MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

灰猪特价 2.3.3.APK

APP名称:	灰猪特价
包名:	com.xiaomanxiong.huizhu
域名线索:	56条
URL线索:	61条
邮箱线索:	2条
分析日期:	2022年1月25日 22:02

文件信息

文件名: hztj.apk
文件大小: 6.09MB
MD5值: 0cb8bb3d9cafa62b7cd71a7108d1e906
SHA1值: affd61c5d58b75a1098988ec57d8b3197957e70d
SHA256值: 82374000b7be4160db4d0744b6188a0a702164e12c28abf578de964bcdd073cf

APP 信息

App名称: 灰猪特价
包名: com.xiaomanxiong.huizhu
主活动**Activity:** com.uzmap.pkg.LauncherUI
安卓版本名称: 2.3.3
安卓版本: 127

域名线索

域名	是否危险域名	服务器信息
login.waptest.taobao.com	good	**IP:** 11.163.138.11 所属国家: United States of America 地区: Ohio 城市: Columbus 纬度: 39.966381 经度: -83.012772 查看地图: Google Map

域名	是否危险域名	服务器信息
accountlink.taobao.com	good	IP: 59.82.31.115 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
s.apicloud.com	good	没有服务器地理信息.
www.slf4j.org	good	IP: 83.173.251.158 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366669 经度: 8.550000 查看地图: Google Map
mobilegw.alipay.com	good	IP: 203.209.255.248 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
accountlink.daily.taobao.net	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
pages.tmall.com	good	IP: 60.21.152.107 所属国家: China 地区: Liaoning 城市: Dandong 纬度: 40.129169 经度: 124.394722 查看地图: Google Map
api.weixin.qq.com	good	IP: 109.244.145.152 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
qrlogin.taobao.com	good	IP: 59.82.31.115 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
m.alipay.com	good	IP: 203.209.245.74 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map

域名	是否危险域名	服务器信息
r.apicloud.com	good	IP: 182.92.145.58 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
d.apicloud.com	good	IP: 47.94.176.24 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
mcgw.alipay.com	good	IP: 203.209.250.6 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
as.apicloud.com	good	没有服务器地理信息.
github.com	good	IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903 查看地图: Google Map

域名	是否危险域名	服务器信息
mclient.alipay.com	good	IP: 203.209.250.6 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
login.m.taobao.com	good	IP: 203.119.144.58 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
127.0.0.1	good	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
login.waptest.tbsandbox.com	good	IP: 140.205.69.8 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
pre.nbsdk-baichuan.taobao.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
baichuan-sdk.alicdn.com	good	IP: 123.6.12.252 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613 查看地图: Google Map
main.m.taobao.com	good	IP: 60.21.152.107 所属国家: China 地区: Liaoning 城市: Dandong 纬度: 40.129169 经度: 124.394722 查看地图: Google Map
oss-cn-.aliyuncs.comor	good	没有服务器地理信息.
loggw-exsdk.alipay.com	good	IP: 110.75.130.123 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
m.duanqu.com	good	IP: 59.82.31.175 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
hz.pre.tbusergw.taobao.net	good	没有服务器地理信息.
mobilegw.alipaydev.com	good	IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
open.weixin.qq.com	good	IP: 175.24.209.30 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
render.alipay.com	good	IP: 218.24.90.118 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432777 查看地图: Google Map

域名	是否危险域名	服务器信息
p.apicloud.com	good	IP: 47.93.154.30 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
mgw.m.taobao.com	good	IP: 59.82.31.182 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
wappaygw.alipay.com	good	IP: 203.209.250.6 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
long.open.weixin.qq.com	good	IP: 109.244.217.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
h5.m.taobao.com	good	IP: 60.21.152.107 所属国家: China 地区: Liaoning 城市: Dandong 纬度: 40.129169 经度: 124.394722 查看地图: Google Map
wgo.mmstat.com	good	IP: 59.82.34.234 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
userlink.alicdn.com	good	IP: 180.97.251.251 所属国家: China 地区: Jiangsu 城市: Xuzhou 纬度: 34.266666 经度: 117.166664 查看地图: Google Map
hydra.alibaba.com	good	IP: 203.119.175.213 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
hz.tbusergw.taobao.net	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
login.wapa.taobao.com	good	IP: 140.205.215.168 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
blog.csdn.net	good	IP: 182.92.187.217 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
pre-baichuan-sdk.taobao.com	good	IP: 59.82.17.132 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
image.cnamedomain.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
shop.m.taobao.com	good	**IP:** 203.119.169.89 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
schemas.android.com	good	没有服务器地理信息.
test-baichuan-sdk.alibaba.net	good	没有服务器地理信息.
oss-cn-hangzhou.aliyuncs.com	good	**IP:** 118.31.219.248 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看地图:** Google Map
nbsdk-baichuan.alicdn.com	good	**IP:** 150.138.39.223 **所属国家:** China **地区:** Shandong **城市:** Jinan **纬度:** 36.668331 **经度:** 116.997223 **查看地图:** Google Map
mobilegw.stable.alipay.net	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
a.apicloud.com	good	IP: 182.92.145.58 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
qrlogin.daily.taobao.net	good	没有服务器地理信息.
xmlpull.org	good	IP: 74.50.61.58 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204 查看地图: Google Map
www.alipay.com	good	IP: 203.209.250.50 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
oss.aliyuncs.com	good	IP: 118.178.29.5 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map

域名	是否危险域名	服务器信息
100.69.205.47	good	IP: 100.69.205.47 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map

URL线索

URL信息	Url所在文件
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java

URL信息	Url所在文件
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.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
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/cons/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	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://h5.m.taobao.com/mlapp/olist.html	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://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java

URL信息	Url所在文件
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/c/a/e.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/c/a/a.java
http://hydra.alibaba.com/	com/ta/utdid2/a/b.java
http://schemas.android.com/apk/res/android	com/apicloud/third/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	com/apicloud/third/gif/GifTextView.java
http://schemas.android.com/apk/res/android	com/apicloud/third/gif/GifViewUtils.java
https://www.alipay.com/webviewbridge	com/ali/auth/third/ui/LoginWebViewActivity.java
https://login.m.taobao.com/minisdk/login.htm	com/ali/auth/third/core/config/ConfigManager.java
http://login.m.taobao.com/cooperation/bindLogin.htm?code=%s&IBB=%s&appkey=%s	com/ali/auth/third/core/config/ConfigManager.java
https://qrlogin.taobao.com/qrcodelogin/generateNoLoginQRCode.do?lt=m	com/ali/auth/third/core/config/ConfigManager.java
https://login.m.taobao.com/qrcodeShow.htm?appKey=%s&from=bcqrlogin	com/ali/auth/third/core/config/ConfigManager.java
http://login.waptest.taobao.com/qrcodeShow.htm?appKey=%s&from=bcqrlogin	com/ali/auth/third/core/config/ConfigManager.java
https://login.m.taobao.com/qrcodeLogin.htm?shortURL=%s&from=bcqrlogin	com/ali/auth/third/core/config/ConfigManager.java
https://accountlink.taobao.com/sdkUnbind.htm	com/ali/auth/third/core/config/ConfigManager.java
https://login.waptest.tbsandbox.com/minisdk/login.htm	com/ali/auth/third/core/config/ConfigManager.java

URL信息	Url所在文件
https://login.waptest.taobao.com/minisdk/login.htm	com/ali/auth/third/core/config/ConfigManager.java
https://login.wapa.taobao.com/minisdk/login.htm	com/ali/auth/third/core/config/ConfigManager.java
http://login.waptest.tbsandbox.com/cooperation/bindLogin.htm?code=%s&IBB=%s&appkey=%s	com/ali/auth/third/core/config/ConfigManager.java
http://login.waptest.taobao.com/cooperation/bindLogin.htm?code=%s&IBB=%s&appkey=%s	com/ali/auth/third/core/config/ConfigManager.java
http://login.wapa.taobao.com/cooperation/bindLogin.htm?code=%s&IBB=%s&appkey=%s	com/ali/auth/third/core/config/ConfigManager.java
https://accountlink.daily.taobao.net/sdkUnbind.htm	com/ali/auth/third/core/config/ConfigManager.java
http://login.wapa.taobao.com/qrcodeShow.htm?appKey=%s&from=bcqrlogin	com/ali/auth/third/core/config/ConfigManager.java
http://login.m.taobao.com/qrcodeShow.htm?appKey=%s&from=bcqrlogin	com/ali/auth/third/core/config/ConfigManager.java
http://qrlogin.daily.taobao.net/qrcodelogin/generateNoLoginQRCode.do?lt=m	com/ali/auth/third/core/config/ConfigManager.java
http://hz.pre.tbusergw.taobao.net/gw.do	com/ali/auth/third/core/rpc/b.java
http://hz.tbusergw.taobao.net/gw.do	com/ali/auth/third/core/rpc/b.java
https://mgw.m.taobao.com/gw.do	com/ali/auth/third/core/rpc/b.java
https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code	com/uzmap/pkg/uzmodules/uzWx/tasks/AccessTokenTask.java

URL信息	Url所在文件
https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=%s&grant_type=refresh_token&refresh_token=%s	com/uzmap/pkg/uzmodules/uzWx/tasks/AccessTokenTask.java
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s&lang=%s	com/uzmap/pkg/uzmodules/uzWx/tasks/GetUserInfoTask.java
http://blog.csdn.net/diyangxia	com/handsome/zhihuiyuntian/insharemodule/InShareModule.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.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
http://oss-cn-hangzhou.aliyuncs.com	com/alibaba/sdk/android/oss/common/OSSConstants.java
http://100.69.205.47/authHint.htm?apiList=	com/alibaba/baichuan/trade/biz/auth/AlibcAuth.java
http://pre.nbsdk-baichuan.taobao.com/authHint.htm?apiList=	com/alibaba/baichuan/trade/biz/auth/AlibcAuth.java
https://nbsdk-baichuan.alicdn.com/authHint.htm?apiList=	com/alibaba/baichuan/trade/biz/auth/AlibcAuth.java
https://h5.m.taobao.com/awp/core/detail.htm	com/alibaba/baichuan/trade/biz/core/config/AlibcConfigService.java
https://shop.m.taobao.com/shop/shop_index.htm	com/alibaba/baichuan/trade/biz/core/config/AlibcConfigService.java

URL信息	Url所在文件
https://main.m.taobao.com/cart/index.html	com/alibaba/baichuan/trade/biz/core/config/AlibcConfigService.java
https://h5.m.taobao.com/cm/snap/index.html	com/alibaba/baichuan/trade/biz/core/config/AlibcConfigService.java
https://h5.m.taobao.com/mlapp/olist.html	com/alibaba/baichuan/trade/biz/core/config/AlibcConfigService.java
https://pre-baichuan-sdk.taobao.com/%s/%s/%s/%s/rule.htm	com/alibaba/baichuan/trade/biz/core/config/AlibcConfigBusiness.java
https://test-baichuan-sdk.alibaba.net/%s/%s/%s/%s/rule.htm	com/alibaba/baichuan/trade/biz/core/config/AlibcConfigBusiness.java
https://baichuan-sdk.alicdn.com/%s/%s/%s/%s/rule.htm	com/alibaba/baichuan/trade/biz/core/config/AlibcConfigBusiness.java
https://shop.m.taobao.com/shop/shop_index.htm?shop_id=%s	com/alibaba/baichuan/trade/biz/applink/adapter/AlibcApplinkPlugin.java
https://h5.m.taobao.com/awp/core/detail.htm?id=%s	com/alibaba/baichuan/trade/biz/applink/adapter/AlibcApplinkPlugin.java
https://wgo.mmstat.com/%s?	com/alibaba/baichuan/trade/common/adapter/ut/a/a.java
https://h5.m.taobao.com/	com/alibaba/baichuan/android/trade/AlibcContext.java
https://m.duanqu.com?	com/alibaba/baichuan/android/trade/AlibcContext.java
https://userlink.alicdn.com/matrix_app/android/matrix_app_config.json	com/alibaba/alibclinkpartner/smartlink/config/ALSLConfigration.java
https://userlink.alicdn.com/matrix_app/android/safe_package_config.json	com/alibaba/alibclinkpartner/smartlink/config/ALSLConfigration.java
https://userlink.alicdn.com/smart_link/smart_link_config.json	com/alibaba/alibclinkpartner/smartlink/config/ALSLConfigration.java
https://userlink.alicdn.com/smart_link/android/alsl_switch_config.json	com/alibaba/alibclinkpartner/smartlink/config/ALSLConfigration.java

URL信息	Url所在文件
https://wgo.mmstat.com/%s?	com/alibaba/alibclinkpartner/smartlink/b/a.java
https://)?((?:	com/alibaba/alibclinkpartner/smartlink/util/g.java
https://h5.m.taobao.com/hd/downLoadAnroidSimple.html	com/alibaba/alibclinkpartner/smartlink/callback/ALSLLocalConfig.java
https://pages.tmall.com/wow/mit/act/download	com/alibaba/alibclinkpartner/smartlink/callback/ALSLLocalConfig.java
http://h5.m.taobao.com/awp/core/detail.htm?id=%s	com/alibaba/alibclinkpartner/linkpartner/constants/ALPParamConstant.java
http://shop.m.taobao.com/shop/shopIndex.htm?shop_id=%s	com/alibaba/alibclinkpartner/linkpartner/constants/ALPParamConstant.java
http://www.slf4j.org/codes.html#no_static_mdc_binder	org/slf4j/MDC.java
http://www.slf4j.org/codes.html#null_MDCA	org/slf4j/MDC.java
http://www.slf4j.org/codes.html	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#loggerNameMismatch	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#multiple_bindings	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#StaticLoggerBinder	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#null_LF	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#replay	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#substituteLogger	org/slf4j/LoggerFactory.java

URL信息	Url所在文件
http://www.slf4j.org/codes.html#unsuccessfulInit	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#version_mismatch	org/slf4j/LoggerFactory.java
https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection	org/java_websocket/AbstractWebSocket.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
https://a.apicloud.com	compile/Properties.java
https://d.apicloud.com	compile/Properties.java
https://s.apicloud.com	compile/Properties.java
https://p.apicloud.com	compile/Properties.java
https://r.apicloud.com	compile/Properties.java
https://as.apicloud.com	compile/Properties.java

邮箱线索

邮箱地址	所在文件
123@app3c.com	com/uzmap/pkg/uzmodules/uzxml/UzXml.java
developer@apicloud.com	com/uzmap/pkg/uzcore/b/d.java

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
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。
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.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_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.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

向手机申请的权限	是否危险	类型	详细情况
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.READ_INTERNAL_STORAGE	未知	Unknown permission	Unknown permission from android reference
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
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_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_MEDIA_STORAGE	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
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.RUN_INSTRUMENTATION	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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=(zh), ST=(Beijing), L=(Beijing), O=(dyy@qiaomeng.net), OU=(dyy@qiaomeng.net), CN=(dyy@qiaomeng.net)
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-12-21 03:01:42+00:00
Valid To: 2119-11-27 03:01:42+00:00
Issuer: C=(zh), ST=(Beijing), L=(Beijing), O=(dyy@qiaomeng.net), OU=(dyy@qiaomeng.net), CN=(dyy@qiaomeng.net)
Serial Number: 0x1c2949e8

Hash Algorithm: sha256
md5: fe3a9aebdbc5b68165fb76701b29d79d
sha1: d25b12182c6efd68afb08bb0ff69de25a74cc997
sha256: 8959df664045217c455b42d91a9e3211b9831f838111f91a55ec63e240cf378a
sha512: df1db5402dc7f902013062c83ef14841b3ce3e89a8a46bd8b70286319976b17175c058d521333c05a49f1b7c132177a654bb3c46d08d6c8b0d79342a1f4813e9
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: c5754d35d14e280e858f98fd9947639e85aa7df0249422ffa5d74d7cc668e366

硬编码敏感信息

可能的敏感信息
"ali_auth_sms_veri_title" : "请输入 %s 收到的验证码"
"ali_auth_verification_reGetCode" : "重新获取验证码"
"aliusersdk_api_unauthorized" : "API未授权"
"com_alibc_auth_actiivty_auth_ok" : "确认授权"
"com_alibc_auth_actiivty_cancel" : "取消"
"com_alibc_auth_actiivty_get" : "获取"
"com_taobao_tae_sdk_authorize_title" : "登录授权"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.alibaba.baichuan.android.trade.ui.AlibcBackActivity	Schemes: alisdk://,

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 编译器 / dx
classes10.dex	壳列表 / 详细情况 编译器 / dx
classes11.dex	壳列表 / 详细情况 编译器 / dx
classes12.dex	壳列表 / 详细情况 编译器 / dx

文件列表	分析结果
classes13.dex	壳列表 | 详细情况 编译器 | dx
classes14.dex	壳列表 | 详细情况 编译器 | dx
classes15.dex	壳列表 | 详细情况 编译器 | dx
classes16.dex	壳列表 | 详细情况 编译器 | dx
classes17.dex	壳列表 | 详细情况 编译器 | dx

文件列表	分析结果
classes18.dex	壳列表 / 详细情况 编译器 / dx
classes19.dex	壳列表 / 详细情况 编译器 / dx
classes2.dex	壳列表 / 详细情况 编译器 / dx
classes20.dex	壳列表 / 详细情况 编译器 / dx
classes21.dex	壳列表 / 详细情况 编译器 / dx

文件列表	分析结果
classes22.dex	壳列表 / 详细情况 编译器 / dx
classes23.dex	壳列表 / 详细情况 编译器 / dx
classes24.dex	壳列表 / 详细情况 编译器 / dx
classes25.dex	壳列表 / 详细情况 编译器 / dx
classes26.dex	壳列表 / 详细情况 编译器 / dx

文件列表	分析结果
classes27.dex	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table>

文件列表	分析结果
classes28.dex	壳列表 / 详细情况 反虚拟机：Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check device ID check subscriber ID check ro.product.device check ro.kernel.qemu check emulator file check 编译器：dx

文件列表	分析结果
classes29.dex	壳列表 / 详细情况 编译器 / dx
classes3.dex	壳列表 / 详细情况 编译器 / dx
classes30.dex	壳列表 / 详细情况 编译器 / dx
classes31.dex	壳列表 / 详细情况 编译器 / dx
classes32.dex	壳列表 / 详细情况 编译器 / dx

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes33.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
<tr><td>classes34.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
<tr><td>classes35.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
<tr><td>classes36.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
<tr><td>classes37.dex</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>Build.MANUFACTURER check</td></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
</table>

文件列表	分析结果
classes38.dex	壳列表 详细情况 编译器 dx
classes39.dex	壳列表 详细情况 编译器 dx
classes4.dex	壳列表 详细情况 编译器 dx
classes40.dex	壳列表 详细情况 编译器 dx
classes41.dex	壳列表 详细情况 编译器 dx

文件列表	分析结果
classes42.dex	壳列表 | 详细情况 编译器 | dx
classes43.dex	壳列表 | 详细情况 编译器 | dx
classes44.dex	壳列表 | 详细情况 编译器 | dx
classes45.dex	壳列表 | 详细情况 编译器 | dx
classes46.dex	壳列表 | 详细情况 编译器 | dx

文件列表	分析结果
classes47.dex	壳列表 / 详细情况 编译器 / dx
classes48.dex	壳列表 / 详细情况 编译器 / dx
classes5.dex	壳列表 / 详细情况 编译器 / dx
classes6.dex	壳列表 / 详细情况 编译器 / dx

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
possible Build.SERIAL check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>classes8.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>classes9.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi/libsgavmp.so!classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>lib/armeabi/libsgmain.so!classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>subscriber ID check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi/libsgsecuritybody.so!classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi/libsgsgmiddletier.so!classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
