



白娘子 1.0.0.0.APK 分析报告



APP名称:

白娘子

包名:	com.bnzcq.sysdk
域名线索:	21条
URL线索:	22条
邮箱线索:	1条
分析日期:	2025年6月30日
分析平台:	摸瓜APK反编译平台

文件名: bainiangzi1.1_2265.com.apk
文件大小: 298.08MB
MD5值: e60810bc02c57c69ec552bad22a9b511
SHA1值: b27aaf5681f1abd27ddc108050ae5ce5d4791913
SHA256值: 9aa57c4b39b359c3c6591b25ff71203554177064a667d03e6c43c263a1eaaddc

i APP 信息

App名称: 白娘子
包名: com.bnzcq.sysdk
主活动Activity: com.cilugame.h1.UnityPlayerActivity
安卓版本名称: 1.0.0.0
安卓版本: 1

🔍 域名线索

域名	服务器信息
weixin.qq.com	IP: 182.50.12.167 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
d.alipay.com	IP: 123.125.216.242 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
dev.sdk.cilugame.com	IP: 183.6.21.133 所属国家: China 地区: Guangdong

	城市: Guangzhou 纬度: 23.127361 经度: 113.264572
dev.185sy.com	IP: 81.68.185.27 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
apilocate.amap.com	IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.sy527.com	IP: 154.92.62.28 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
restapi.amap.com	IP: 106.11.43.113 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
p.185sy.com	IP: 118.89.186.125 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

www.qq.com	IP: 221.198.70.47 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
182.254.116.117	IP: 182.254.116.117 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545673 经度: 114.068108
www.baidu.com	IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
api.uca.cloud.unity3d.com	IP: 43.156.88.56 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
pingma.qq.com	IP: 116.147.19.64 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
cgicol.amap.com	IP: 123.125.216.212 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501

	经度: 116.397102
apilocatesrc.amap.com	IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
config.uca.cloud.unity3d.com	IP: 34.111.113.40 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
log.reyun.com	IP: 52.80.199.120 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
abroad.apilocate.amap.com	IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
api.185sy.com	IP: 81.68.185.27 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
stats.unity3d.com	没有服务器地理信息.

lbs.amap.com	IP: 59.82.31.203 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
--------------	--

 URL线索

URL信息	Url所在文件
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/amap/api/location/AMapLocation.java
https://dev.sdk.cilugame.com/v1/sdkc/pay/orderid.json	com/cilugame/h1/CLSDKPlugin.java
http://restapi.amap.com/v3/place/around?	com/loc/a.java
http://restapi.amap.com/v3/place/text?	com/loc/a.java
http://restapi.amap.com/v3/config/district?	com/loc/a.java
http://apilocate.amap.com/mobile/binary	com/loc/cs.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/cs.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/cl.java
http://apilicatesrc.amap.com/mobile/binary	com/loc/cl.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/cx.java
http://cgicol.amap.com/collection/writedata?ver=v1.0_ali&	com/loc/ce.java

https://restapi.amap.com/v3/iasdkauth	com/loc/l.java
http://restapi.amap.com/v3/iasdkauth	com/loc/l.java
http://restapi.amap.com	com/loc/q.java
http://restapi.amap.com/v3/geocode/regeo	com/loc/bu.java
http://log.reyun.com/	com/reyun/common/ReYunConst.java
http://log.reyun.com/receive/rest/heartbeat	com/reyun/sdk/ReYunGame.java
http://log.reyun.com/receive/pkginfo	com/reyun/utis/HttpNetworkUtil.java
http://log.reyun.com/receive/tkio/	com/reyun/utis/HttpNetworkUtil.java
http://log.reyun.com/receive/rest/	com/reyun/utis/HttpNetworkUtil.java
http://log.reyun.com/receive/track/	com/reyun/utis/HttpNetworkUtil.java
http://dev.185sy.com	com/ssy185/sdk/SDKManager.java
http://www.sy527.com	com/sy/sdk/model/HttpUrls.java
http://api.185sy.com/	com/sy/sdk/model/HttpUrls.java
http://p.185sy.com/index.php?g=api&m=FreeSub&a=get_c	com/sy/sdk/model/HttpUrls.java
http://api.185sy.com/index.php?g=api&m=index&a=map	com/sy/sdk/model/HttpUrls.java
http://api.185sy.com/index.php?g=api&m=user&a=upload_log	com/sy/sdk/resloader/ReadConfig.java
https://d.alipay.com	com/sy/sdk/ui/dialog/PayDialog.java
https://weixin.qq.com	com/sy/sdk/ui/dialog/PayDialog.java

http://182.254.116.117/d?dn=99e2d153e4d0527186ebed5ac5608367&id=6&ttl=1	com/tencent/android/tpush/service/b/b.java
http://www.baidu.com	com/tencent/android/tpush/service/channel/i.java
http://www.qq.com	com/tencent/android/tpush/service/channel/i.java
http://pingma.qq.com:80/mstat/report	com/tencent/android/tpush/stat/c.java
http://rp	com/xsj/crasheye/util/Utils.java
https://stats.unity3d.com/HWStatsUpdate.cgi	lib/armeabi-v7a/libunity.so
https://stats.unity3d.com/HWStats.cgi	lib/armeabi-v7a/libunity.so
https://config.uca.cloud.unity3d.com	lib/armeabi-v7a/libunity.so
https://api.uca.cloud.unity3d.com/v1/events	lib/armeabi-v7a/libunity.so

 邮箱线索

邮箱地址	所在文件
ctwap@mycdma.cn	com/tencent/mid/a/a.java

 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=china, ST=sichuan, L=chengdu, O=jiangxihuyu, OU=rc, CN=lz
签名算法: rsassa_pkcs1v15
有效期自: 2017-10-17 02:34:43+00:00
有效期至: 2027-10-15 02:34:43+00:00
发行人: C=china, ST=sichuan, L=chengdu, O=jiangxihuyu, OU=rc, CN=lz
序列号: 0x2c69f187
哈希算法: sha256
md5值: 1985aba51314baca016662533522ed3c
sha1值: 2261b8176af6219d418c8f03dbb381cd00da67df
sha256值: 2f13e3076a26ef0ae2d21fe98c4a1b61ea281054a06be23d53c6e7ab077843b4
sha512值: aa8e01066899be3deb97fb7bd6e34e0aed504a8df23c92b0a8b4b70ab7ce28abd67fbadd8e6eaabd718ced47c78752fbf8cdbd57b504c04ba83b2c66a2712bf1

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.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.BATTERY_STATS	合法	修改电池统计信息	允许修改收集的电池统计信息。不供普通应用程序使用
android.permission.WRITE_MEDIA_STORAGE	未知	Unknown permission	Unknown permission from android reference
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_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.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.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.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消

			息,从而使您付出代价
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令, 恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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。
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference

android.permission.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
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.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小

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。