MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

办公软件office 1.3.APK

APP名称:	办公软件office
包名:	com.bgrj.office.software
域名线索:	32条
URL线索:	37条
邮箱线索:	0条

分析日期: 2022年2月2日 17:06

文件信息

文件名: bgrjoffice562237.apk
文件大小: 9.11MB
MD5值: 899f85a4224f844b4b07b967d8c4b832
SHA1值: 51eb839b523c3023d9f37c09261ef53b77398b6b
SHA256值: e216e5759d34b31588c0dfdc16573bdc8610405f813c4fd99fa7d71aa1f0746a

APP 信息

App名称: 办公软件office
包名: com.bgrj.office.software
主活动Activity: com.bgrj.office.software.activity.LauncherActivity
安卓版本名称: 1.3
安卓版本: 13

域名线索

域名	是否危险域名	服务器信息
api.weixin.qq.com	good	**IP:** 81.69.216.43 **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
ichannel.snssdk.com	good	**IP:** 101.26.39.229 **所属国家:** China **地区:** Hebei **城市:** Handan **纬度:** 36.600559 **经度:** 114.467781 **查看地图:** Google Map
sf6-ttcdn-tos.pstatp.com	good	**IP:** 106.38.176.115 **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
toblog.ctobsnssdk.com	good	**IP:** 221.195.241.101 **所属国家:** China **地区:** Hebei **城市:** Cangzhou **纬度:** 38.316669 **经度:** 116.866669 **查看地图:** Google Map
errlog.umeng.com	good	**IP:** 106.8.130.60 **所属国家:** China **地区:** Hebei **城市:** Zhangjiakou **纬度:** 40.810001 **经度:** 114.879440 **查看地图:** Google Map
is.snssdk.com	good	**IP:** 42.81.156.229 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看地图:** Google Map
pangolin.snssdk.com	good	**IP:** 140.249.89.228 **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
rtlog.snssdk.com	good	**IP:** 58.58.80.174 **所属国家:** China **地区:** Shandong **城市:** Yantai **纬度:** 37.533329 **经度:** 121.400002 **查看地图:** Google Map

域名	是否危险域名	服务器信息
api.mycat.sousui.cn	good	**IP:** 116.62.64.143 **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
rtapplog.snssdk.com	good	**IP:** 125.39.135.220 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看地图:** Google Map
www.baidu.com	good	**IP:** 110.242.68.4 **所属国家:** China **地区:** Hebei **城市:** Baoding **纬度:** 38.851109 **经度:** 115.490280 **查看地图:** Google Map
i.snssdk.com	good	**IP:** 27.128.147.239 **所属国家:** China **地区:** Hebei **城市:** Shijiazhuang **纬度:** 38.041389 **经度:** 114.478607 **查看地图:** Google Map
api.mch.weixin.qq.com	good	**IP:** 182.254.50.109 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
sf3-ttcdn-tos.pstatp.com	good	**IP:** 36.102.10.239 **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
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

域名	是否危险域名	服务器信息
applog.snssdk.com	good	**IP:** 125.39.135.218 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看地图:** Google Map
sf1-ttcdn-tos.pstatp.com	good	**IP:** 42.81.213.226 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看地图:** Google Map
pangolin16.snssdk.com	good	没有服务器地理信息.
errlogos.umeng.com	good	**IP:** 47.246.110.18 **所属国家:** Hong Kong **地区:** Hong Kong **城市:** Hong Kong **纬度:** 22.285521 **经度:** 114.157692 **查看地图:** Google Map
p3-tt.byteimg.com	good	**IP:** 36.102.10.239 **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
image.cnamedomain.com	good	没有服务器地理信息.
api-access.pangolin-sdk-toutiao.com	good	**IP:** 140.249.88.207 **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

域名	是否危险域名	服务器信息
log.snssdk.com	good	**IP:** 27.185.6.213 **所属国家:** China **地区:** Hebei **城市:** Shijiazhuang **纬度:** 38.041389 **经度:** 114.478607 **查看地图:** Google Map
runduoconfig.oss-cn-hangzhou.aliyuncs.com	good	**IP:** 47.110.23.244 **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-cn-.aliyuncs.comor	good	没有服务器地理信息.
tobapplog.ctobsnssdk.com	good	**IP:** 125.39.135.221 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看地图:** Google Map
oss-cn-hangzhou.aliyuncs.com	good	**IP:** 118.31.219.251 **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
www.chengzijianzhan.com	good	**IP:** 140.249.88.200 **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
aiapi.jd.com	good	**IP:** 116.196.123.78 **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
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
success.ctobsnssdk.com	good	**IP:** 119.96.137.225 **所属国家:** China **地区:** Hubei **城市:** Wuhan **纬度:** 30.583330 **经度:** 114.266670 **查看地图:** Google Map

URL线索

URL信息
https://errlog.umeng.com/api/crashsdk/logcollect
https://errlogos.umeng.com/api/crashsdk/logcollect
https://errlog.umeng.com/api/crashsdk/logcollect
http://127.0.0.1:
https://pangolin.snssdk.com
https://is.snssdk.com
https://pangolin16.snssdk.com
https://api-access.pangolin-sdk-toutiao.com
http://p3-tt.byteimg.com/img/web.business.image/201907245d0d495a0568785742e0b940~100x100.image
http://sf3-ttcdn-tos.pstatp.com/obj/mosaic-legacy/2b96e0005c6b6019f8a5b
https://www.chengzijianzhan.com/tetris/page/1639938884171780/? ad_id=1639940885031987&_toutiao_params=%7B%22cid%22%3A1639941324071955%2C%22device_id%22%3A38167681029%2C%22log_extra%22%3A%22%7B%5C%22ad_price%5C%22%3A%5C%22XThCVgADKYpdOEJWAAMpijdExKKDLYCp1GNXWw%5C%22%2C%5C%22c bf4b-4ff8-be68-9149e288a420u6714%5C%22%2C%5C%22rit%5C%22%3A901121375%7D%22%2C%22orit%22%3A900000000%2C%22req_id%22%3A%220781feb2-bf4b-4ff8-be68-9149e288a420u6714%22%2C%22rit%22%3A901121375%2C%22sign%22%3A%22D41D8CD98F
http://sf3-ttcdn-tos.pstatp.com/img/mosaic-legacy/2b96e0005c6b6019f8a5b~noop.jpg
https://sf1-ttcdn-tos.pstatp.com/obj/union-fe/playable/97699c8fb31e7836e828cffdd428bc80/index.html?toutiao_card_params=%7B%22name%22%3A%20%22%5Cu5168%5Cu6c11%5Cu6f02%5Cu79fb- 3D%5Cu98d9%5Cu8f66%22%2C%20%22pkg_name%22%3A%20%22com.joyfort.merge.car%22%2C%20%22id%22%3A%2016392999793285l6%2C%20%22download_url%22%3A%20%22https%3A//itunes.apple.com/cn/app/%25E5%2585%25A8%25E6%25B0%2591%25E6%2
http://sf1-ttcdn-tos.pstatp.com/obj/ttfe/adfe/union_endcard/union_test_tool.mp4

URL信息
http://sf1-ttcdn-tos.pstatp.com/obj/ttfe/adfe/union_endcard/Lark20190725-175511.png
https://i.snssdk.com/inspect/aegis/client/page/
http://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html
http://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html
https://sf3-ttcdn-tos.pstatp.com/obj/ad-pattern/renderer/package.json
https://log.snssdk.com/service/2/device_register_only/
https://ichannel.snssdk.com/service/2/app_alert_check/
https://log.snssdk.com/service/2/app_log/
https://applog.snssdk.com/service/2/app_log/
https://rtlog.snssdk.com/service/2/app_log/
https://rtapplog.snssdk.com/service/2/app_log/
https://log.snssdk.com/service/2/log_settings/
https://toblog.ctobsnssdk.com/service/2/device_register_only/
https://toblog.ctobsnssdk.com/service/2/app_alert_check/
https://toblog.ctobsnssdk.com/service/2/app_log/
https://tobapplog.ctobsnssdk.com/service/2/app_log/
https://toblog.ctobsnssdk.com/service/2/log_settings/
https://toblog.ctobsnssdk.com/service/2/abtest_config/
https://success.ctobsnssdk.com/service/2/app_log/
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://api.mycat.sousui.cn/v1/goods/lists?categoryId=3&endGold=0&goodsColor=&num=20&order=recommendTime&search=&startGold=0
https://runduoconfig.oss-cn-hangzhou.aliyuncs.com/kefu_qq.json?OSSAccessKeyId=LTAI4FpaXVGm2tWR41f2NGau&Expires=360001622528447&Signature=B2SBaecympEPmmC5KOJ79Es7Df8%3D
https://aiapi.jd.com/jdai/general_ocr?appkey=ca8d834ea33e4cba72ea4b449d567cf0&timestamp=
https://api.mycat.sousui.cn/v1/down/addr
https://www.baidu.com/
https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code

URL信息
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s&lang=zh_CN
https://api.mch.weixin.qq.com/pay/unifiedorder
https://ip.
http://oss-cn-****.aliyuncs.com',or
http://image.cnamedomain.com'!
http://oss.aliyuncs.com
http://127.0.0.1
http://oss-cn-****.aliyuncs.com',or
http://image.cnamedomain.com'!
http://oss-cn-hangzhou.aliyuncs.com
https://errlog.umeng.com/api/crashsdk/logcollect
https://errlogos.umeng.com/api/crashsdk/logcollect
https://errlog.umeng.com
https://errlogos.umeng.com

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.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_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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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

向手机申请的权限	是否危险	类型	详细情况
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
com.bgrj.office.software.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=cn, ST=cs, L=cs, O=quexin, OU=quexin, CN=quexin
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-06-11 06:38:56+00:00
Valid To: 2128-03-22 06:38:56+00:00
Issuer: C=cn, ST=cs, L=cs, O=quexin, OU=quexin, CN=quexin
Serial Number: 0x6f7ea82b
Hash Algorithm: sha256
md5: 358f5d8c21f2cb079d313072528b1ef0
sha1: 1f532dfbc79b2cb44b78f0058b69deb0b166ffaa
sha256: a6ebe3b95b66b88a65581ee5821c051813763703ab93f7393ecffee248d16c21
sha512: af8dd73266ff7572686d424aac22d46d15f9f48032a40409136b5e09cb0696c490dc9064bba94a58ae709f37ab55fe66d26ec65cffa3cf9529b5d3a77dc0498a
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 65e6d410f047973152c5aab36fd7333eb0b2f321fefef1377cf3bac147984aed

Exodus威胁情报

名称	分类	URL链接
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

加壳分析

文件列表	分析结果

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>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>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
SIM operator check
network operator name check
subscriber ID check
network interface name check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>