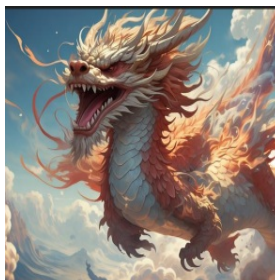




## 道士出观-潜龙出渊 3.2.0.APK 分析报告



APP名称:

道士出观-潜龙出渊

包名: com.xinyu.hc\_993000082

域名线索: 45条

URL线索: 28条

邮箱线索: 0条

分析日期: 2025年6月26日

分析平台: [摸瓜APK反编译平台](#)

文件名: 道士出观-潜龙.apk  
文件大小: 59.29MB  
MD5值: 3a30e31f97eed1a1185820d18437f77a  
SHA1值: 92b34ceebce18baf22b146a57b1fbef45705578  
SHA256值: 708660e07dd0c3d595de61a43ed7518841b3559560cdeda137669c830f76ab29

## i APP 信息

App名称: 道士出观-潜龙出渊  
包名: com.xinyu.hc\_993000082  
主活动Activity: com.xinyu.deviceutils.DevicesUtils  
安卓版本名称: 3.2.0  
安卓版本: 1

## 🔍 域名线索

| 域名                     | 服务器信息                                                                                              |
|------------------------|----------------------------------------------------------------------------------------------------|
| 140.210.20.53          | IP: 140.210.20.53<br>所属国家: China<br>地区: Jiangsu<br>城市: Yangzhou<br>纬度: 32.397221<br>经度: 119.435600 |
| paygate-yf.meituan.com | IP: 103.37.152.89<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102  |
| rtapplog.snssdk.com    | IP: 42.56.93.207<br>所属国家: China<br>地区: Liaoning                                                    |

|                         |                                                                                                       |
|-------------------------|-------------------------------------------------------------------------------------------------------|
|                         | 城市: Shenyang<br>纬度: 41.792221<br>经度: 123.432877                                                       |
| mta.qq.com              | IP: 0.0.0.1<br>所属国家: -<br>地区: -<br>城市: -<br>纬度: 0.000000<br>经度: 0.000000                              |
| long.open.weixin.qq.com | IP: 112.65.193.150<br>所属国家: China<br>地区: Shanghai<br>城市: Shanghai<br>纬度: 31.224333<br>经度: 121.468948  |
| alogsus.umeng.com       | IP: 223.109.148.130<br>所属国家: China<br>地区: Jiangsu<br>城市: Nanjing<br>纬度: 32.061668<br>经度: 118.777992   |
| open.weixin.qq.com      | IP: 116.128.169.212<br>所属国家: China<br>地区: Shanghai<br>城市: Shanghai<br>纬度: 31.224333<br>经度: 121.468948 |
| ichannel.snssdk.com     | IP: 111.202.5.198<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102     |
|                         | IP: 116.136.186.208                                                                                   |

|                        |                                                                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| success.ctobsnssdk.com | <b>所属国家:</b> China<br><b>地区:</b> Nei Mongol<br><b>城市:</b> Hohhot<br><b>纬度:</b> 40.810650<br><b>经度:</b> 111.650665                                         |
| api.weixin.qq.com      | <b>IP:</b> 116.128.170.42<br><b>所属国家:</b> China<br><b>地区:</b> Shanghai<br><b>城市:</b> Shanghai<br><b>纬度:</b> 31.224333<br><b>经度:</b> 121.468948            |
| mclient.alipay.com     | <b>IP:</b> 218.24.90.224<br><b>所属国家:</b> China<br><b>地区:</b> Liaoning<br><b>城市:</b> Shenyang<br><b>纬度:</b> 41.792221<br><b>经度:</b> 123.432877             |
| ouplog.umeng.com       | <b>IP:</b> 47.246.110.93<br><b>所属国家:</b> Singapore<br><b>地区:</b> Singapore<br><b>城市:</b> Singapore<br><b>纬度:</b> 1.289987<br><b>经度:</b> 103.850281        |
| mta.oa.com             | <b>IP:</b> 141.144.196.217<br><b>所属国家:</b> Netherlands<br><b>地区:</b> Noord-Holland<br><b>城市:</b> Amsterdam<br><b>纬度:</b> 52.378502<br><b>经度:</b> 4.899980 |
| www.baidu.com          | <b>IP:</b> 110.242.69.21<br><b>所属国家:</b> China<br><b>地区:</b> Hebei<br><b>城市:</b> Baoding<br><b>纬度:</b> 38.851109<br><b>经度:</b> 115.490280                 |

|                               |                                                                                                      |
|-------------------------------|------------------------------------------------------------------------------------------------------|
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息.                                                                                           |
| pay.bjylhyu.com               | 没有服务器地理信息.                                                                                           |
| toblog.ctobsnssdk.com         | IP: 111.161.204.165<br>所属国家: China<br>地区: Tianjin<br>城市: Tianjin<br>纬度: 39.142181<br>经度: 117.176102  |
| ucc.umeng.com                 | IP: 203.119.169.82<br>所属国家: China<br>地区: Zhejiang<br>城市: Hangzhou<br>纬度: 30.293650<br>经度: 120.161583 |
| errlog.umeng.com              | IP: 223.109.148.129<br>所属国家: China<br>地区: Jiangsu<br>城市: Nanjing<br>纬度: 32.061668<br>经度: 118.777992  |
| pv.sohu.com                   | IP: 101.72.227.61<br>所属国家: China<br>地区: Hebei<br>城市: Langfang<br>纬度: 39.509720<br>经度: 116.694717     |
| deeplink.umeng.com            | IP: 59.82.31.210<br>所属国家: China<br>地区: Zhejiang<br>城市: Hangzhou<br>纬度: 30.293650<br>经度: 120.161583   |

|                         |                                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| gjapplog.ucweb.com      | IP: 157.185.189.158<br>所属国家: Canada<br>地区: Ontario<br>城市: North York<br>纬度: 43.771862<br>经度: -79.331528                         |
| applog.snssdk.com       | IP: 116.136.186.207<br>所属国家: China<br>地区: Nei Mongol<br>城市: Hohhot<br>纬度: 40.810650<br>经度: 111.650665                           |
| issuetracker.google.com | IP: 74.125.142.113<br>所属国家: United States of America<br>地区: California<br>城市: Mountain View<br>纬度: 37.405991<br>经度: -122.078514 |
| log.snssdk.com          | IP: 106.74.132.33<br>所属国家: China<br>地区: Shandong<br>城市: Jinan<br>纬度: 36.668331<br>经度: 116.997223                                |
| databyterangers.com.cn  | 没有服务器地理信息.                                                                                                                      |
| rtlog.snssdk.com        | IP: 116.136.186.207<br>所属国家: China<br>地区: Nei Mongol<br>城市: Hohhot<br>纬度: 40.810650<br>经度: 111.650665                           |
|                         | IP: 125.39.155.58                                                                                                               |

|                          |                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| h5.m.taobao.com          | <b>所属国家:</b> China<br><b>地区:</b> Tianjin<br><b>城市:</b> Tianjin<br><b>纬度:</b> 39.142181<br><b>经度:</b> 117.176102                          |
| mobilegw.aaa.alipay.net  | 没有服务器地理信息.                                                                                                                               |
| plbslog.umeng.com        | IP: 36.156.202.68<br><b>所属国家:</b> China<br><b>地区:</b> Jiangsu<br><b>城市:</b> Yangzhou<br><b>纬度:</b> 32.397221<br><b>经度:</b> 119.435600    |
| tobapplog.ctobsnssdk.com | IP: 211.90.25.203<br><b>所属国家:</b> China<br><b>地区:</b> Hebei<br><b>城市:</b> Handan<br><b>纬度:</b> 36.600559<br><b>经度:</b> 114.467781        |
| developer.umeng.com      | IP: 59.82.112.112<br><b>所属国家:</b> China<br><b>地区:</b> Zhejiang<br><b>城市:</b> Hangzhou<br><b>纬度:</b> 30.293650<br><b>经度:</b> 120.161583   |
| applog.uc.cn             | IP: 116.132.223.75<br><b>所属国家:</b> China<br><b>地区:</b> Hebei<br><b>城市:</b> Shijiazhuang<br><b>纬度:</b> 38.041599<br><b>经度:</b> 114.478081 |
| mobilegw.alipay.com      | IP: 203.209.255.248<br><b>所属国家:</b> China<br><b>地区:</b> Zhejiang                                                                         |



|                        |                                                                                                                                         |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
|                        | <b>城市:</b> Hangzhou<br><b>纬度:</b> 30.293650<br><b>经度:</b> 120.161583                                                                    |
| alogus.umeng.com       | IP: 223.109.148.176<br><b>所属国家:</b> China<br><b>地区:</b> Jiangsu<br><b>城市:</b> Nanjing<br><b>纬度:</b> 32.061668<br><b>经度:</b> 118.777992  |
| mcgw.alipay.com        | IP: 116.142.234.145<br><b>所属国家:</b> China<br><b>地区:</b> Beijing<br><b>城市:</b> Beijing<br><b>纬度:</b> 39.907501<br><b>经度:</b> 116.397102  |
| pslog.umeng.com        | IP: 59.82.60.44<br><b>所属国家:</b> China<br><b>地区:</b> Zhejiang<br><b>城市:</b> Hangzhou<br><b>纬度:</b> 30.293650<br><b>经度:</b> 120.161583    |
| mobilegw.alipaydev.com | IP: 110.75.132.131<br><b>所属国家:</b> China<br><b>地区:</b> Zhejiang<br><b>城市:</b> Hangzhou<br><b>纬度:</b> 30.293650<br><b>经度:</b> 120.161583 |
| m.alipay.com           | IP: 203.209.245.74<br><b>所属国家:</b> China<br><b>地区:</b> Zhejiang<br><b>城市:</b> Hangzhou<br><b>纬度:</b> 30.293650<br><b>经度:</b> 120.161583 |
|                        |                                                                                                                                         |

|                            |                                                                                                                                |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| pingma.qq.com              | IP: 0.0.0.1<br>所属国家: -<br>地区: -<br>城市: -<br>纬度: 0.000000<br>经度: 0.000000                                                       |
| mobilegw.stable.alipay.net | 没有服务器地理信息.                                                                                                                     |
| wappaygw.alipay.com        | IP: 116.142.234.146<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                            |
| ulogs.umengcloud.com       | IP: 223.109.148.176<br>所属国家: China<br>地区: Jiangsu<br>城市: Nanjing<br>纬度: 32.061668<br>经度: 118.777992                            |
| ulogs.umeng.com            | IP: 223.109.148.176<br>所属国家: China<br>地区: Jiangsu<br>城市: Nanjing<br>纬度: 32.061668<br>经度: 118.777992                            |
| xmlpull.org                | IP: 185.199.111.153<br>所属国家: United States of America<br>地区: Pennsylvania<br>城市: California<br>纬度: 40.065647<br>经度: -79.891724 |

## URL线索

| URL信息                                                                  | Url所在文件                                                     |
|------------------------------------------------------------------------|-------------------------------------------------------------|
| https://issuetracker.google.com/issues/116541301\n                     | android/databinding/tool/writer/BaseLayoutBinderWriter.java |
| https://mobilegw.alipay.com/mgw.htm                                    | com/alipay/sdk/cons/a.java                                  |
| https://mobilegw.alipaydev.com/mgw.htm                                 | com/alipay/sdk/cons/a.java                                  |
| http://m.alipay.com/?action=h5quit                                     | com/alipay/sdk/cons/a.java                                  |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm?                  | com/alipay/sdk/cons/a.java                                  |
| https://mclient.alipay.com/home/exterfaceAssign.htm?                   | com/alipay/sdk/cons/a.java                                  |
| https://mcgw.alipay.com/sdklog.do                                      | com/alipay/sdk/packet/impl/c.java                           |
| http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=\$OrderId\$&   | com/alipay/sdk/data/a.java                                  |
| https://mobilegw.alipay.com/mgw.htm                                    | com/alipay/apmobilesecuritysdk/b/a.java                     |
| http://mobilegw.aaa.alipay.net/mgw.htm                                 | com/alipay/apmobilesecuritysdk/b/a.java                     |
| http://mobilegw-1-64.test.alipay.net/mgw.htm                           | com/alipay/apmobilesecuritysdk/b/a.java                     |
| http://mobilegw.stable.alipay.net/mgw.htm                              | com/alipay/apmobilesecuritysdk/b/a.java                     |
| https://paygate-yf.meituan.com/paygate/notify/alipay/paynotify/simple\ | com/alipay/test/a.java                                      |
| https://databyterangers.com.cn                                         | com/bytedance/applog/r0.java                                |
| https://log.snssdk.com/service/2/device_register/                      | com/bytedance/applog/util/UriConstants.java                 |

|                                                          |                                                  |
|----------------------------------------------------------|--------------------------------------------------|
| https://ichannel.snssdk.com/service/2/app_alert_check/   | com/bytedance/applog/util/UriConstants.java      |
| https://log.snssdk.com/service/2/app_log/                | com/bytedance/applog/util/UriConstants.java      |
| https://applog.snssdk.com/service/2/app_log/             | com/bytedance/applog/util/UriConstants.java      |
| https://rtlog.snssdk.com/service/2/app_log/              | com/bytedance/applog/util/UriConstants.java      |
| https://rtapplog.snssdk.com/service/2/app_log/           | com/bytedance/applog/util/UriConstants.java      |
| https://log.snssdk.com/service/2/log_settings/           | com/bytedance/applog/util/UriConstants.java      |
| https://toblog.ctobsnssdk.com/service/2/device_register/ | com/bytedance/applog/util/UriConstants.java      |
| https://toblog.ctobsnssdk.com/service/2/app_alert_check/ | com/bytedance/applog/util/UriConstants.java      |
| https://toblog.ctobsnssdk.com/service/2/app_log/         | com/bytedance/applog/util/UriConstants.java      |
| https://tobapplog.ctobsnssdk.com/service/2/app_log/      | com/bytedance/applog/util/UriConstants.java      |
| https://toblog.ctobsnssdk.com/service/2/log_settings/    | com/bytedance/applog/util/UriConstants.java      |
| https://toblog.ctobsnssdk.com/service/2/abtest_config/   | com/bytedance/applog/util/UriConstants.java      |
| https://success.ctobsnssdk.com/service/2/app_log/        | com/bytedance/applog/util/UriConstants.java      |
| http://pay.bjylhyu.com                                   | com/m3sdk/common/webview/C_WebViewActivity.java  |
| http://pay.bjylhyu.com                                   | com/m3sdk/common/webview/C_WebViewActivity2.java |
| http://mta.qq.com/                                       | com/tencent/wxop/stat/StatServiceImpl.java       |
| http://mta.oa.com/                                       | com/tencent/wxop/stat/StatServiceImpl.java       |
|                                                          |                                                  |

|                                                                                                              |                                                 |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| http://pingma.qq.com:80/mstat/report                                                                         | com/tencent/wxop/stat/common/StatConstants.java |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuiid=%s                                          | com/tencent/mm/opensdk/diffdev/a/f.java         |
| https://open.weixin.qq.com/connect/sdk/qrconnect?<br>appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s | com/tencent/mm/opensdk/diffdev/a/d.java         |
| https://errlog.umeng.com/upload                                                                              | com/uc/crashsdk/e.java                          |
| https://gjapplog.ucweb.com/collect                                                                           | com/uc/crashsdk/a/h.java                        |
| https://applog.uc.cn/collect                                                                                 | com/uc/crashsdk/a/h.java                        |
| https://errlog.umeng.com/api/crashsdk/validate                                                               | com/uc/crashsdk/a/d.java                        |
| https://deeplink.umeng.com/deeplink/match                                                                    | com/umeng/analytics/b.java                      |
| http://developer.umeng.com/docs/66650/cate/66650                                                             | com/umeng/analytics/pro/i.java                  |
| https://ucc.umeng.com/v1/fetch                                                                               | com/umeng/analytics/pro/ai.java                 |
| https://pslog.umeng.com/ablog                                                                                | com/umeng/analytics/pro/ai.java                 |
| https://ulogs.umeng.com                                                                                      | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogus.umeng.com                                                                                     | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogsus.umeng.com                                                                                    | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://ulogs.umengcloud.com                                                                                 | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://pslog.umeng.com                                                                                      | com/umeng/commonsdk/vchannel/a.java             |
| https://pslog.umeng.com/                                                                                     | com/umeng/commonsdk/vchannel/a.java             |
|                                                                                                              |                                                 |

|                                                           |                                           |
|-----------------------------------------------------------|-------------------------------------------|
| https://developer.umeng.com/docs/66632/detail/            | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://plbslog.umeng.com                                 | com/umeng/commonsdk/stateless/a.java      |
| https://ulogs.umeng.com                                   | com/umeng/commonsdk/stateless/a.java      |
| https://ouplog.umeng.com                                  | com/umeng/commonsdk/stateless/a.java      |
| http://140.210.20.53:9222/hit/report?                     | com/xinyu/deviceutils/DevicesUtils.java   |
| https://www.baidu.com                                     | com/xinyu/deviceutils/DevicesUtils.java   |
| http://pv.sohu.com/cityjson?ie=utf-8                      | com/xinyu/deviceutils/DevicesUtils.java   |
| https://api.weixin.qq.com/sns/oauth2/access_token?appid=  | com/xinyu/pingtai/MainActivity.java       |
| https://api.weixin.qq.com/sns/auth?access_token=          | com/xinyu/pingtai/MainActivity.java       |
| https://api.weixin.qq.com/sns/oauth2/refresh_token?appid= | com/xinyu/pingtai/MainActivity.java       |
| https://api.weixin.qq.com/sns/userinfo?access=            | com/xinyu/pingtai/MainActivity.java       |
| http://xmlpull.org/v1/doc/features.html                   | com/ta/utdid2/b/a/e.java                  |
| http://xmlpull.org/v1/doc/features.html                   | com/ta/utdid2/b/a/a.java                  |

 邮箱线索

 手机线索

|     |      |
|-----|------|
| 手机号 | 所在文件 |
|-----|------|

|             |                              |
|-------------|------------------------------|
| 15552175049 | com/bytedance/applog/n1.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=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown  
签名算法: rsassa\_pkcs1v15  
有效期自: 2023-12-12 06:53:12+00:00  
有效期至: 2123-11-18 06:53:12+00:00  
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown  
序列号: 0x437f973a  
哈希算法: sha256  
md5值: 66b2adf67bdc8f84b2335152444af270  
sha1值: 53cf2449cefceea6499175bbec2cec60ab8a2f84  
sha256值: a16deabdcdb16d470833202b250cbb1362c805af3ec4f6c968aac002ad16e6d  
sha512值: 03b86a7838e7588651fa790fd9b8838c188e463e6d1f9474ceb9b4db126aff882bdb3db51b4ee4959cbc83f4adb65e7b7bd5ce86aaf69b5c49e36d7c36468070  
公钥算法: rsa  
密钥长度: 2048  
指纹: 9120dafdef8b3e534f9624acf6b1ff02e937fec017b745dc8d81f1a250b51b07

## 🔑 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.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.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.MODIFY_AUDIO_SETTINGS  | 正常   | 更改您的音频设置       | 允许应用程序修改全局音频设置,例如音量和路由                                        |
| 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你的位置,并可能消耗额外的电池电量     |



|                                                |    |                    |                                                         |
|------------------------------------------------|----|--------------------|---------------------------------------------------------|
|                                                |    | (GPS)              | 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.READ_PRIVILEGED_PHONE_STATE | 未知 | Unknown permission | Unknown permission from android reference               |
| com.asus.msa.SupplementaryDID.ACCESS           | 未知 | Unknown permission | Unknown permission from android reference               |
| freemme.permission.msa                         | 未知 | Unknown permission | Unknown permission from android reference               |
| android.permission.PERMISSION_GRANTED          | 未知 | Unknown permission | Unknown permission from android reference               |
| 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                       |

应用内通信

| 活动(ACTIVITY)                                     | 通信(INTENT)                                                                      |
|--------------------------------------------------|---------------------------------------------------------------------------------|
| com.bytedance.applog.util.SimulateLaunchActivity | Schemes: rangersapplog.byax6uyt://,<br>Hosts: rangersapplog,<br>Paths: /picker, |