Evaluation Warning: The document was created with Spire.Doc for Python.

**道士出观-潜龙出渊（ 3.2.0版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 道士出观-潜龙出渊 |
| 版本 | 3.2.0 |
| 包名 | com.xinyu.hc\_993000082 |
| 域名线索 | 45条 |
| URL线索 | 28条 |
| APP图标 |  |
| 分析日期 | 2025年6月26日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 道士出观-潜龙.apk |
| 文件大小 | 59.29MB |
| MD5值 | 3a30e31f97eed1a1185820d18437f77a |
| SHA1值 | 92b34ceebce18baf22b146a57b1fbeff45705578 |
| SHA256值 | 708660e07dd0c3d595de61a43ed7518841b3559560cdeda137669c830f76ab29 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 140.210.20.53 | IP: 140.210.20.53 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| paygate-yf.meituan.com | IP: 103.37.152.89 所属国家: China 地区: Beijing 城市: Beijing  |
| rtapplog.snssdk.com | IP: 42.56.93.207 所属国家: China 地区: Liaoning 城市: Shenyang  |
| mta.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| alogsus.umeng.com | IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| open.weixin.qq.com | IP: 116.128.169.212 所属国家: China 地区: Shanghai 城市: Shanghai  |
| ichannel.snssdk.com | IP: 111.202.5.198 所属国家: China 地区: Beijing 城市: Beijing  |
| success.ctobsnssdk.com | IP: 116.136.186.208 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| api.weixin.qq.com | IP: 116.128.170.42 所属国家: China 地区: Shanghai 城市: Shanghai  |
| mclient.alipay.com | IP: 218.24.90.224 所属国家: China 地区: Liaoning 城市: Shenyang  |
| ouplog.umeng.com | IP: 47.246.110.93 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| mta.oa.com | IP: 141.144.196.217 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| www.baidu.com | IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding  |
| 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 所属国家: China 地区: Tianjin 城市: Tianjin  |
| ucc.umeng.com | IP: 203.119.169.82 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| errlog.umeng.com | IP: 223.109.148.129 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| pv.sohu.com | IP: 101.72.227.61 所属国家: China 地区: Hebei 城市: Langfang  |
| deeplink.umeng.com | IP: 59.82.31.210 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| gjapplog.ucweb.com | IP: 157.185.189.158 所属国家: Canada 地区: Ontario 城市: North York  |
| applog.snssdk.com | IP: 116.136.186.207 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| issuetracker.google.com | IP: 74.125.142.113 所属国家: United States of America 地区: California 城市: Mountain View  |
| log.snssdk.com | IP: 106.74.132.33 所属国家: China 地区: Shandong 城市: Jinan  |
| databyterangers.com.cn | 没有服务器地理信息.  |
| rtlog.snssdk.com | IP: 116.136.186.207 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| h5.m.taobao.com | IP: 125.39.155.58 所属国家: China 地区: Tianjin 城市: Tianjin  |
| mobilegw.aaa.alipay.net | 没有服务器地理信息.  |
| plbslog.umeng.com | IP: 36.156.202.68 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| tobapplog.ctobsnssdk.com | IP: 211.90.25.203 所属国家: China 地区: Hebei 城市: Handan  |
| developer.umeng.com | IP: 59.82.112.112 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| applog.uc.cn | IP: 116.132.223.75 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| mobilegw.alipay.com | IP: 203.209.255.248 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| alogus.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| mcgw.alipay.com | IP: 116.142.234.145 所属国家: China 地区: Beijing 城市: Beijing  |
| pslog.umeng.com | IP: 59.82.60.44 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mobilegw.alipaydev.com | IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| m.alipay.com | IP: 203.209.245.74 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| pingma.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| mobilegw.stable.alipay.net | 没有服务器地理信息.  |
| wappaygw.alipay.com | IP: 116.142.234.146 所属国家: China 地区: Beijing 城市: Beijing  |
| ulogs.umengcloud.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| ulogs.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| xmlpull.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |

### **4.2 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&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/f.java  |
| https://open.weixin.qq.com/connect/sdk/qrconnect?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  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15552175049  | com/bytedance/applog/n1.java  |

## **5. 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: a16deabcdcb16d470833202b250cbb1362c805af3ec4f6c968aaac002ad16e6d sha512值: 03b86a7838e7588651fa790fd9b8838c188e463e6d1f9474ceb9b4db126aff882bdb3db51b4ee4959cbc83f4adb65e7b7bd5ce86aaf69b5c49e36d7c36468070 公钥算法: rsa 密钥长度: 2048 指纹: 9120dafdef8b3e534f9624acf6b1ff02e937fec017b745dc8d81f1a250b51b07**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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 |

## **10. 应用内通信**

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

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