正常		希望访问通知策略的应用程序的标记权限。
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.offshore.pikachu.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.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。
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
	正	显示应用程	

android.permission.READ_APP_BADGE	常	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。
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
com.google.android.gms.permission.AD_ID	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

应用内通信