



MoGua

台灣彩券 3.2.1.APK 分析報告



APP名称:

台灣彩券

包名: `com.taiwanlottery.newmobileselect`

域名线索: 14条

URL线索: 16条

邮箱线索: 1条

分析日期: 2025年6月12日

分析平台: [摸瓜APK反编译平台](#)

文件名: base.apk
文件大小: 6.64MB
MD5值: c70af881d6d0f1be697668a229c5a44c
SHA1值: db521396e4cb8a6ace8d35285a8f1a7c71a9db64
SHA256值: d9dbd334fd52b88a3a44b96931f057c00ac794d3e821ce2278534a7df0f70c94

i APP 信息

App名称: 台灣彩券
包名: com.taiwanlottery.newmobileselect
主活动Activity: com.softmobile.newmobileselect.ui.home.HomeActivity
安卓版本名称: 3.2.1
安卓版本: 57

🔍 域名线索

域名	服务器信息
google.com	IP: 74.125.20.139 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
schemas.android.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
firebaseinstallations.googleapis.com	IP: 192.178.163.95 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: 114.250.67.38 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
pagead2.googleadsyndication.com	IP: 114.250.65.38 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
issuetracker.google.com	IP: 74.125.142.102 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.google.com	IP: 31.13.94.36 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires 纬度: -34.603600 经度: -58.381554
firebase-settings.crashlytics.com	IP: 114.250.67.34 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

goo.gl	IP: 74.125.20.102 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
maps.google.com	IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
app-measurement.com	IP: 114.250.63.33 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.taiwanlottery.com	IP: 31.13.81.4 所属国家: Poland 地区: Mazowieckie 城市: Warsaw 纬度: 52.229771 经度: 21.011780
accounts.google.com	IP: 142.250.107.84 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: 142.250.99.113 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991

🌐 URL线索

URL信息	Url所在文件
https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/	B3/r.java
https://firebase.google.com/docs/crashlytics/get-started?platform=android	B3/r.java
https://www.google.com	B3/C0027p.java
https://app-measurement.com/a	K1/AbstractC0078z.java
https://goo.gl/NAOOOI.	K1/m1.java
https://goo.gl/NAOOOI	K1/m1.java
https://google.com/search?	K1/RunnableC0077y0.java
https://firebase.google.com/support/guides/disable-analytics	K1/C.java
https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=	K1/RunnableC0067t0.java
http://schemas.android.com/apk/res/android	C/b.java
http://maps.google.com/maps?	D4/a.java
http://maps.google.com/maps?	com/softmobile/newmobileselect/ui/station/StationInfoCardFragment.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	W/u.java

https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	W0/c.java
https://firebase.google.com/support/privacy/init-options.	v3/c.java
https://accounts.google.com/o/oauth2/revoke?token=	a1/RunnableC0135c.java
https://firebaseinstallations.googleapis.com/v1/	x3/C1231c.java
https://www.taiwanlottery.com	E4/b.java

 邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	d1/k.java

 手机线索

手机号	所在文件
15552000000	K1/D0.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=TW, L=Taipei, CN=Sky
签名算法: rsassa_pkcs1v15
有效期自: 2017-10-16 02:35:55+00:00
有效期至: 2116-09-22 02:35:55+00:00
发行人: C=TW, L=Taipei, CN=Sky
序列号: 0x1fcbb570
哈希算法: sha256
md5值: f11c54aaea1bd5fd85214da4b1f89300
sha1值: 1489575d8aabb5bb920786303d9911efe981d176
sha256值: f4c38ea581770e6e24d43e514cb083f633847b1cac5bccf2418d1a19fdaa8a61
sha512值: add2522c2505ef1bf0afbc1c64413aadecf01734e5519a5d033088143a00a41d21a94df29557cb1df9d095200e06516b013fecb1c9afcd6940d2796d5bcb4233
公钥算法: rsa
密钥长度: 2048
指纹: 9d7469f9c8c71e45fceccea847926a5b19a9922735e2b7570e1016074d2a0e7e

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.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.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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
android.permission.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
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
	正	防止手机睡	

android.permission.WAKE_LOCK	常	眠	允许应用程序防止手机进入睡眠状态
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	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.taiwanlottery.newmobileselect.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.softmobile.newmobileselect.ui.home.HomeActivity	Schemes: @string/url_scheme://,