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

**小年糕（ 1.24.5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 | 小年糕 |
| 版本 | 1.24.5 |
| 包名 | cn.xiaoniangao.xngapp |
| 域名线索 | 67条 |
| URL线索 | 82条 |
| APP图标 |  |
| 分析日期 | 2025年6月9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 | xng\_120983.apk |
| 文件大小 | 81.0MB |
| MD5值 | 456e1c4b2c03e0b291dc968293a059d4 |
| SHA1值 | f4fbf332e6f1c09ff417cd5c933a75491f8c13be |
| SHA256值 | 5d8795aeadb0e3c08f36cd61b22fdc1fb697eb1e45ce8d467904c0fcda14565d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 小年糕 |
| 包名 | cn.xiaoniangao.xngapp |
| 主活动Activity | cn.xiaoniangao.xngapp.splash.SplashActivity |
| 安卓版本名称 | 1.24.5 |
| 安卓版本 | 210 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| onekey.cmpassport.com | IP: 120.197.235.28  所属国家: China  地区: Guangdong  城市: Guangzhou |
| openmobile.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| oss.aliyuncs.com | IP: 118.178.29.5  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mp.weixin.qq.com | IP: 223.167.82.219  所属国家: China  地区: Shanghai  城市: Shanghai |
| pms.mb.qq.com | IP: 60.29.240.17  所属国家: China  地区: Tianjin  城市: Tianjin |
| debugx5.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| api.meishesdk.com | IP: 211.159.158.214  所属国家: China  地区: Beijing  城市: Beijing |
| log1.cmpassport.com | IP: 36.138.255.61  所属国家: China  地区: Gansu  城市: Lanzhou |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| oss-cn-hangzhou.aliyuncs.com | IP: 118.31.219.248  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| pre-verify-cloud.alibaba-inc.com | IP: 59.82.17.148  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 |
| www.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| cfg.imtt.qq.com | IP: 60.29.240.17  所属国家: China  地区: Tianjin  城市: Tianjin |
| debugtbs.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| bsedit-1257467088.cos.ap-beijing.myqcloud.com | IP: 218.12.98.48  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| developer.mozilla.org | IP: 34.111.97.67  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| oss-cn-.aliyuncs.comor | 没有服务器地理信息. |
| cgi.qplus.com | 没有服务器地理信息. |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.118.26  所属国家: United States of America  地区: California  城市: San Francisco |
| fusion.qq.com | IP: 116.130.229.204  所属国家: China  地区: Beijing  城市: Beijing |
| mocks.alibaba-inc.com | IP: 59.82.112.188  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| up.xiaoniangao.cn | IP: 106.55.175.254  所属国家: China  地区: Beijing  城市: Beijing |
| green.cn-hangzhou.aliyuncs.com | IP: 106.11.162.143  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| huatuocode.huatuo.qq.com | 没有服务器地理信息. |
| www.xiaoniangao.cn | IP: 119.29.45.60  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| log.tbs.qq.com | IP: 124.95.224.248  所属国家: China  地区: Liaoning  城市: Shenyang |
| oss-cn-zhangjiakou.aliyuncs.com | IP: 47.92.17.37  所属国家: China  地区: Beijing  城市: Beijing |
| wap.cmpassport.com | IP: 120.197.235.27  所属国家: China  地区: Guangdong  城市: Guangzhou |
| unilog.wostore.cn | IP: 116.128.209.129  所属国家: China  地区: Beijing  城市: Beijing |
| astat.bugly.qcloud.com | IP: 119.28.121.133  所属国家: Singapore  地区: Singapore  城市: Singapore |
| jiaocheng.xiaoniangao.cn | IP: 119.29.45.60  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| www.cmpassport.com | IP: 120.197.235.28  所属国家: China  地区: Guangdong  城市: Guangzhou |
| mqqad.html5.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| www.samsungapps.com | IP: 52.31.24.56  所属国家: Ireland  地区: Dublin  城市: Dublin |
| test-app-api.xiaoniangao.cn | IP: 114.242.199.155  所属国家: China  地区: Beijing  城市: Beijing |
| test-kapi-xng-app.xiaoniangao.cn | IP: 114.242.199.155  所属国家: China  地区: Beijing  城市: Beijing |
| ai.login.umeng.com | IP: 59.82.31.160  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86  所属国家: China  地区: Shandong  城市: Qingdao |
| mdc.html5.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| config.cmpassport.com | IP: 120.232.169.180  所属国家: China  地区: Guangdong  城市: Guangzhou |
| ai-login.aliplus.test | 没有服务器地理信息. |
| market.m.taobao.com | IP: 125.39.103.205  所属国家: China  地区: Tianjin  城市: Tianjin |
| www.slf4j.org | IP: 195.15.222.169  所属国家: Switzerland  地区: Geneve  城市: Carouge |
| mta.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| pre-ailogin.umeng.com | 没有服务器地理信息. |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| mta.oa.com | IP: 141.144.196.217  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| image.cnamedomain.com | 没有服务器地理信息. |
| open.weixin.qq.com | IP: 140.207.58.67  所属国家: China  地区: Shanghai  城市: Shanghai |
| opencloud.wostore.cn | IP: 116.128.209.136  所属国家: China  地区: Beijing  城市: Beijing |
| appsupport.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| pingma.qq.com | IP: 116.147.19.64  所属国家: China  地区: Beijing  城市: Beijing |
| e.189.cn | IP: 42.123.76.65  所属国家: China  地区: Beijing  城市: Beijing |
| clairvoyance.xiaoniangao.cn | IP: 111.230.120.140  所属国家: China  地区: Beijing  城市: Beijing |
| login.imgcache.qq.com | IP: 60.213.134.138  所属国家: China  地区: Shandong  城市: Tai'an |
| test-up.xiaoniangao.cn | IP: 114.242.199.155  所属国家: China  地区: Beijing  城市: Beijing |
| rqd.uu.qq.com | IP: 60.28.219.32  所属国家: China  地区: Tianjin  城市: Tianjin |
| android.bugly.qq.com | IP: 124.95.225.169  所属国家: China  地区: Liaoning  城市: Shenyang |
| cgi.connect.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| test-kapi.xiaoniangao.cn | IP: 114.242.199.155  所属国家: China  地区: Beijing  城市: Beijing |
| static2.xiaoniangao.cn | IP: 61.54.7.129  所属国家: China  地区: Henan  城市: Anyang |
| kapi.xiaoniangao.cn | IP: 193.112.231.236  所属国家: China  地区: Beijing  城市: Beijing |
| kapi-xng-app.xiaoniangao.cn | IP: 193.112.231.236  所属国家: China  地区: Beijing  城市: Beijing |
| eco.taobao.com | IP: 59.82.121.179  所属国家: China  地区: Beijing  城市: Beijing |
| id6.me | IP: 42.123.77.138  所属国家: China  地区: Beijing  城市: Beijing |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://h5. | android/taobao/windvane/config/GlobalConfig.java |
| http://h5. | android/taobao/windvane/config/GlobalConfig.java |
| http://api. | android/taobao/windvane/config/GlobalConfig.java |
| https://kapi-xng-app.xiaoniangao.cn | cn/xiaoniangao/common/e/a.java |
| https://kapi.xiaoniangao.cn/live | cn/xiaoniangao/common/e/a.java |
| https://up.xiaoniangao.cn | cn/xiaoniangao/common/e/a.java |
| https://kapi.xiaoniangao.cn | cn/xiaoniangao/common/e/a.java |
| https://test-kapi-xng-app.xiaoniangao.cn | cn/xiaoniangao/common/e/a.java |
| https://test-up.xiaoniangao.cn | cn/xiaoniangao/common/e/a.java |
| https://test-kapi.xiaoniangao.cn/live | cn/xiaoniangao/common/e/a.java |
| https://test-kapi.xiaoniangao.cn | cn/xiaoniangao/common/e/a.java |
| https://test-kapi.xiaoniangao.cn/live-dev | cn/xiaoniangao/common/e/a.java |
| http://test-app-api.xiaoniangao.cn | cn/xiaoniangao/lib/logupload/net/Constants.java |
| https://mp.weixin.qq.com/s?\_\_biz=MzA5MjA3Mjg5Nw==&mid=204183542&idx=1&sn=c2d970883b5d9e225f263238d29ba62a&scene=21 | cn/xiaoniangao/xngapp/bind/config/b.java |
| https://mp.weixin.qq.com/s?\_\_biz=MzA5MjA3Mjg5Nw==&mid=208814832&idx=1&sn=83ff16fb1e70e55bd41930ffb1051b99&scene=21 | cn/xiaoniangao/xngapp/bind/config/b.java |
| https://www.xiaoniangao.cn/privacy | cn/xiaoniangao/xngapp/me/activity/AboutActivity.java |
| https://mp.weixin.qq.com/s?\_\_biz=MzA5MjA3Mjg5Nw==&mid=204183542&idx=1&sn=c2d970883b5d9e225f263238d29ba62a&scene=21 | cn/xiaoniangao/xngapp/me/activity/AboutActivity.java |
| https://static2.xiaoniangao.cn/web/guide/v2/index.html | cn/xiaoniangao/xngapp/me/activity/LoginActivity.java |
| https://static2.xiaoniangao.cn/web/guide/v2/index.html | cn/xiaoniangao/xngapp/me/activity/SettingsActivity.java |
| http://jiaocheng.xiaoniangao.cn/ | cn/xiaoniangao/xngapp/me/activity/SettingsActivity.java |
| https://mp.weixin.qq.com/s?\_\_biz=MzA5MjA3Mjg5Nw==&mid=204183542&idx=1&sn=c2d970883b5d9e225f263238d29ba62a&scene=21 | cn/xiaoniangao/xngapp/me/fragments/LoginWxFragment.java |
| https://www.xiaoniangao.cn/privacy | cn/xiaoniangao/xngapp/me/fragments/LoginWxFragment.java |
| https://e.189.cn/sdk/agreement/detail.do?appKey=E\_189&hidetop=true&returnUrl= | cn/xiaoniangao/xngapp/widget/s.java |
| https://mp.weixin.qq.com/s?\_\_biz=MzA5MjA3Mjg5Nw==&mid=204183542&idx=1&sn=c2d970883b5d9e225f263238d29ba62a&scene=21 | cn/xiaoniangao/xngapp/widget/s.java |
| https://mp.weixin.qq.com/s?\_\_biz=MzA5MjA3Mjg5Nw==&mid=208814832&idx=1&sn=83ff16fb1e70e55bd41930ffb1051b99&scene=21 | cn/xiaoniangao/xngapp/widget/s.java |
| https://mp.weixin.qq.com/s?\_\_biz=MzA5MjA3Mjg5Nw==&mid=204183542&idx=1&sn=c2d970883b5d9e225f263238d29ba62a&scene=21 | cn/xiaoniangao/xngapp/widget/d0/g.java |
| https://www.xiaoniangao.cn/privacy | cn/xiaoniangao/xngapp/widget/d0/h.java |
| https://www.xiaoniangao.cn/privacy | cn/xiaoniangao/xngapp/widget/d0/i.java |
| https://kapi-xng-app.xiaoniangao.cn | cn/xngapp/lib/collect/d/a.java |
| http://test-app-api.xiaoniangao.cn | cn/xngapp/lib/collect/d/a.java |
| https://test-kapi-xng-app.xiaoniangao.cn | cn/xngapp/lib/collect/d/a.java |
| https://test-kapi.xiaoniangao.cn | cn/xngapp/lib/collect/d/a.java |
| https://kapi.xiaoniangao.cn | cn/xngapp/lib/collect/d/a.java |
| https://kapi.xiaoniangao.cn/wallet | cn/xngapp/lib/live/h1/a.java |
| https://kapi.xiaoniangao.cn/gift | cn/xngapp/lib/live/h1/a.java |
| https://test-kapi.xiaoniangao.cn/wallet | cn/xngapp/lib/live/h1/a.java |
| https://test-kapi.xiaoniangao.cn/gift | cn/xngapp/lib/live/h1/a.java |
| https://test-kapi.xiaoniangao.cn/wallet-dev | cn/xngapp/lib/live/h1/a.java |
| https://test-kapi.xiaoniangao.cn/gift-dev | cn/xngapp/lib/live/h1/a.java |
| https://kapi.xiaoniangao.cn/clairvoyance | cn/xngapp/lib/report/c/a.java |
| https://clairvoyance.xiaoniangao.cn | cn/xngapp/lib/report/c/a.java |
| https://static2.xiaoniangao.cn/app/qingjian/qingjianHelpVideoo.MOV | cn/xngapp/lib/video/player/HowMakeVideoPlayerActivity.java |
| https://kapi.xiaoniangao.cn/wallet | cn/xngapp/lib/wallet/c/a.java |
| https://test-kapi.xiaoniangao.cn/wallet | cn/xngapp/lib/wallet/c/a.java |
| https://test-kapi.xiaoniangao.cn/wallet-dev | cn/xngapp/lib/wallet/c/a.java |
| https://ip. | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-hangzhou.aliyuncs.com | com/alibaba/sdk/android/oss/common/OSSConstants.java |
| http://oss.aliyuncs.com | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://127.0.0.1 | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| https://market.m.taobao.com/app/msd/m-rp-h5/cloud.html | com/alibaba/security/realidentity/RPVerify.java |
| https://market.m.taobao.com/app/msd/m-rp-h5/cloud.html | com/alibaba/security/realidentity/build/C.java |
| https://oss-cn-zhangjiakou.aliyuncs.com\ | com/alibaba/security/realidentity/build/\_a.java |
| https://mocks.alibaba-inc.com/mock/cloudauth | com/alibaba/security/realidentity/build/C0295db.java |
| https://green.cn-hangzhou.aliyuncs.com | com/alibaba/security/realidentity/build/C0295db.java |
| http://pre-verify-cloud.alibaba-inc.com | com/alibaba/security/realidentity/build/C0295db.java |
| https://green.cn-hangzhou.aliyuncs.com | com/alibaba/security/realidentity/build/C0302fb.java |
| http://pre-verify-cloud.alibaba-inc.com | com/alibaba/security/realidentity/build/C0302fb.java |
| http://wap.cmpassport.com/resources/html/contract.html | com/cmic/sso/sdk/activity/LoginAuthActivity.java |
| https://e.189.cn/sdk/agreement/detail.do | com/cmic/sso/sdk/activity/LoginAuthActivity.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/danikula/videocache/h.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/danikula/videocache/h.java |
| http://%s:%d/%s | com/danikula/videocache/f.java |
| https://api.meishesdk.com/license/index.php | com/meicam/sdk/NvsCheckExpirationOnline.java |
| https://api.meishesdk.com/statistics/index.php | com/meicam/sdk/NvsStatisticsSender.java |
| https://eco.taobao.com/router/rest | com/mobile/auth/BuildConfig.java |
| https://opencloud.wostore.cn/openapi/netauth/precheck/wp? | com/mobile/auth/ao/b.java |
| https://unilog.wostore.cn:18080/logserver/account/sdknopasswd | com/mobile/auth/ao/b.java |
| https://collect.ux.21cn.com/collect/custom/accountMsg | com/mobile/auth/c/d.java |
| https://id6.me/auth/preauth.do | com/mobile/auth/d/a.java |
| https://wap.cmpassport.com/resources/html/contract.html | com/mobile/auth/gatewayauth/Constant.java |
| https://e.189.cn/sdk/agreement/detail.do?isWap=true&hidetop=true&appKey=8138111118 | com/mobile/auth/gatewayauth/Constant.java |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true | com/mobile/auth/gatewayauth/Constant.java |
| https://id6.me/auth/preauth.do | com/mobile/auth/gatewayauth/utils/b.java |
| https://opencloud.wostore.cn/openapi/netauth/precheck/wp? | com/mobile/auth/gatewayauth/utils/b.java |
| http://www.cmpassport.com/unisdk/rs/getPrePhonescrip | com/mobile/auth/gatewayauth/utils/b.java |
| https://config.cmpassport.com/client/uniConfig | com/mobile/auth/h/a.java |
| https://log1.cmpassport.com:9443/log/logReport | com/mobile/auth/k/y.java |
| https://onekey.cmpassport.com:443/unisdk/ | com/mobile/auth/k/y.java |
| http://onekey.cmpassport.com/unisdk/ | com/mobile/auth/k/y.java |
| http://onekey.cmpassport.com/unisdk/ | com/mobile/auth/k/e.java |
| https://config.cmpassport.com/client/uniConfig | com/mobile/auth/k/e.java |
| https://id6.me/auth/preauth.do | com/mobile/auth/t/c.java |
| https://github.com/yyued/SVGAPlayer-Android | com/opensource/svgaplayer/g.java |
| http://rqd.uu.qq.com/rqd/sync | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java |
| http://android.bugly.qq.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java |
| http://astat.bugly.qcloud.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/a.java |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | com/tencent/bugly/crashreport/common/strategy/a.java |
| http://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | com/tencent/bugly/crashreport/common/strategy/a.java |
| https://openmobile.qq.com/oauth2.0/me | com/tencent/connect/UnionInfo.java |
| https://login.imgcache.qq.com/ptlogin/static/qzsjump.html? | com/tencent/connect/auth/a.java |
| https://openmobile.qq.com/v3/user/get\_info | com/tencent/connect/auth/AuthAgent.java |
| https://openmobile.qq.com/oauth2.0/m\_authorize? | com/tencent/connect/auth/AuthAgent.java |
| https://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi | com/tencent/connect/auth/AuthAgent.java |
| https://openmobile.qq.com/user/user\_login\_statis | com/tencent/connect/auth/AuthAgent.java |
| https://openmobile.qq.com/oauth2.0/m\_jump\_by\_version? | com/tencent/connect/common/BaseApi.java |
| https://login.imgcache.qq.com/ptlogin/static/qzsjump.html? | com/tencent/connect/common/BaseApi.java |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1 | com/tencent/connect/share/QQShare.java |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1 | com/tencent/connect/share/QzoneShare.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://login.imgcache.qq.com/open/mobile/invite/sdk\_invite.html? | com/tencent/open/SocialApiIml.java |
| https://login.imgcache.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html? | com/tencent/open/SocialApiIml.java |
| https://login.imgcache.qq.com | com/tencent/open/SocialApiIml.java |
| https://login.imgcache.qq.com/open/mobile/request/sdk\_request.html? | com/tencent/open/SocialApiIml.java |
| https://openmobile.qq.com/cgi-bin/qunopensdk/check\_group | com/tencent/open/SocialOperation.java |
| https://openmobile.qq.com/cgi-bin/qunopensdk/unbind | com/tencent/open/SocialOperation.java |
| https://huatuocode.huatuo.qq.com | com/tencent/open/a/d.java |
| https://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf | com/tencent/open/utils/f.java |
| http://cgi.qplus.com/report/report | com/tencent/open/utils/k.java |
| https://debugtbs.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugx5.qq.com | com/tencent/smtt/sdk/WebView.java |
| http://debugtbs.qq.com?10000\ | com/tencent/smtt/sdk/WebView.java |
| http://pms.mb.qq.com/rsp204 | com/tencent/smtt/sdk/j.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041 | com/tencent/smtt/sdk/ui/dialog/d.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047 | com/tencent/smtt/sdk/ui/dialog/d.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079 | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u= | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs | com/tencent/smtt/utils/d.java |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k= | com/tencent/smtt/utils/m.java |
| https://log.tbs.qq.com/ajax?c=pu&tk= | com/tencent/smtt/utils/m.java |
| https://log.tbs.qq.com/ajax?c=dl&k= | com/tencent/smtt/utils/m.java |
| https://cfg.imtt.qq.com/tbs?v=2&mk= | com/tencent/smtt/utils/m.java |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k= | com/tencent/smtt/utils/m.java |
| https://mqqad.html5.qq.com/adjs | com/tencent/smtt/utils/m.java |
| https://log.tbs.qq.com/ajax?c=ucfu&k= | com/tencent/smtt/utils/m.java |
| http://pingma.qq.com:80/mstat/report | com/tencent/stat/StatConfig.java |
| http://mta.qq.com/mta/api/ctr\_feedback/add\_feedback | com/tencent/stat/d.java |
| http://mta.qq.com/mta/api/ctr\_feedback/get\_feedback | com/tencent/stat/d.java |
| http://mta.qq.com/mta/api/ctr\_feedback/reply\_feedback | com/tencent/stat/d.java |
| http://mta.qq.com/ | com/tencent/stat/StatServiceImpl.java |
| http://mta.oa.com/ | com/tencent/stat/StatServiceImpl.java |
| http://mta.qq.com/mta/api/ctr\_feedback | com/tencent/stat/common/StatConstants.java |
| http://pingma.qq.com:80/mstat/report | com/tencent/stat/common/StatConstants.java |
| http://pingma.qq.com:80/mstat/report | com/tencent/wxop/stat/StatConfig.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://ai.login.umeng.com/api/umed/mobile/log | com/umeng/umverify/b/a.java |
| http://ai-login.aliplus.test/api/umed/cache | com/umeng/umverify/utils/g.java |
| https://pre-ailogin.umeng.com/api/umed/cache | com/umeng/umverify/utils/g.java |
| https://ai.login.umeng.com/api/umed/cache | com/umeng/umverify/utils/g.java |
| http://www.samsungapps.com/appquery/appDetail.as?appId= | com/xng/jsbridge/utils/AppStoreUtils.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/a.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/e.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/q.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/i.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | io/reactivex/exceptions/OnErrorNotImplementedException.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/exceptions/UndeliverableException.java |
| http://www.slf4j.org/codes.html | org/slf4j/LoggerFactory.java |
| http://www.slf4j.org/codes.html | org/slf4j/MDC.java |
| https://bsedit-1257467088.cos.ap-beijing.myqcloud.com/image/18301371763/B771663C-5FDA-4C77-BF55-4A191FAB4AB6\_L0\_001.png | Mogua Engine V2 |
| https://bsedit-1257467088.cos.ap-beijing.myqcloud.com/image/18301371763/67AA2931-2636-48DA-A0B7-C4EAD34AF0ED\_L0\_001.png | Mogua Engine V2 |
| https://bsedit-1257467088.cos.ap-beijing.myqcloud.com/image/18301371763/IMG\_20200729\_194400.jpg | Mogua Engine V2 |
| https://bsedit-1257467088.cos.ap-beijing.myqcloud.com/audio/18301371763/%E6%A6%A3%E5%B1%B1%E9%81%97%E9%9F%B5%20%E5%8F%98%E8%B0%83.mp3 | Mogua Engine V2 |
| https://bsedit-1257467088.cos.ap-beijing.myqcloud.com/audio/18301371763/1598425182036.wav | Mogua Engine V2 |
| https://bsedit-1257467088.cos.ap-beijing.myqcloud.com/image/18301371763/1598238625495.png | Mogua Engine V2 |
| http://www.apache.org/licenses/LICENSE-2.0 | Mogua Engine V2 |
| https://developer.mozilla.org/en-US/docs/Web/API/Document/execCommand | Mogua Engine V2 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com | com/danikula/videocache/h.java |
| ctwap@mycdma.cn | com/tencent/mid/a/b.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15778476000 | org/joda/time/chrono/BasicChronology.java |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |
| 18301371763 | Mogua Engine V2 |

## **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=cn, ST=北京, L=北京, O=北京小年糕互联网技术有限公司, OU=北京小年糕互联网技术有限公司, CN=小年糕 签名算法: rsassa\_pkcs1v15 有效期自: 2017-08-08 11:13:09+00:00 有效期至: 2044-12-24 11:13:09+00:00 发行人: C=cn, ST=北京, L=北京, O=北京小年糕互联网技术有限公司, OU=北京小年糕互联网技术有限公司, CN=小年糕 序列号: 0x6126edf8 哈希算法: sha256 md5值: 724a6f5518ff773b1ff0b1a9509686ba sha1值: 1cd5fb925683ff2627c96e9dbc1a3f8a631a0982 sha256值: cd502a8764475a72532da7e4f4551e4dec2193717fa60f92dca37beb285b6787 sha512值: 7ffe43ec7c27c3b8f6af5daf8b8b4eb575160374f4d67ee2002aed36b1e931a8153c1bec68e6a247937dc4ea98d43df494df9fd4e566e44b6e0fe2377e3fba78 公钥算法: rsa 密钥长度: 2048 指纹: 96ffec5cfae87b8e65c17b5ec745a585b166f78277ecd11c3e9fb5723d415dc3**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "album\_no\_private\_notice" : "参与活动作品不支持设为私密哦" |
| "bind\_onekey\_phone\_authentication" : "中国移动认证服务条款" |
| "bind\_onekey\_phone\_user" : "用户协议" |
| "china\_mobile\_authentication" : "中国移动认证服务条款" |
| "china\_telecom\_authentication" : "中国电信认证服务条款" |
| "china\_unicom\_authentication" : "中国联通认证服务条款" |
| "face\_auth\_announce" : "由阿里实人认证提供服务" |
| "face\_detect\_auth\_begin\_cancel" : "放弃" |
| "face\_detect\_auth\_begin\_ok" : "开始验证" |
| "face\_detect\_auth\_begin\_title" : "安全验证" |
| "face\_detect\_auth\_pass" : "验证通过" |
| "live\_s\_online\_user" : "%s人" |
| "live\_s\_total\_user" : "%s人已看" |
| "me\_private\_success\_notice" : "已设为隐私 他人只有通过你的分享才能查看" |
| "private\_agree" : "感谢您信任并使用小年糕。 我们将依据《小年糕用户使用协议》及《小年糕隐私政策》来帮助您了解我们在收集、使用、存储和共享您个人信息的情况以及您享有的相关权利。 1. 当您使用小年糕有声影集服务时，服务器会自动记录一些信息，例如您对我们服务的使用情况、IP地址、所访问服务的URL、浏览器的类型和使用的语言以及访问日期和时间等。 2. 当您安装、激活、更新、卸载相关服务或当这些服务定期与小年糕有声影集通信（例如软件的更新）时，系统会将此编号以及与安装相关的信息（例如操作系统类型和应用程序版本号）发送给小年糕有声影集。 3.当您使用具有定位功能的小年糕有声影集服务时，系统会自动处理有关设备的位置信息，以使得您不需要手动输入自身地理坐标就可获得相关服务。 4.为了对不同型号的设备提供更好的服务与体验改善，小年糕有声影集会记录硬件型号、操作系统版本号、手机的国际移动设备身份码（IMEI）、手机的网络设备的硬件地址（MAC）等信息。 5.我们的产品集成友盟+SDK，友盟+SDK需要收集您的设备Mac地址、唯一设备识别码（IMEI/android ID/IDFA/OPENUDID/GUID、SIM 卡 IMSI 信息）以提供统计分析服务，并通过地理位置校准报表数据准确性，提供基础反作弊能力。 " |

## **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.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.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。 |
| 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.permission.BROADCAST\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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\_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.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.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.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.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| cn.xiaoniangao.xngapp.andpermission.bridge | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| cn.xiaoniangao.xngapp.splash.SplashActivity | **Schemes**: xiaoniangao://, http://, https://, tingyun.41670://,  **Hosts:** wx.xiaoniangao.cn, |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent1106164611://, |

**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。**