MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

白杏云 1.0.0.APK

APP名称:	白杏云
包名:	com.baix.yun
域名线索:	23条
URL线索:	29条
邮箱线索:	2条
分析日期:	2022年1月28日 21:59

文件信息

文件名: baixingyun.apk
文件大小: 9.88MB
MD5值: 929e194c8fa57b35f654a9c6694559a0
SHA1值: af27ca989206c4970bd348138ec5c468aae6dd46
SHA256值: da461a4bc5679dc5124f372d2785f2b73797a20ae42815698efced1cc6cc5011

APP 信息

App名称: 白杏云
包名: com.baix.yun
主活动**Activity:** com.baix.yun.view.main.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
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

域名	是否危险域名	服务器信息
playready.directtaps.net	good	**IP:** 40.70.71.156 所属国家: United States of America 地区: Virginia 城市: Boydton 纬度: 36.667641 经度: -78.387497 查看地图: Google Map
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
schemas.microsoft.com	good	**IP:** 23.73.226.14 所属国家: United States of America 地区: New Jersey 城市: Edison 纬度: 40.518719 经度: -74.412102 查看地图: Google Map
api.newcloud.ztao.top	good	没有服务器地理信息.
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

域名	是否危险域名	服务器信息
www.openssl.org	good	**IP:** 184.27.21.43 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map
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
www.qiniu.com	good	**IP:** 118.182.230.56 所属国家: China 地区: Gansu 城市: Wuwei 纬度: 37.928055 经度: 102.641388 查看地图: Google Map
open.weixin.qq.com	good	**IP:** 175.24.219.72 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:** 140.249.89.232 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
render.alipay.com	good	**IP:** 150.138.144.196 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941 查看地图: Google Map
mobilegw.alipay.com	good	**IP:** 203.209.245.78 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
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
www.google.com	good	**IP:** 69.197.153.180 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.147839 经度: -94.568878 查看地图: Google Map
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
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
httpdns.qnydns.net	good	没有服务器地理信息.
loggw-exsdk.alipay.com	good	**IP:** 110.75.134.8 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

域名	是否危险域名	服务器信息
xml.apache.org	good	**IP:** 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map
www.baidu.com	good	**IP:** 110.242.68.3 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
pipeline.qiniu.com	good	**IP:** 180.97.147.247 所属国家: China 地区: Jiangsu 城市: Suzhou 纬度: 31.311390 经度: 120.618057 查看地图: Google Map
m.alipay.com	good	**IP:** 203.209.245.120 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

URL线索

URL信息	Url所在文件
www.baidu.com	com/blankj/utilcode/util/NetworkUtils.java
http://xml.apache.org/xslt}indent-amount	com/blankj/utilcode/util/LogUtils.java
http://api.newcloud.ztao.top/	com/baix/yun/constant/Constants.java
https://www.qiniu.com	com/qiniu/android/storage/GlobalConfiguration.java
https://www.baidu.com	com/qiniu/android/storage/GlobalConfiguration.java
https://www.google.com	com/qiniu/android/storage/GlobalConfiguration.java
https://pipeline.qiniu.com	com/qiniu/android/bigdata/Configuration.java
http://httpdns.qnydns.net:18302/	com/qiniu/android/dns/http/QiniuDns.java
https://httpdns.qnydns.net:18443/	com/qiniu/android/dns/http/QiniuDns.java
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.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

URL信息	Url所在文件
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://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache/HttpUrlSource.java
http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/Pinger.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
http://playready.directtaps.net/pr/svc/rightsmanager.asmx	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
ftp://upload.ffmpeg.org/incoming/	lib/armeabi-v7a/libijkplayer.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	com/danikula/videocache/HttpUrlSource.java
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
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_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_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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=SH
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-08-19 02:27:32+00:00
Valid To: 2046-08-13 02:27:32+00:00
Issuer: CN=SH
Serial Number: 0x40e2435b
Hash Algorithm: sha256
md5: 68371007188f3fda5d7b90e04b819d4f
sha1: 742d6f812723f88ac341c77bf19cb19ead34cdc9
sha256: 28653439abe6a722687ff6ec14a249844dc7a3046ae63bff0563e416d762a8dc
sha512: c5a97b15a3a3480aa931100ba1c8b5ac0ced61aee2cdabc2fcb9865f9bf30cc02c83a9ba93342f0e1a6c90b2e4bb56c03ad20e54d9e18070ef063f0f6d116baf
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: d559c4d484cf120b441d6044b6d3ae3df6f33f854747463de88f03d0c6f40113

加壳分析

<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
possible Build.SERIAL check
SIM operator check
network operator name check
device ID check
subscriber ID check
possible VM 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>
