MoGua

GTV 2.0.2.APK 分析报告

APP名称: GTV

包名:	jp.tazyk.hlbixm
域名线索:	17条
URL线索:	21条
邮箱线索:	2条
分析日期:	2025年7月7日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: gtv_2.0.2_250510_1.apk
文件大小: 13.46MB
MD5值: 4db815ebfce387b74b43be1a017d530d
SHA1值: c46819bb3ea273578954054d7531f50fb99a4168
SHA256值: 8c9b49eb472dde90dac30a0a06751c1b37dbb1b41e3a709a9efef2c36352861b

APP 信息

App名称: GTV
包名: jp.tazyk.hlbixm
主活动Activity: com.xgaymv.activity.SplashActivity
安卓版本名称: 2.0.2
安卓版本: 202

域名线索

域名	服务器信息
www.example.com	**IP**: 23.220.70.41 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
cfg.flurry.com	**IP**: 69.147.80.15 **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
www.openssl.org	**IP**: 34.49.79.89 **所属国家**: United States of America **地区**: California

	城市: Mountain View **纬度**: 37.405991 **经度**: -122.078514
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
schemas.microsoft.com	**IP**: 13.107.246.73 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
staff.yitkan.com	**IP**: 172.67.174.76 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api1.abriyezu.xyz	**IP**: 156.255.123.52 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
api.login.yahoo.com	**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
data.flurry.com	没有服务器地理信息.

api2.abriyezu.xyz	**IP**: 156.255.123.52 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
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
api3.abriyezu.xyz	**IP**: 156.255.123.52 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
h.trace.qq.com	**IP**: 113.56.189.246 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170 **经度**: 115.077606
ns.adobe.com	没有服务器地理信息.
dashif.org	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
	IP: 104.18.22.19

www.w3.org	**所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
raw.githubusercontent.com	**IP**: 185.199.111.133 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724

URL线索

URL**信息**	Url**所在文件**
http://www.example.com	com/flurry/sdk/ee.java
https://cfg.flurry.com/sdk/v1/config	com/flurry/sdk/cm.java
https://cfg.flurry.com/sdk/v1/config	com/flurry/sdk/bz.java
https://data.flurry.com/aap.do	com/flurry/sdk/br.java
https://data.flurry.com/v1/flr.do	com/flurry/sdk/bs.java
https://api.login.yahoo.com/oauth2/device_session	com/flurry/sdk/eg.java
https://raw.githubusercontent.com/little-5/backup/master/gv.txt	com/xgaymv/activity/SplashActivity.java
https://staff.yitkan.com/	com/xgaymv/videoplayer/SimpleCoverVideoPlayer.java
https://github.com/danikula/AndroidVideoCache/issues/88.	d/d/a/i.java

https://github.com/danikula/AndroidVideoCache/issues/43.	d/d/a/i.java
https://github.com/danikula/AndroidVideoCache/issues.	d/d/a/i.java
http://%s:%d/%s	d/d/a/k.java
https://github.com/danikula/AndroidVideoCache/issues/134.	d/d/a/k.java
http://%s:%d/%s	d/d/a/g.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	d/g/a/a/i2.java
http://dashif.org/guidelines/trickmode	d/g/a/a/z2/u0/f.java
http://dashif.org/guidelines/last-segment-number	d/g/a/a/z2/u0/m/d.java
http://dashif.org/guidelines/trickmode	d/g/a/a/z2/u0/m/d.java
https://x</LA_URL>	d/g/a/a/s2/i0.java
https://x	d/g/a/a/s2/i0.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	d/g/a/a/s2/j0.java
http://ns.adobe.com/xap/1.0/	d/g/a/a/u2/h0/a.java
https://h.trace.qq.com/kv	d/n/a/a/b/b.java
https://api1.abriyezu.xyz/api.php	d/p/j/j.java
https://api2.abriyezu.xyz/api.php	d/p/j/j.java
https://api3.abriyezu.xyz/api.php	d/p/j/j.java

https://github.com/vinc3m1	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView.git	摸瓜V1引擎
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	d/d/a/i.java
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

手机线索

手机号	所在文件
17512775099	d/g/b/c/a.java
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=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=.
签名算法: rsassa_pkcs1v15
有效期自: 2025-05-10 08:59:02+00:00
有效期至: 2026-05-10 08:59:02+00:00
发行人: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=.
序列号: 0x3dbe727e
哈希算法: sha256
md5值: 425113eac30a450ef258ffb21cb0c941
sha1值: b364d816dfebd41d9a5f60d0cdf3a7fa8bd39a9f
sha256值: e04a8bada5dadf42b4bc5d140d61014ef82291b208af5c035b286714b2dc217e
sha512值: 739e8450697c48294b7f91631e8f6571e29e938734fa52a83ff0bafaf491ead6e3ea9a4981f63e87a32a67cde784ac178bbef84d52856261dc3fae72744e6732
公钥算法: rsa
密钥长度: 2048
指纹: 657225a233f8c3b4cc060381bff852d52ed849786c711135e98ed1c3f66501b7

🔑 硬编码敏感信息

可能的敏感信息
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"modify_pwd" : "修改密碼"
"modify_pwd_img" : "修改中..."
"modify_pwd_success" : "密碼修改成功"
"pwd_not_same" : "前後密碼不一致"
"reg_input_pwd_1" : "請填寫密碼"

"reg_input_pwd_2" : "請確認密碼"
"str_account_certificate" : "賬號憑證"
"str_authorize_now" : "馬上授權"
"str_general_user" : "普通用戶"
"str_input_account_user_name" : "請輸入持卡人姓名"
"str_mod_pwd" : "修改密碼"
"str_private_letters" : "私信"
"str_save_account_certificate" : "保存賬號憑證"
"str_user" : "用戶"
"video_author" : "视频作者"

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.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.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.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_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

应用内通信