



MoGua

谜妹漫画 1.7.6-942.APK 分析报告



APP名称:

谜妹漫画

包名:	com.mimei17
域名线索:	25条
URL线索:	28条
邮箱线索:	7条
分析日期:	2025年10月8日
分析平台:	摸瓜APK反编译平台

文件名: mimei1_lilgosu01_17mimei1.com.apk
文件大小: 17.95MB
MD5值: ea372b4773291c86e9c1a5ec31f844c1
SHA1值: bcf0ee1bc7e4706e90077f58a98867dbb112381c
SHA256值: e929b4eb3b573da01cf4040368345c3e4298b137c9f0d276dc87e73412abf37b

i APP 信息

App名称: 谜妹漫画
包名: com.mimei17
主活动Activity: com.mimei17.activity.splash.SplashActivity
安卓版本名称: 1.7.6-942
安卓版本: 942

🔍 域名线索

域名	服务器信息
in.appcenter.ms	IP: 40.70.161.102 所属国家: United States of America 地区: Virginia 城市: Boydton 纬度: 36.667641 经度: -78.387497
mimei-formal.firebaseio.com	IP: 35.201.97.85 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
xml.org	IP: 104.239.240.11 所属国家: United States of America 地区: Texas

	城市: Windcrest 纬度: 29.499678 经度: -98.399246
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
firebase-settings.crashlytics.com	IP: 58.254.149.162 所属国家: China 地区: Guangdong 城市: Yunfu 纬度: 22.930559 经度: 112.037300
plus.google.com	IP: 157.240.10.36 所属国家: United States of America 地区: California 城市: Menlo Park 纬度: 37.436935 经度: -122.193604
image.zcm360.com	IP: 13.33.5.18 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
update.crashlytics.com	IP: 58.254.149.162 所属国家: China 地区: Guangdong 城市: Yunfu 纬度: 22.930559 经度: 112.037300
reports.crashlytics.com	没有服务器地理信息.

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
mobile.events.data.microsoft.com	IP: 20.189.173.12 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418
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
public.zxxll.cn	IP: 60.28.216.232 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
crashpad.chromium.org	IP: 142.251.42.243 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
	IP: 61.241.140.113 所属国家: China 地区: Anhui

public.gtyu1.cn	城市: Bozhou 纬度: 33.877220 经度: 115.770279
www.googleadservices.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
www.android.com	IP: 172.217.160.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
public.meme95.com	IP: 13.224.141.109 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
goo.gl	IP: 172.217.160.110 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: 118.107.180.216 所属国家: Palestine, State of 地区: Hebron 城市: Hebron 纬度: 31.533266 经度: 35.100475

ns.adobe.com	没有服务器地理信息.
google.com	IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan 纬度: 45.464336 经度: 9.188547
d8mn34.zcm360.com	IP: 13.33.5.69 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
app-measurement.com	IP: 58.254.149.161 所属国家: China 地区: Guangdong 城市: Yunfu 纬度: 22.930559 经度: 112.037300
public.meme92.com	IP: 13.224.141.106 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322

URL线索

URL信息	Url所在文件
https://plus.google.com/	a5/u0.java

https://github.com/Zielony/Carbon/issues.	carbon/widget/EditText.java
http://www.android.com/	d4/a.java
https://firebase.google.com/support/privacy/init-options.	e8/b.java
https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	g7/c.java
http://www.w3.org/1999/xlink	j1/j.java
http://xml.org/sax/properties/lexical-handler	j1/j.java
http://www.w3.org/2000/svg	j1/j.java
http://www.w3.org/TR/SVG11/feature	j1/j.java
https://in.appcenter.ms	k9/a.java
https://mobile.events.data.microsoft.com/OneCollector/1.0	k9/c.java
https://app-measurement.com/a	l5/aa.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	pd/d.java
https://firebase.google.com/support/guides/disable-analytics	q5/a2.java
https://google.com/search?	q5/b5.java
https://www.google.com	q5/c5.java
https://goo.gl/NAOOOI.	q5/h7.java
https://goo.gl/NAOOOI	q5/h7.java

https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s	q5/n4.java
https://app-measurement.com/a	q5/w1.java
https://update.crashlytics.com/spi/v1/platforms/android/apps/%s	r7/g.java
https://reports.crashlytics.com/spi/v1/platforms/android/apps/%s/reports	r7/g.java
https://reports.crashlytics.com/sdk-api/v1/platforms/android/apps/%s/minidumps	r7/g.java
https://d8mn34.zcm360.com	sc/a.java
https://public.meme92.com/host_app.txt	sc/a.java
https://public.meme95.com/host_app.txt	sc/a.java
https://public.zxzxll.cn/host_app.txt	sc/a.java
https://public.gtyu1.cn/host_app.txt	sc/a.java
http://hostname/?	t4/n.java
https://image.zcm360.com	vc/a.java
https://mimei-formal.firebaseio.com	Mogua Engine V1
https://crashpad.chromium.org/bug/new	lib/arm64-v8a/libcrashlytics-common.so
https://crashpad.chromium.org/	lib/arm64-v8a/libcrashlytics-common.so
https://crashpad.chromium.org/bug/new	lib/armeabi-v7a/libcrashlytics-common.so
https://crashpad.chromium.org/	lib/armeabi-v7a/libcrashlytics-common.so

http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libnative-imagetranscoder.so
https://crashpad.chromium.org/bug/new	lib/x86/libcrashlytics-common.so
https://crashpad.chromium.org/	lib/x86/libcrashlytics-common.so
https://crashpad.chromium.org/bug/new	lib/x86_64/libcrashlytics-common.so
https://crashpad.chromium.org/	lib/x86_64/libcrashlytics-common.so

 邮箱线索

邮箱地址	所在文件
this@changebindfragment.childfragm	com/mimei17/activity/info/changebind/ChangeBindFragment.java
this@forgetpwdfragment.childfragm	com/mimei17/activity/info/forget/ForgetPwdFragment.java
this@loginfragment.childfragm	com/mimei17/activity/info/login/LoginFragment.java
this@bindfragment.childfragm	com/mimei17/activity/info/register/BindFragment.java
mimei.service@gmail.com	com/mimei17/activity/info/setting/SettingFragment.java
mimei.service@gmail.com	com/mimei17/app/BaseViewModel.java
u0013android@android.com0 u0013android@android.com	x4/p.java

 手机线索

手机号	所在文件
17179869184	j1/j.java
17179869184	j1/g.java
15552000000	q5/d5.java
17512775099	x6/a.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: O=17mimei
签名算法: rsassa_pkcs1v15
有效期自: 2019-07-05 10:54:20+00:00
有效期至: 2044-06-28 10:54:20+00:00
发行人: O=17mimei
序列号: 0x100bbf3d
哈希算法: sha256
md5值: ae2ce2e8954ea7e670c300716f23c097
sha1值: ba1e12e24dc061ed4ba95890b8c81e5a7b47f0bd
sha256值: 0fdbfddc1a7ccc3bdb13d34da71f36019694d6f4717f60e7392970f1a276eeb7
sha512值: b17f33fa9f9aebdefbd1f817ea5419f230a301c8d89ebfb0431d07f5e20e2e8d7811c2bf2487db4797b65ebfaf88c20c7af7298616d3e4ab241ba5cdf52ee54
公钥算法: rsa
密钥长度: 2048
指纹: b70efa7988a41fd577d2c85ae16471b9baece4737c606cd92c938e2da704263d

🔑 硬编码敏感信息

可能的敏感信息
"bottom_nav_user" : "会员"
"com.google.firebase.crashlytics.mapping_file_id" : "45adcff236724491871690fab7eb7106"
"comic_intro_author" : "漫画作者"
"firebase_database_url" : "https://mimei-formal.firebaseio.com"
"google_api_key" : "AlzaSyABazzxFfH-E3veQyWyCZQLOQRGCKxXZ0U"
"google_crash_reporting_api_key" : "AlzaSyABazzxFfH-E3veQyWyCZQLOQRGCKxXZ0U"
"info_enter_password" : "请输入密码"
"info_forget_password" : "忘记密码"
"info_password" : "密码"
"info_set_password" : "设定密码"
"info_wrong_format_password" : "密码格式不符合，请重新输入"
"info_wrong_password" : "密码有误，请重新输入"
"bottom_nav_user" : "会员"
"comic_intro_author" : "漫画作者"
"info_enter_password" : "请输入密码"
"info_forget_password" : "忘记密码"
"info_password" : "密码"

"info_set_password" : "设定密码"
"info_wrong_format_password" : "密码格式不符合，请重新输入"
"info_wrong_password" : "密码有误，请重新输入"
"bottom_nav_user" : "會員"
"comic_intro_author" : "漫畫作者"
"info_enter_password" : "請輸入密碼"
"info_forget_password" : "忘記密碼"
"info_password" : "密碼"
"info_set_password" : "設定密碼"
"info_wrong_format_password" : "密碼格式不符合，請重新輸入"
"info_wrong_password" : "密碼有誤，請重新輸入"

 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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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.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.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.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。
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
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
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
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

应用内通信