MoGua

他他GV 1.2.2.APK 分析报告

APP名称:	他他GV

包名:	com.android.d1737023149465182549
域名线索:	9条
URL线索:	17条
邮箱线索:	1条
分析日期:	2025年9月29日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: ssdh666_1.2.2_23240870.apk
文件大小: 25.42MB
MD5值: af101a3b093a08a547ad8a5853a06706
SHA1值: 4aff7f42fdfcd07390ceadbe9b7cd0d02cd651ae
SHA256值: 09f110a582e478a9c986f6da9b3e2ae7de889e66b58e72c36314ae7f501b2def

APP 信息

App名称: 他他GV
包名: com.android.d1737023149465182549
主活动Activity: com.grass.mh.ui.SplashActivity
安卓版本名称: 1.2.2
安卓版本: 122

域名线索

域名	服务器信息
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
playready.directtaps.net	**IP**: 104.45.231.79 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
ns.adobe.com	没有服务器地理信息.
	IP: 98.136.147.18

data.flurry.com	**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
schemas.android.com	没有服务器地理信息.
tc-bj-alijs-1324672756.cos.ap-beijing.myqcloud.com	IP: 119.188.21.26 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223
github.com	IP: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
d3ic7k4g8955c9.cloudfront.net	IP: 13.32.53.103 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
schemas.microsoft.com	IP: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	b/j/b/b/e.java
http://ns.adobe.com/xap/1.0/\u0000	b/n/a/a.java
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videocache/HttpUrlSource.java
http://%s:%d/%s	com/danikula/videocache/Pinger.java
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java
https://tc-bj-alijs-1324672756.cos.ap-beijing.myqcloud.com/nt.json	com/grass/mh/ui/SplashActivity.java
https://d3ic7k4g8955c9.cloudfront.net/nt.json	com/grass/mh/ui/SplashActivity.java
https://data.flurry.com/aap.do	d/e/b/s0.java
https://data.flurry.com/v1/flr.do	d/e/b/t0.java
http://schemas.android.com/apk/res/android	l/a/a/f.java
http://schemas.android.com/apk/res/android	org/dsq/library/widget/tablayout/SlidingTabLayout.java
http://schemas.android.com/apk/res/android	org/dsq/library/widget/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	org/dsq/library/widget/tablayout/CommonTabLayout.java

http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://playready.directtaps.net/pr/svc/rightsmanager.asmx	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	com/danikula/videocache/HttpUrlSource.java

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.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=24, ST=24, L=24, O=24, OU=24, CN=24
签名算法: rsassa_pkcs1v15
有效期自: 2023-03-07 12:53:42+00:00
有效期至: 2048-02-29 12:53:42+00:00
发行人: C=24, ST=24, L=24, O=24, OU=24, CN=24
序列号: 0x52b8a6d5
哈希算法: sha256
md5值: 7fb92a0abbbde89f6cb2c77a589e5a5e
sha1值: 72f80a6e6e05263e666d979e237d2d94252155bf
sha256值: 949fc56d959f35cbc80a0ed8c759a97cb4b2724d02f041b9c7938f427fbaf809
sha512值: d7af34a56f2cd65783d18b1a8180bf155a7ea34216d803fd542ad550eba26e98640ff3137e6cd7700b712d36e59b199bb3b3137056f74cc058576cd71ce5f5db
公钥算法: rsa
密钥长度: 2048
指纹: 134f915744306059b413db7b42320d20cb17111e5886c37e712f13adaeed1519

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.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.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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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_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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference

应用内通信
