



# MoGua

## 哥特少女勇闯恶魔城 1.0.23.APK 分析报告



APP名称:

哥特少女勇闯恶魔城

包名:	com.yxxinglin.xzid37330
域名线索:	4条
URL线索:	3条
邮箱线索:	2条
分析日期:	2024年9月19日
分析平台:	<a href="#">摸瓜APK反编译平台</a>

## 文件信息

文件名: gtsnycemc.apk

文件大小: 6.9MB

MD5值: 60b23a2e72afb3988d3faa10b0452338

SHA1值: 576c5feafd2d722baaac2bf997d4083577d64fbc

SHA256值: cc66ed7c6c16bb87f8aea493e36854ef5ccfaa18d6927a2b014ce2fa36b434e9

## i APP 信息

App名称: 哥特少女勇闯恶魔城

包名: com.yxxinglin.xzid37330

主活动Activity: com.KillmondayGames.FranBowCh3.RunnerActivity

安卓版本名称: 1.0.23

安卓版本: 1000023

## 🔍 域名线索

域名	服务器信息
market.android.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
sdb.amazonaws.com	IP: 54.239.24.238 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.043720 经度: -77.487488
www.openssl.org	IP: 23.11.156.84 所属国家: Thailand 地区: Krung Thep Maha Nakhon 城市: Bangkok

	纬度: 13.750000 经度: 100.516670
pingback.yoyogames.com	没有服务器地理信息.

## URL线索

URL信息	Url所在文件
<a href="http://market.android.com/support/bin/answer.py?answer=1050566&amp;hl=%lang%&amp;dl=%region%">http://market.android.com/support/bin/answer.py?answer=1050566&amp;hl=%lang%&amp;dl=%region%</a>	Mogua Engine V1
<a href="http://pingback.yoyogames.com?a=">http://pingback.yoyogames.com?a=</a>	lib/armeabi/libyoyo.so
<a href="http://www.openssl.org/support/faq.html">http://www.openssl.org/support/faq.html</a>	lib/armeabi/libyoyo.so
<a href="http://sdb.amazonaws.com">http://sdb.amazonaws.com</a>	lib/armeabi/libyoyo.so
<a href="http://pingback.yoyogames.com?a=">http://pingback.yoyogames.com?a=</a>	lib/armeabi-v7a/libyoyo.so
<a href="http://www.openssl.org/support/faq.html">http://www.openssl.org/support/faq.html</a>	lib/armeabi-v7a/libyoyo.so
<a href="http://sdb.amazonaws.com">http://sdb.amazonaws.com</a>	lib/armeabi-v7a/libyoyo.so

## 邮箱线索

邮箱地址	所在文件
ftp@example.com	lib/armeabi/libyoyo.so
ftp@example.com	lib/armeabi-v7a/libyoyo.so

## 手机线索

## 签名证书

APK已签名

v1 签名: True

v2 签名: False

v3 签名: False

找到 1 个唯一证书

主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com

签名算法: rsassa\_pkcs1v15

有效期自: 2008-02-29 01:33:46+00:00

有效期至: 2035-07-17 01:33:46+00:00

发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com

序列号: 0x936eacbe07f201df

哈希算法: sha1

md5值: e89b158e4bcf988ebd09eb83f5378e87

sha1值: 61ed377e85d386a8df6e6b864bd85b0bfaa5af81

sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc

sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569

## 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
登录摸瓜网站后查看		

## 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.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_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
com.android.vending.CHECK_LICENSE	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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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

## 应用内通信

---

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。