MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

银元转 1.0.1.APK

APP名称:	银元转
包名:	com.xihe.yinyuanzhang
域名线索:	37条
URL线索:	43条
邮箱线索:	3条
分析日期:	2022年1月20日 22:18

文件信息

文件名: yinyuanzhuan.apk
文件大小: 16.57MB
MD5值: 13cf9a3573636816d8eeb7738212e54b
SHA1值: f443e1e3e1431a923125b3571833a08e9380a576
SHA256值: caaa3ebfe76cefad3c3d8e5dc1224b859a5ac04ef9f88b85eec43c23eaea43a6

APP 信息

App名称: 银元转
包名: com.xihe.yinyuanzhang
主活动**Activity:** com.xihe.bhz.ui.activity.SplashActivity
安卓版本名称: 1.0.1
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
mta.qq.com	good	**IP:** 111.161.14.94 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

域名	是否危险域名	服务器信息
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
img.zcool.cn	good	**IP:** 139.227.225.136 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
schemas.microsoft.com	good	**IP:** 184.29.179.44 所属国家: United States of America 地区: Georgia 城市: Atlanta 纬度: 33.749001 经度: -84.387978 查看地图: Google Map
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

域名	是否危险域名	服务器信息
mp.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
meiqia.com	good	**IP:** 203.107.63.12 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
pslog.umeng.com	good	**IP:** 59.82.31.160 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
weixin.sogou.com	good	**IP:** 49.7.176.60 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
alogus.umeng.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
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
7xjmzj.com1.z0.glb.clouddn.com	good	**IP:** 124.163.195.187 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.560280 查看地图: Google Map
ulogs.umengcloud.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

域名	是否危险域名	服务器信息
notify.bugsnag.com	good	**IP:** 35.186.205.6 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568 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
eco-api.meiqia.com	good	**IP:** 203.107.63.12 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
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

域名	是否危险域名	服务器信息
chky.oss-cn-hangzhou.aliyuncs.com	good	**IP:** 47.110.177.41 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
cmnsguider.yunos.com	good	**IP:** 203.119.169.224 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
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
azhong.tk	good	没有服务器地理信息.
errlog.umeng.com	good	**IP:** 111.225.159.19 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

域名	是否危险域名	服务器信息
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
oversea.goodday666.com	good	**IP:** 123.58.198.126 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
pingma.qq.com	good	**IP:** 119.45.78.184 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
eco-api-upload.meiqia.com	good	**IP:** 203.107.43.76 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
ucc.umeng.com	good	**IP:** 203.119.169.41 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
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
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
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
plbslog.umeng.com	good	**IP:** 59.82.43.171 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
ns.adobe.com	good	没有服务器地理信息.
alogsus.umeng.com	good	**IP:** 106.11.40.44 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:** 59.82.29.163 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
mta.oa.com	good	**IP:** 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690 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
new-api.meiqia.com	good	**IP:** 203.107.63.12 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
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://ulogs.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java

URL信息	Url所在文件
https://ulogs.umengcloud.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/v.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/w.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.java
https://ucc.umeng.com/v1/fetch	com/umeng/analytics/pro/ah.java
https://pslog.umeng.com/ablog	com/umeng/analytics/pro/ah.java
https://eco-api.meiqia.com/	com/meiqia/meiqiasdk/util/HttpUtils.java
https://new-api.meiqia.com/client/send_msg	com/meiqia/core/g.java
https://new-api.meiqia.com/knowledge/questions/	com/meiqia/core/g.java
https://new-api.meiqia.com/client/file_downloaded	com/meiqia/core/g.java
https://new-api.meiqia.com/client/tickets_v2/	com/meiqia/core/g.java
https://new-api.meiqia.com/client/msg_delivered	com/meiqia/core/g.java

URL信息	Url所在文件
https://new-api.meiqia.com/client/end_conversation	com/meiqia/core/g.java
https://new-api.meiqia.com/client/queue/position	com/meiqia/core/g.java
https://new-api.meiqia.com/client/tickets_v2/categories	com/meiqia/core/g.java
https://eco-api-upload.meiqia.com/upload?user_id=	com/meiqia/core/g.java
https://new-api.meiqia.com/upload/oss/policies	com/meiqia/core/g.java
https://new-api.meiqia.com/client/inputting	com/meiqia/core/g.java
https://new-api.meiqia.com/conversation/	com/meiqia/core/g.java
https://new-api.meiqia.com/sdk/init_sdk_user	com/meiqia/core/g.java
https://new-api.meiqia.com/client/device_token	com/meiqia/core/g.java
https://new-api.meiqia.com/sdk/statistics	com/meiqia/core/g.java
https://new-api.meiqia.com/client/forms	com/meiqia/core/g.java
https://new-api.meiqia.com/client/attrs	com/meiqia/core/g.java
https://new-api.meiqia.com/client/	com/meiqia/core/g.java
https://new-api.meiqia.com/scheduler	com/meiqia/core/g.java
https://new-api.meiqia.com/sdk/init	com/meiqia/core/g.java

URL信息	Url所在文件
https://new-api.meiqia.com/client/tickets_v2	com/meiqia/core/g.java
https://new-api.meiqia.com/client/tickets	com/meiqia/core/g.java
https://new-api.meiqia.com/client/msg_read	com/meiqia/core/g.java
https://new-api.meiqia.com/sdk/get_dev_client_id	com/meiqia/core/g.java
https://new-api.meiqia.com/sdk/refresh_push_info	com/meiqia/core/g.java
https://new-api.meiqia.com/client/client_events	com/meiqia/core/g.java
https://new-api.meiqia.com/client/send_msg	com/meiqia/core/d.java
https://notify.bugsnag.com	com/meiqia/core/a/e.java
http://meiqia.com/	com/meiqia/core/a/e.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

URL信息	Url所在文件
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
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
http://azhong.tk:8081/api/	com/azhon/appupdate/utils/HttpUtil.java
http://oversea.goodday666.com	com/xihe/bhz/net/api/URL.java
https://chky.oss-cn-hangzhou.aliyuncs.com/common/h5/pyq.html	com/xihe/bhz/ui/activity/TransmitMakeMoneyActivity.java
http://7xjmzj.com1.z0.glb.clouddn.com/20171026175005_JObCxCE2.mp4	com/xihe/bhz/ui/activity/SimpleDetailActivityMode2.java
https://weixin.sogou.com	com/xihe/bhz/ui/activity/UploadingActivity.java
https://mp.weixin.qq.com/	com/xihe/bhz/component/web/WebActivity.java
https://img.zcool.cn/community/013de756fb63036ac7257948747896.jpg	com/xihe/bhz/bean/DataBean.java
https://img.zcool.cn/community/01639a56fb62ff6ac725794891960d.jpg	com/xihe/bhz/bean/DataBean.java
https://img.zcool.cn/community/01270156fb62fd6ac72579485aa893.jpg	com/xihe/bhz/bean/DataBean.java
https://img.zcool.cn/community/01233056fb62fe32f875a9447400e1.jpg	com/xihe/bhz/bean/DataBean.java

URL信息	Url所在文件
https://img.zcool.cn/community/016a2256fb63006ac7257948f83349.jpg	com/xihe/bhz/bean/DataBean.java
https://api.weixin.qq.com/sns/oauth2/access_token	com/xihe/yinyuanzhang/wxapi/WXEntryActivity.java
https://api.weixin.qq.com/sns/userinfo?access_token=	com/xihe/yinyuanzhang/wxapi/WXEntryActivity.java
https://errlog.umeng.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://errlog.umeng.com	com/uc/crashsdk/a/d.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
ftp://upload.ffmpeg.org/incoming/	lib/armeabi-v7a/libijkplayer.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libimagepipeline.so
https://applog.uc.cn/collect	lib/armeabi-v7a/libcrashsdk.so
https://gjapplog.ucweb.com/collect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so

URL信息	Url所在文件
ftp://upload.ffmpeg.org/incoming/	lib/armeabi/libijkplayer.so
https://applog.uc.cn/collect	lib/armeabi/libcrashsdk.so
https://gjapplog.ucweb.com/collect	lib/armeabi/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi/libcrashsdk.so
http://www.openssl.org/support/faq.html	lib/armeabi/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
ffmpeg-devel@ffmpeg.org	lib/armeabi/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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.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。

向手机申请的权限	是否危险	类型	详细情况
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=lcd, ST=lcd, L=lcd, O=lcd, OU=lcd, CN=lcd
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-07-14 03:09:48+00:00
Valid To: 2048-11-29 03:09:48+00:00
Issuer: C=lcd, ST=lcd, L=lcd, O=lcd, OU=lcd, CN=lcd
Serial Number: 0x16416ffd
Hash Algorithm: sha256
md5: 34f8d8cb6be145d926f08a41cf97c166
sha1: 1243246a928c860e55e96b1e07421e807032c482
sha256: 40f9c969ec1734a0cd06e43946c869ed630ae5b0450335130c381b2c660486df
sha512: e0b7c5b5fdc18812b90fea74ef1740e8fefef021647564b5233dbeefddd568dfd9493a5c1cfba8067282ef0d45d86d78a0e200628655ea6408cae6653bb70e59
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c0cbf1e4edd4ba6d7db1a725d27a9bd8e2203c46132782a18d080cdfaf65b59e

Exodus威胁情报

名称	分类	URL链接
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

硬编码敏感信息

可能的敏感信息
"mq_auth_code" : "验证码"
"mq_auth_code" : "CAPTCHA"
"mq_auth_code" : "Kode verifikaso"
"mq_auth_code" : "Kod pengesahan"
"mq_auth_code" : "驗證碼"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.xihe.bhz.ui.activity.MainActivity	Schemes: v3b3re://,

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
Build.TAGS check
SIM operator check
network operator 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>反虚拟机</td><td>Build.MANUFACTURER 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>