MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

蝴蝶鱼快讯 1.0.0.APK

APP名称:	蝴蝶鱼快讯
包名:	com.iyoyi.news.hudieyukx
域名线索:	71条
URL线索:	66条
邮箱线索:	1条
分析日期:	2022年2月2日 11:50

文件信息

文件名: hdykx.apk
文件大小: 9.88MB
MD5值: 67205f218367486a54805a28deb6b32c
SHA1值: 6195e4ab88a1049f173af9bc09b704751d8b6876
SHA256值: d0e6543db26ee7691fc49ebccc4d0a68557e02a787602a6b702eaf1bf9502825

APP 信息

App名称: 蝴蝶鱼快讯
包名: com.iyoyi.news.hudieyukx
主活动**Activity:** com.iyoyi.prototype.ui.activity.SplashActivity
安卓版本名称: 1.0.0
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
mobile.umeng.com	good	**IP:** 59.82.31.209 **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
astat.bugly.qcloud.com	good	**IP:** 150.109.29.135 **所属国家:** Korea (Republic of) **地区:** Seoul-teukbyeolsi **城市:** Seoul **纬度:** 37.568260 **经度:** 126.977829 **查看地图:** Google Map
debugtbs.qq.com	good	**IP:** 175.27.9.46 **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
soft.tbs.imtt.qq.com	good	**IP:** 121.51.175.84 **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
appapi.ncrte5.cn	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
100.69.168.33	good	**IP:** 100.69.168.33 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map
register.xmpush.global.xiaomi.com	good	**IP:** 47.88.199.5 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
up4.ucweb.com	good	**IP:** 111.62.164.93 **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
upload.ffmpeg.org	good	**IP:** 213.36.253.119 **所属国家:** France **地区:** Ile-de-France **城市:** Paris **纬度:** 48.853409 **经度:** 2.348800 **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
cfg.imtt.qq.com	good	**IP:** 121.51.158.70 **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
www.jivesoftware.com	good	**IP:** 35.238.7.255 **所属国家:** United States of America **地区:** Iowa **城市:** Council Bluffs **纬度:** 41.261940 **经度:** -95.860832 **查看地图:** Google Map
adash.man.aliyuncs.com	good	**IP:** 59.82.40.77 **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
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
172.16.0.12	good	**IP:** 172.16.0.12 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map
cmnsguider.yunos.com	good	**IP:** 203.119.169.141 **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
gjapplog.ucweb.com	good	**IP:** 168.235.204.12 **所属国家:** United States of America **地区:** California **城市:** Monrovia **纬度:** 34.142773 **经度:** -117.999565 **查看地图:** Google Map

域名	是否危险域名	服务器信息
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
ccc.sys.miui.com	good	**IP:** 120.133.33.125 **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
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
mqqad.html5.qq.com	good	**IP:** 0.0.0.1 **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
wpk-auth.ucweb.com	good	**IP:** 120.241.2.239 **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
plbslog.umeng.com	good	**IP:** 59.82.66.230 **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
applog.uc.cn	good	**IP:** 111.62.115.33 **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
norma-external-collect.meizu.com	good	**IP:** 113.106.27.98 **所属国家:** China **地区:** Guangdong **城市:** Zhongshan **纬度:** 22.520580 **经度:** 113.382317 **查看地图:** Google Map

域名	是否危险域名	服务器信息
ulogs.umeng.com	good	**IP:** 203.119.174.133 **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
idmb.register.xmpush.global.xiaomi.com	good	**IP:** 3.109.136.30 **所属国家:** United States of America **地区:** Washington **城市:** Seattle **纬度:** 47.627499 **经度:** -122.346199 **查看地图:** Google Map
alog.umengcloud.com	good	**IP:** 106.11.86.69 **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
developer.umeng.com	good	**IP:** 59.82.60.43 **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
long.open.weixin.qq.com	good	**IP:** 109.244.216.15 **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
appapi.wz12356.com	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
www.umeng.com	good	**IP:** 59.82.60.43 **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
alog.umeng.com	good	**IP:** 106.11.86.78 **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
api-push.in.meizu.com	good	**IP:** 206.161.233.191 **所属国家:** United States of America **地区:** Virginia **城市:** Herndon **纬度:** 38.978210 **经度:** -77.386993 **查看地图:** Google Map
adash.m.taobao.com	good	**IP:** 59.82.39.14 **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
agoodm.wapa.taobao.com	good	没有服务器地理信息.
c-adash.m.taobao.com	good	**IP:** 59.82.39.13 **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
openmobile.qq.com	good	**IP:** 113.96.208.233 **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
mdc.html5.qq.com	good	**IP:** 175.27.9.46 **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
metok.sys.miui.com	good	**IP:** 124.251.100.14 **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
log.tbs.qq.com	good	**IP:** 109.244.244.37 **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
uop.umeng.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
wup.imtt.qq.com	good	**IP:** 182.254.57.56 **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
api.xmpush.xiaomi.com	good	**IP:** 117.48.116.220 **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
log.umsns.com	good	**IP:** 59.82.29.162 **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
ru.register.xmpush.global.xiaomi.com	good	**IP:** 107.155.52.56 **所属国家:** Russian Federation **地区:** Moskva **城市:** Moscow **纬度:** 55.752220 **经度:** 37.615559 **查看地图:** Google Map

域名	是否危险域名	服务器信息
agoodm.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
dsappapi.415003.com	good	**IP:** 42.192.208.30 **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
resolver.msg.xiaomi.net	good	**IP:** 120.92.96.13 **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
100.69.165.28	good	**IP:** 100.69.165.28 **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
graph.qq.com	good	**IP:** 113.96.208.232 **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
api-push.meizu.com	good	**IP:** 125.94.213.129 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000 **查看地图:** Google Map
fr.register.xmpush.global.xiaomi.com	good	**IP:** 18.185.221.188 **所属国家:** Germany **地区:** Hessen **城市:** Frankfurt am Main **纬度:** 50.115520 **经度:** 8.684170 **查看地图:** Google Map
android.myapp.com	good	**IP:** 109.244.244.91 **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
www.qq.com	good	**IP:** 175.27.8.138 **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
aexception.bugly.qq.com	good	**IP:** 101.226.233.161 **所属国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.222219 **经度:** 121.458061 **查看地图:** Google Map
pms.mb.qq.com	good	**IP:** 121.51.158.70 **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
rqd.uu.qq.com	good	**IP:** 182.254.88.184 **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

域名	是否危险域名	服务器信息
cn.register.xmpush.xiaomi.com	good	**IP:** 203.100.92.32 **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
ouplog.umeng.com	good	**IP:** 47.74.172.218 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
agapiv3.iju.cn	good	**IP:** 42.192.208.30 **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
hbapi.ncrte5.cn	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
android.bugly.qq.com	good	**IP:** 109.244.244.137 **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
alogsus.umeng.com	good	**IP:** 106.11.86.78 **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
allapp.iju.cn	good	**IP:** 49.235.3.99 **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
up4-intl.ucweb.com	good	**IP:** 157.185.188.1 **所属国家:** United States of America **地区:** California **城市:** Monrovia **纬度:** 34.142773 **经度:** -117.999565 **查看地图:** Google Map

域名	是否危险域名	服务器信息
ulogs.umengcloud.com	good	**IP:** 59.82.29.246 **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
debugx5.qq.com	good	**IP:** 175.27.9.46 **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
alogus.umeng.com	good	**IP:** 203.119.174.133 **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
woodpecker.uc.cn	good	**IP:** 111.62.164.93 **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

URL线索

URL信息	Url所在文件
https://developer.umeng.com/docs/66632/detail/	com/umeng/b/b/g.java
https://ulogs.umeng.com/unify_logs	com/umeng/b/h/d.java
https://ulogs.umengcloud.com/unify_logs	com/umeng/b/h/d.java
https://alogus.umeng.com/unify_logs	com/umeng/b/h/d.java
https://alogsus.umeng.com/unify_logs	com/umeng/b/h/d.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/b/h/b/u.java
https://plbslog.umeng.com	com/umeng/b/g/b.java
https://ouplog.umeng.com	com/umeng/b/g/b.java
http://alog.umeng.com/app_logs	com/umeng/a/d.java
http://alog.umengcloud.com/app_logs	com/umeng/a/d.java
https://uop.umeng.com	com/umeng/a/d.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/a/b/o.java
http://log.umsns.com/	com/umeng/a/c/f.java
http://log.umsns.com/share/api/	com/umeng/a/c/f.java

URL信息	Url所在文件
http://log.umsns.com/share/api/	com/umeng/a/c/g.java
https://api.weixin.qq.com/sns/auth?access_token=	com/umeng/socialize/media/j.java
https://mobile.umeng.com/images/pic/home/social/img-1.png	com/umeng/socialize/net/d.java
https://log.umsns.com/	com/umeng/socialize/net/b/b.java
http://www.umeng.com/social	com/umeng/socialize/d/c.java
https://log.umsns.com/	com/umeng/socialize/d/c.java
https://log.umsns.com/link/qq/download/	com/umeng/socialize/d/c.java
https://log.umsns.com/link/weixin/download/	com/umeng/socialize/d/c.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/socialize/utils/l.java
https://api.weixin.qq.com/sns/oauth2/access_token?	com/umeng/socialize/handler/UMWXHandler.java
https://api.weixin.qq.com/sns/oauth2/refresh_token?	com/umeng/socialize/handler/UMWXHandler.java
https://api.weixin.qq.com/sns/userinfo?access_token=	com/umeng/socialize/handler/UMWXHandler.java
http://log.umsns.com/link/weixin/download/	com/umeng/socialize/handler/UMWXHandler.java
https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=	com/umeng/socialize/handler/UMWXHandler.java
https://log.umsns.com/	com/umeng/socialize/g/b.java

URL信息	Url所在文件
https://graph.qq.com/oauth2.0/me?access_token=	com/umeng/qq/handler/UmengQQHandler.java
http://log.umsns.com/link/qq/download/	com/umeng/qq/handler/UmengQQHandler.java
https://openmobile.qq.com/user/get_simple_userinfo?status_os=	com/umeng/qq/handler/UmengQQHandler.java
http://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/CrashReport.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://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
http://aexception.bugly.qq.com:8012/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
http://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugtbs.qq.com?10000	com/tencent/smtt/sdk/WebView.java
www.qq.com	com/tencent/smtt/sdk/i.java
http://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/i.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/b/a/a.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/b/a/a.java

URL信息	Url所在文件
http://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/a/c.java
http://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
http://wup.imtt.qq.com:8080	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
http://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.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://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties	com/liulishuo/filedownloader/services/a.java
http://100.69.165.28/agoo/report	com/taobao/accs/b/a.java
http://agoodm.m.taobao.com/agoo/report	com/taobao/accs/b/a.java

URL信息	Url所在文件
http://agoodm.wapa.taobao.com/agoo/report	com/taobao/accs/b/a.java
http://100.69.168.33/agoo/report	com/taobao/accs/b/a.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/b/a/e.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/b/a/a.java
https://api-push.meizu.com	com/meizu/cloud/pushsdk/b/c/e.java
https://api-push.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/a/a.java
https://api-push.in.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/a/a.java
http://norma-external-collect.meizu.com/push/android/external/add.do	com/meizu/cloud/pushsdk/a/a/b.java
http://norma-external-collect.meizu.com/android/exchange/getpublickey.do	com/meizu/cloud/pushsdk/a/a/a.java
https://api-push.meizu.com/garcia/api/server/getPublicKey	com/meizu/cloud/pushsdk/handler/a/a.java
http://agapiv3.iju.cn/APIAppGeneraliz/App	com/iyoyi/prototype/c.java
http://appapi.ncrte5.cn/	com/iyoyi/prototype/h/c.java
http://hbapi.ncrte5.cn/	com/iyoyi/prototype/h/c.java
http://dsappapi.415003.com/update/getInfo	com/iyoyi/prototype/h/c.java
http://appapi.wz12356.com/global/actiontest?type=popRedpack	com/iyoyi/prototype/e/b/a/b.java

URL信息	Url所在文件
http://appapi.wz12356.com/global/actiontest?type=adRedpack	com/iyoyi/prototype/e/b/a/b.java
https://allapp.iju.cn/base/init?id=%s&os=%d	com/iyoyi/prototype/g/d.java
http://android.myapp.com/myapp/detail.htm?apkName=com.yooee.headline#CommentList	com/iyoyi/library/d/m.java
http://172.16.0.12:8888/emulator/index.html	com/iyoyi/jsbridge/a.java
http://%1$s/gslb/?ver=4.0	com/xiaomi/push/ds.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/hm.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/gk.java
https://metok.sys.miui.com	com/xiaomi/push/bl.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/gu.java
http://ccc.sys.miui.com	com/xiaomi/push/br.java
http://www.jivesoftware.com/xmlns/xmpp/properties	com/xiaomi/push/hf.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/hn.java
http://resolver.msg.xiaomi.net/psc/?t=a	com/xiaomi/push/service/bb.java
www.baidu.com:80	com/xiaomi/push/service/ad.java
https://cn.register.xmpush.xiaomi.com	com/xiaomi/push/service/l.java

URL信息	Url所在文件
https://register.xmpush.global.xiaomi.com	com/xiaomi/push/service/l.java
https://fr.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/l.java
https://ru.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/l.java
https://idmb.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/l.java
https://api.xmpush.xiaomi.com/upload/xmsf_log?file=	com/xiaomi/mipush/sdk/w.java
https://api.xmpush.xiaomi.com/upload/app_log?file=	com/xiaomi/mipush/sdk/w.java
https://api.xmpush.xiaomi.com/upload/crash_log?file=	com/xiaomi/mipush/sdk/y.java
https://up4-intl.ucweb.com/upload	com/uc/crashsdk/e.java
https://up4.ucweb.com/upload	com/uc/crashsdk/e.java
https://applog.uc.cn/collect	com/uc/crashsdk/a/h.java
https://gjapplog.ucweb.com/collect	com/uc/crashsdk/a/h.java
https://woodpecker.uc.cn	com/uc/crashsdk/a/d.java
https://wpk-auth.ucweb.com	com/uc/crashsdk/a/d.java
https://adash.man.aliyuncs.com/man/api?ak=23356390&s=	com/alibaba/sdk/android/utils/AMSDevReporter.java
http://adash.m.taobao.com/rest/abtest	com/alibaba/motu/tbrest/rest/RestConstants.java

URL信息	Url所在文件
http://c-adash.m.taobao.com/rest/gc	com/alibaba/motu/tbrest/rest/RestConstants.java
http://adash.m.taobao.com/rest/sur	com/alibaba/motu/tbrest/rest/RestConstants.java
https://github.com/vinc3m1	Android String Resource
https://github.com/vinc3m1/RoundedImageView	Android String Resource
https://github.com/vinc3m1/RoundedImageView.git	Android String Resource
ftp://upload.ffmpeg.org/incoming/	lib/armeabi-v7a/libijkplayer.so
https://applog.uc.cn/collect	lib/armeabi-v7a/libcrashsdk.so
https://gjapplog.ucweb.com/collect	lib/armeabi-v7a/libcrashsdk.so
https://woodpecker.uc.cn	lib/armeabi-v7a/libcrashsdk.so
https://wpk-auth.ucweb.com	lib/armeabi-v7a/libcrashsdk.so

邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

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
com.iyoyi.puppet.command	未知	Unknown permission	Unknown permission from android reference
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.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.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_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.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.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.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.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.ACCESS_DOWNLOAD_MANAGER	未知	Unknown permission	Unknown permission from android reference
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
android.permission.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
android.permission.EXPAND_STATUS_BAR	正常	展开/折叠状态栏	允许应用程序展开或折叠状态栏
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.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.READ_SETTINGS	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

向手机申请的权限	是否危险	类型	详细情况
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.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_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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.iyoyi.news.hudieyukx.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.iyoyi.news.hudieyukx.permission.C2D_MESSAGE	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
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.iyoyi.news.hudieyukx.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-04-09 07:53:00+00:00
Valid To: 2020-07-08 07:53:00+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Serial Number: 0x6a84030b
Hash Algorithm: sha256
md5: ada1f5d2532d94ca409081d4898cff17
sha1: b94a84f32ed43e606cf119e6593ddcce98f6cc7f
sha256: c564895901cca178310d4e248b83415207f132f32e9eff64fc1d31aec4ca0720

sha512: 1b7a622c184e69f20628c7237571cf748ebbb0e66d5268ad73912f4beac2e1b77d61c6a65d60daf8d5adfd3d0570a90687bc9e02a0ef13a26ee950c2ad656a5e

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

硬编码敏感信息

可能的敏感信息
"fragment_modify_pwd_filed_label1" : "旧密码"
"fragment_modify_pwd_filed_label2" : "新密码"
"fragment_modify_pwd_success" : "修改成功，请重新登录"
"fragment_modify_pwd_title" : "修改密码"
"fragment_oauth_mobile" : "手机号登录"
"fragment_reset_pwd_filed_label1" : "手机号"
"fragment_reset_pwd_filed_label2" : "验证码"
"fragment_reset_pwd_filed_label3" : "新密码"

可能的敏感信息
"fragment_reset_pwd_filed_label4" : "确认新密码"
"fragment_reset_pwd_get_verify_code" : "点击获取"
"fragment_reset_pwd_success" : "重设密码成功，请登录"
"fragment_reset_pwd_title" : "重设密码"
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"need_password" : "请输入密码"
"pref_key_enable_background_play" : "pref.enable_background_play"
"pref_key_enable_no_view" : "pref.enable_no_view"
"pref_key_enable_surface_view" : "pref.enable_surface_view"
"pref_key_last_directory" : ""
"pref_key_media_codec_handle_resolution_change" : "pref.media_codec_handle_resolution_change"
"pref_key_pixel_format" : "pref.pixel_format"
"pref_key_player" : "pref.player"
"pref_key_using_media_codec" : "pref.using_media_codec"

可能的敏感信息
"pref_key_using_media_codec_auto_rotate" : "pref.using_media_codec_auto_rotate"
"pref_key_using_mediadatasource" : "pref.using_mediadatasource"
"pref_key_using_opensl_es" : "pref.using_opensl_es"
"warning_oauth_failed" : "授权失败"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.iyoyi.prototype.ui.activity.MainActivity	Schemes: hdykx://, hdykx.xg.push://, Hosts: return_app,
com.tencent.tauth.AuthActivity	Schemes: tencent1106331557://,

加壳分析

文件列表	分析结果

文件列表	分析结果
classes.dex	<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 ro.kernel.qemu check possible ro.secure check emulator file check possible VM check</td></tr><tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr></table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes2.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</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
