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

**枪战英雄（ 0.6.4.077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 | 枪战英雄 |
| 版本 | 0.6.4.077 |
| 包名 | com.sy4399.zjqz |
| 域名线索 | 62条 |
| URL线索 | 69条 |
| APP图标 |  |
| 分析日期 | 2025年9月3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 | qiangzhanyingxiong.apk |
| 文件大小 | 233.95MB |
| MD5值 | 1509567f61e21703027044ec3c96e536 |
| SHA1值 | f3398b36dee089c1ee5378f16a72c8ad9af48989 |
| SHA256值 | b607dc68d81b3c873926d5846d9497d75698eead96f9cb3c8c0d15d402dac1cd |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 枪战英雄 |
| 包名 | com.sy4399.zjqz |
| 主活动Activity | com.fnsdk.unity.FnSdkUnityActivity |
| 安卓版本名称 | 0.6.4.077 |
| 安卓版本 | 2108231130 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| wap.cmpassport.com | IP: 120.232.169.168  所属国家: China  地区: Guangdong  城市: Guangzhou |
| www.openssl.org | IP: 34.49.79.89  所属国家: United States of America  地区: California  城市: Mountain View |
| fusion.qq.com | IP: 116.130.229.204  所属国家: China  地区: Beijing  城市: Beijing |
| collect.ux.21cn.com | IP: 222.93.106.185  所属国家: China  地区: Jiangsu  城市: Suzhou |
| openmobile.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| sdk.open.phone.igexin.com | IP: 101.68.218.177  所属国家: China  地区: Zhejiang  城市: Jiaxing |
| cdn.h5wan.4399sj.com | IP: 123.117.133.190  所属国家: China  地区: Beijing  城市: Beijing |
| cdp.cloud.unity3d.com | IP: 43.156.88.56  所属国家: Singapore  地区: Singapore  城市: Singapore |
| qzs.qq.com | IP: 221.204.20.189  所属国家: China  地区: Shanxi  城市: Taiyuan |
| api-test.4399sy.com | 没有服务器地理信息. |
| xmlpull.org | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| sdk.open.inc2.igexin.com | 没有服务器地理信息. |
| cdn.4399sj.com | IP: 123.126.74.113  所属国家: China  地区: Beijing  城市: Beijing |
| dev.voicecloud.cn | IP: 125.254.169.47  所属国家: China  地区: Beijing  城市: Beijing |
| openapi.openspeech.cn | IP: 125.254.169.47  所属国家: China  地区: Beijing  城市: Beijing |
| mta.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| service.weibo.com | IP: 116.133.8.18  所属国家: China  地区: Beijing  城市: Beijing |
| c.isdspeed.qq.com | 没有服务器地理信息. |
| e.189.cn | IP: 42.123.76.65  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw.stable.alipay.net | 没有服务器地理信息. |
| hxqd.openspeech.cn | IP: 114.118.75.245  所属国家: China  地区: Beijing  城市: Beijing |
| api.yqbgn.com | IP: 42.62.62.45  所属国家: China  地区: Beijing  城市: Beijing |
| m.weibo.cn | IP: 116.133.8.18  所属国家: China  地区: Beijing  城市: Beijing |
| dldir1.qq.com | IP: 118.212.139.65  所属国家: China  地区: Jiangxi  城市: Nanchang |
| api.uca.cloud.unity3d.com | IP: 101.32.104.143  所属国家: Singapore  地区: Singapore  城市: Singapore |
| m.alipay.com | IP: 203.209.245.74  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| api.4399sy.com | IP: 211.159.158.242  所属国家: China  地区: Beijing  城市: Beijing |
| cgi.connect.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| mobile.unionpay.com | 没有服务器地理信息. |
| 4399sy.com | IP: 111.161.121.98  所属国家: China  地区: Tianjin  城市: Tianjin |
| media.weibo.cn | IP: 123.125.107.14  所属国家: China  地区: Beijing  城市: Beijing |
| api.23x32y.com | IP: 119.28.226.139  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| 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 |
| appsupport.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| open.weibo.cn | IP: 123.125.107.13  所属国家: China  地区: Beijing  城市: Beijing |
| fnsdk.4399sy.com | IP: 62.234.43.132  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw.aaa.alipay.net | 没有服务器地理信息. |
| appcashier256.95516.com | IP: 180.130.108.165  所属国家: China  地区: Yunnan  城市: Zhaotong |
| open.weixin.qq.com | IP: 116.128.171.214  所属国家: China  地区: Shanghai  城市: Shanghai |
| ms.zzx9.cn | IP: 124.64.196.28  所属国家: China  地区: Beijing  城市: Beijing |
| api.weibo.com | IP: 123.125.107.13  所属国家: China  地区: Beijing  城市: Beijing |
| dpdcs.4399sy.com | IP: 109.244.60.70  所属国家: China  地区: Beijing  城市: Beijing |
| wlc.4399sy.com | IP: 109.244.51.115  所属国家: China  地区: Beijing  城市: Beijing |
| mcgw.alipay.com | IP: 119.188.53.105  所属国家: China  地区: Shandong  城市: Jinan |
| mobilegw.alipay.com | IP: 203.209.243.27  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: - |
| sdk.open.lbs.igexin.com | 没有服务器地理信息. |
| h5.m.taobao.com | IP: 121.29.103.126  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| www.4399.cn | IP: 123.117.133.134  所属国家: China  地区: Beijing  城市: Beijing |
| mta.oa.com | IP: 141.144.196.217  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| sdk.open.amp.igexin.com | IP: 124.160.124.197  所属国家: China  地区: Zhejiang  城市: Wenzhou |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息. |
| opencloud.wostore.cn | IP: 210.22.123.92  所属国家: China  地区: Shanghai  城市: Shanghai |
| appcashier.test.95516.com | IP: 180.95.171.99  所属国家: China  地区: Gansu  城市: Jinchang |
| fnsdk.demo.4399sy.com | IP: 109.244.51.33  所属国家: China  地区: Beijing  城市: Beijing |
| www.xfyun.cn | IP: 42.62.43.219  所属国家: China  地区: Beijing  城市: Beijing |
| open.e.189.cn | IP: 42.123.76.75  所属国家: China  地区: Beijing  城市: Beijing |
| router.g263.com | IP: 42.62.62.45  所属国家: China  地区: Beijing  城市: Beijing |
| fnapi.4399sy.com | IP: 211.159.174.33  所属国家: China  地区: Beijing  城市: Beijing |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| hydra.alibaba.com | IP: 203.119.169.241  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.go-mono.com | IP: 13.68.229.189  所属国家: United States of America  地区: Virginia  城市: Washington |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://dpdcs.4399sy.com/sdk\_error.php | com/ssjjsy/net/ak.java |
| http://dpdcs.4399sy.com/front\_error.php | com/ssjjsy/net/al.java |
| http://api-test.4399sy.com/plugin/config? | com/ssjjsy/net/Ssjjsy.java |
| http://api-test.4399sy.com/service/version/plugin? | com/ssjjsy/net/Ssjjsy.java |
| https://api.4399sy.com/plugin/config? | com/ssjjsy/net/Ssjjsy.java |
| http://api.4399sy.com/service/version/plugin? | com/ssjjsy/net/Ssjjsy.java |
| https://api.yqbgn.com/plugin/config? | com/ssjjsy/net/Ssjjsy.java |
| http://api.yqbgn.com/service/version/plugin? | com/ssjjsy/net/Ssjjsy.java |
| http://router.g263.com/r.php | com/ssjjsy/net/BgpMgr.java |
| http://dpdcs.4399sy.com/sdk\_error.php | com/ssjjsy/net/an.java |
| http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$& | com/alipay/sdk/data/a.java |
| http://mobilegw.alipay.com/mgw.htm | com/alipay/sdk/cons/a.java |
| http://m.alipay.com/?action=h5quit | com/alipay/sdk/cons/a.java |
| http://mcgw.alipay.com/sdklog.do | com/alipay/sdk/packet/impl/c.java |
| http://mobilegw.stable.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://mobilegw.alipay.com/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.aaa.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://opencloud.wostore.cn/openapi/netauth/precheck/wp? | com/unicom/xiaowo/account/shield/c/b.java |
| http://fnsdk.4399sy.com/sdk/api/login.php | com/fnsdk/unity/FnSdkUnityActivity.java |
| http://xmlpull.org/v1/doc/features.html | com/ta/utdid2/core/persistent/XmlUtils.java |
| http://xmlpull.org/v1/doc/features.html | com/ta/utdid2/core/persistent/FastXmlSerializer.java |
| http://hydra.alibaba.com/ | com/ta/utdid2/aid/AidRequester.java |
| https://api.weibo.com/2/proxy/sdk/statistic.json | com/sina/weibo/sdk/statistic/LogReport.java |
| https://api.weibo.com/oauth2/getaid.json | com/sina/weibo/sdk/utils/AidTask.java |
| https://api.weibo.com/oauth2/getaid.json | com/sina/weibo/sdk/utils/AidTask4Plug.java |
| http://m.weibo.cn/u/ | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| http://media.weibo.cn/article? | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| http://m.weibo.cn/comment? | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| http://m.weibo.cn/ | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| http://m.weibo.cn/index/router? | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| https://m.weibo.cn/p/100103type=1& | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| http://m.weibo.cn/mblog? | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| http://service.weibo.com/share/mobilesdk.php | com/sina/weibo/sdk/web/param/ShareWebViewRequestParam.java |
| http://service.weibo.com/share/mobilesdk\_uppic.php | com/sina/weibo/sdk/web/param/ShareWebViewRequestParam.java |
| https://open.weibo.cn/oauth2/authorize? | com/sina/weibo/sdk/auth/BaseSsoHandler.java |
| https://api.weibo.com/oauth2/access\_token | com/sina/weibo/sdk/auth/AccessTokenKeeper.java |
| http://dldir1.qq.com/gamesafe/mobile/app/android/tpsafe.apk | com/tencent/tersafe2/res/Res.java |
| http://dldir1.qq.com/gamesafe/mobile/app/android/base.ini | com/tencent/tersafe2/res/Res.java |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | com/tencent/mm/sdk/diffdev/a/f.java |
| http://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s | com/tencent/mm/sdk/diffdev/a/d.java |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1 | com/tencent/connect/share/QzoneShare.java |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1 | com/tencent/connect/share/QQShare.java |
| https://openmobile.qq.com/ | com/tencent/connect/common/Constants.java |
| http://openmobile.qq.com/oauth2.0/m\_jump\_by\_version? | com/tencent/connect/common/BaseApi.java |
| http://qzs.qq.com/open/mobile/login/qzsjump.html? | com/tencent/connect/common/BaseApi.java |
| https://openmobile.qq.com/oauth2.0/m\_authorize? | com/tencent/connect/auth/AuthAgent.java |
| https://openmobile.qq.com/user/user\_login\_statis | com/tencent/connect/auth/AuthAgent.java |
| https://openmobile.qq.com/v3/user/get\_info | com/tencent/connect/auth/AuthAgent.java |
| http://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi | com/tencent/connect/auth/AuthAgent.java |
| http://qzs.qq.com/open/mobile/login/qzsjump.html? | com/tencent/connect/auth/a.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 |
| http://qzs.qq.com/open/mobile/request/sdk\_request.html? | com/tencent/open/SocialApiIml.java |
| http://qzs.qq.com/open/mobile/invite/sdk\_invite.html? | com/tencent/open/SocialApiIml.java |
| http://qzs.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html? | com/tencent/open/SocialApiIml.java |
| http://qzs.qq.com | com/tencent/open/SocialApiIml.java |
| http://c.isdspeed.qq.com/code.cgi | com/tencent/open/b/d.java |
| http://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf | com/tencent/open/utils/e.java |
| http://sdk.open.inc2.igexin.com/api.php | com/igexin/getuiext/data/Consts.java |
| http://sdk.open.phone.igexin.com/api.php | com/igexin/getuiext/data/Consts.java |
| http://sdk.open.phone.igexin.com/api.php?format=json&t=1 | com/igexin/getuiext/service/i.java |
| http://sdk.open.amp.igexin.com/api.htm | com/igexin/push/config/SDKUrlConfig.java |
| http://sdk.open.lbs.igexin.com/api.htm | com/igexin/push/config/SDKUrlConfig.java |
| https://api.weibo.com/oauth2/default.html | com/ssjj/fnsdk/share/weibo/WeiboConfig.java |
| https://cdn.h5wan.4399sj.com/mobile-issue/user\_agreement.html | com/ssjj/fnsdk/core/EnvConfigRes.java |
| https://cdn.h5wan.4399sj.com/mobile-issue/privacy.html | com/ssjj/fnsdk/core/EnvConfigRes.java |
| http://fnapi.4399sy.com/sdk/api/children\_protect.php | com/ssjj/fnsdk/core/EnvConfigRes.java |
| http://fnapi.4399sy.com/sdk/api/user\_agreement.php | com/ssjj/fnsdk/core/EnvConfigRes.java |
| http://fnapi.4399sy.com/sdk/api/privacy.php | com/ssjj/fnsdk/core/EnvConfigRes.java |
| http://fnsdk.demo.4399sy.com/sdk/api/fncfg.php | com/ssjj/fnsdk/core/bx.java |
| http://fnsdk.4399sy.com/sdk/api/inlinepage.php | com/ssjj/fnsdk/core/commonweb/popweb/PopGetPopPageConfigTask.java |
| http://fnsdk.4399sy.com/sdk/api/inlinepage.php | com/ssjj/fnsdk/tool/fnpopweb/FNPopPage.java |
| http://fnapi.4399sy.com/sdk/api/privacy.php | com/ssjj/fnsdk/tool/fnpopweb/FNToolConfig.java |
| http://fnapi.4399sy.com/sdk/api/user\_agreement.php | com/ssjj/fnsdk/tool/fnpopweb/FNToolConfig.java |
| https://api.23x32y.com/pZi6CJdhuBko.html | com/ssjj/fnsdk/platform/FNConfig4399.java |
| https://api.23x32y.com/0dFXTAnKHU83.html | com/ssjj/fnsdk/platform/FNConfig4399.java |
| http://www.4399.cn/app-wap-qd-login4399.html?p=24f7b8a7-65e7-4c64-807e-b7a13fa778d5\_1444815695415\_737eb21d | com/ssjj/fnsdk/platform/FNTestDialog4399.java |
| http://wlc.4399sy.com/wlc\_heartbeat\_collection.php | com/ssjj/fn/common/realname/a/b.java |
| http://mobile.unionpay.com/getclient?platform=android&type=securepayplugin | com/unionpay/UPPayAssistEx.java |
| https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\ | com/unionpay/UPPayAssistEx.java |
| https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\ | com/unionpay/mobile/android/utils/c.java |
| http://openapi.openspeech.cn/webapi/wfr.do | com/iflytek/cloud/d/a/a.java |
| http://dev.voicecloud.cn/msc/help.html\ | com/iflytek/cloud/resource/c.java |
| http://dev.voicecloud.cn/msc/help.html | com/iflytek/cloud/resource/c.java |
| http://dev.voicecloud.cn/msc/help.html\ | com/iflytek/cloud/resource/a.java |
| http://dev.voicecloud.cn/msc/help.html | com/iflytek/cloud/resource/a.java |
| http://dev.voicecloud.cn/msc/help.html\ | com/iflytek/cloud/resource/b.java |
| http://dev.voicecloud.cn/msc/help.html | com/iflytek/cloud/resource/b.java |
| http://www.xfyun.cn/s? | com/iflytek/speech/UtilityConfig.java |
| http://hxqd.openspeech.cn/launchconfig | com/iflytek/common/a/d.java |
| https://cdn.4399sj.com | cn/m4399/login/union/main/a.java |
| https://open.e.189.cn/openapi/special/getTimeStamp.do | cn/com/chinatelecom/account/api/c/a.java |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true&appKey= | cn/com/chinatelecom/account/sdk/a/b.java |
| https://wap.cmpassport.com/resources/html/contract.html | cn/com/chinatelecom/account/sdk/a/b.java |
| https://ms.zzx9.cn/html/oauth/protocol.html | cn/com/chinatelecom/account/sdk/a/b.java |
| https://collect.ux.21cn.com/collect/custom/accountMsg | cn/com/chinatelecom/account/a/c.java |
| https://wap.cmpassport.com/resources/html/contract.html | 摸瓜V1引擎 |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | 摸瓜V1引擎 |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true | 摸瓜V1引擎 |
| http://4399sy.com/hd/sypt/notice/privacy/202006/24-45186.html | 摸瓜V1引擎 |
| http://www.openssl.org/support/faq.html | lib/armeabi-v7a/libuptsmaddonmi.so |
| http://www.openssl.org/support/faq.html | lib/armeabi-v7a/libuptsmaddon.so |
| https://appcashier256.95516.com/gateway/mobile/json | lib/armeabi-v7a/libentryexpro.so |
| https://appcashier.test.95516.com/app/mobile/conf | lib/armeabi-v7a/libentryexpro.so |
| https://appcashier256.95516.com/app/mobile/conf | lib/armeabi-v7a/libentryexpro.so |
| https://appcashier.test.95516.com/app/mobile/hft | lib/armeabi-v7a/libentryexpro.so |
| https://appcashier256.95516.com/app/mobile/hft | lib/armeabi-v7a/libentryexpro.so |
| https://appcashier.test.95516.com/app/mobile/json | lib/armeabi-v7a/libentryexpro.so |
| https://appcashier256.95516.com/app/mobile/json | lib/armeabi-v7a/libentryexpro.so |
| https://appcashier.test.95516.com/gateway/mobile/json | lib/armeabi-v7a/libentryexpro.so |
| https://config.uca.cloud.unity3d.com | lib/armeabi-v7a/libunity.so |
| https://cdp.cloud.unity3d.com/v1/events | lib/armeabi-v7a/libunity.so |
| https://api.uca.cloud.unity3d.com/v1/events | lib/armeabi-v7a/libunity.so |
| http://www.openssl.org/support/faq.html | lib/x86/libuptsmaddonmi.so |
| http://www.openssl.org/support/faq.html | lib/x86/libuptsmaddon.so |
| http://www.go-mono.com/delegate.html | lib/x86/libmono.so |
| https://appcashier256.95516.com/gateway/mobile/json | lib/x86/libentryexpro.so |
| https://appcashier.test.95516.com/gateway/mobile/json | lib/x86/libentryexpro.so |
| https://appcashier256.95516.com/app/mobile/hft | lib/x86/libentryexpro.so |
| https://appcashier.test.95516.com/app/mobile/hft | lib/x86/libentryexpro.so |
| https://appcashier256.95516.com/app/mobile/json | lib/x86/libentryexpro.so |
| https://appcashier.test.95516.com/app/mobile/json | lib/x86/libentryexpro.so |
| https://appcashier256.95516.com/app/mobile/conf | lib/x86/libentryexpro.so |
| https://appcashier.test.95516.com/app/mobile/conf | lib/x86/libentryexpro.so |
| https://config.uca.cloud.unity3d.com | lib/x86/libunity.so |
| https://cdp.cloud.unity3d.com/v1/events | lib/x86/libunity.so |
| https://api.uca.cloud.unity3d.com/v1/events | lib/x86/libunity.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ftp@example.com | lib/armeabi-v7a/libtersafe2.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17369024377 | com/ssjj/fnsdk/core/fnd/b.java |
| 15060355040 | com/unionpay/UPPayAssistEx.java |

## **5. 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=CN, ST=Guangdong, L=Guangzhou, O=4399sy.com, OU=4399sy.com, CN=4399 签名算法: rsassa\_pkcs1v15 有效期自: 2015-04-29 06:46:16+00:00 有效期至: 2124-11-03 06:46:16+00:00 发行人: C=CN, ST=Guangdong, L=Guangzhou, O=4399sy.com, OU=4399sy.com, CN=4399 序列号: 0x19fb5c3c 哈希算法: sha256 md5值: 494ecf3907c3dd5ca1a9cc48e22a65f7 sha1值: 8333fd31f421da2da601522e378e88190abeb3af sha256值: 6391d216eb9b572495143eaf815534de23cfee94a1bc4d451b846ddb0a7a7478 sha512值: 5119f6dfd93e2142fb313598a05df753e24be93640028ea37cbbec9526d5329ee2febea59dbdd80b6bd9b55c3763bb759d33aa5eccf52c915c3c4366c14e3ddf**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "fnsdk\_tkey" : "966ed280e0e827bfd299bc18c3af7baa" |

## **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.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.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.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\_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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.CHANGE\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收 | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| getui.permission.GetuiService.com.sy4399.zjqz | 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.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。 |
| 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.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.NFC | 正常 | 控制近场通信 | 允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信 |
| org.simalliance.openmobileai.SMARTCARD | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.fnsdk.unity.FnSdkUnityActivity | **Schemes**: fnzjqz://, fnzjqz1://, |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent1105683229://, |

**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。**