MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

小贝网 1.40.APK

APP名称:	小贝网
包名:	com.share.share.beili
域名线索:	22条
URL线索:	19条
邮箱线索:	0条
分析日期:	2022年2月2日 14:58

文件信息

文件名: xiaobeiwang.apk
文件大小: 2.77MB
MD5值: ca254e8c4a394b7730a5256a72cae4d6
SHA1值: 18385eafdb9ef066b7fae8b5e384e98bd07cb9c1
SHA256值: cce2d1edc752d8f92d2f41da217fca89ad006432f7ccb2de94ad4a676a869147

APP 信息

App名称: 小贝网
包名: com.share.share.beili
主活动**Activity:** com.share.share.SplashActivity
安卓版本名称: 1.40
安卓版本: 40

域名线索

域名	是否危险域名	服务器信息
fileimg.988svip.com	good	**IP:** 194.156.163.199 **所属国家:** Belgium **地区:** Brussels Hoofdstedelijk Gewest **城市:** Brussels **纬度:** 50.850449 **经度:** 4.348780 **查看地图:** Google Map

域名	是否危险域名	服务器信息
onekey1.cmpassport.com	good	**IP:** 211.136.10.131 **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
u.anyingyong.com	good	没有服务器地理信息.
mobileauth.yunpian.com	good	**IP:** 120.27.219.119 **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
101.201.176.153	good	**IP:** 101.201.176.153 **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
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

域名	是否危险域名	服务器信息
bl.yuu288.cn	good	没有服务器地理信息.
www.cmpassport.com	good	**IP:** 211.136.10.131 **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
smsks1.cmpassport.com	good	**IP:** 211.136.10.131 **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
e.189.cn	good	**IP:** 42.123.76.65 **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

域名	是否危险域名	服务器信息
alog.umeng.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
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
open.e.189.cn	good	**IP:** 42.123.76.87 **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
config.cmpassport.com	good	**IP:** 120.232.169.180 **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

域名	是否危险域名	服务器信息
log1.cmpassport.com	good	**IP:** 120.232.169.169 **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
collect.ux.21cn.com	good	**IP:** 222.93.106.185 **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
wap.cmpassport.com	good	**IP:** 120.197.235.27 **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
alog.umeng.co	good	没有服务器地理信息.
onepass.geetest.com	good	**IP:** 47.100.115.221 **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
opencloud.wostore.cn	good	**IP:** 210.22.123.92 **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
alogus.umeng.com	good	**IP:** 59.82.31.151 **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

URL线索

URL信息	Url所在文件
https://onekey1.cmpassport.com:443/unisdk/rs/ckRequest	com/cmic/sso/sdk/b/b/a.java
https://config.cmpassport.com/client/uniConfig	com/cmic/sso/sdk/b/b/a.java
https://log1.cmpassport.com:9443/log/logReport	com/cmic/sso/sdk/utils/z.java
https://onekey1.cmpassport.com:443/unisdk/	com/cmic/sso/sdk/utils/z.java
https://smsks1.cmpassport.com:443/unisdk/	com/cmic/sso/sdk/utils/z.java

URL信息	Url所在文件
http://www.cmpassport.com/unisdk/	com/cmic/sso/sdk/utils/z.java
http://www.cmpassport.com/unisdk/	com/cmic/sso/sdk/utils/d.java
https://config.cmpassport.com/client/uniConfig	com/cmic/sso/sdk/utils/d.java
https://mobileauth.yunpian.com/	com/qipeng/yp/onelogin/b.java
https://onepass.geetest.com	com/geetest/onelogin/e/a.java
https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true	com/geetest/onelogin/activity/OneLoginActivity.java
https://e.189.cn/sdk/agreement/detail.do?hidetop=true	com/geetest/onelogin/activity/OneLoginActivity.java
http://wap.cmpassport.com/resources/html/contract.html	com/geetest/onelogin/activity/OneLoginActivity.java
http://bl.yuu288.cn/index/home	com/share/share/MainActivityFragment.java
http://u.anyingyong.com/down/zhushou.apk	com/share/share/MainActivityFragment.java
https://mobileauth.yunpian.com/api/auth/acquirePhone	com/share/share/MainActivityFragment.java
http://101.201.176.153/beili.php?version=	com/share/share/MainActivityFragment.java
http://fileimg.988svip.com/wztips.png	com/share/share/ShareActivity.java
https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code	com/share/share/BaseWXEntryActivity.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java

URL信息	Url所在文件
http://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://alogus.umeng.com/app_logs	com/d/a/d.java
http://alog.umeng.com/app_logs	com/d/a/d.java
http://alog.umeng.co/app_logs	com/d/a/d.java
https://opencloud.wostore.cn/openapi/netauth/precheck/wp?	com/unicom/xiaowo/login/c/f.java
https://opencloud.wostore.cn/authz/oauth/token?timestamp=	com/unicom/xiaowo/login/c/f.java
https://opencloud.wostore.cn/openapi/netauth/precheck/wp?	com/unicom/xiaowo/login/c/h.java
https://opencloud.wostore.cn/openapi/netauth/precheck/wp?	com/unicom/xiaowo/login/c/g.java
https://collect.ux.21cn.com/collect/custom/accountMsg	cn/com/chinatelecom/account/a/c.java
https://open.e.189.cn/openapi/special/getTimeStamp.do	cn/com/chinatelecom/account/api/c/a.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

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.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_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.ACCESS_GPS	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_LOCATION	未知	Unknown permission	Unknown permission from android reference
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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2008-02-29 01:33:46+00:00
Valid To: 2035-07-17 01:33:46+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Serial Number: 0x936eacbe07f201df
Hash Algorithm: sha1
md5: e89b158e4bcf988ebd09eb83f5378e87
sha1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.share.share.MainActivity	Schemes: eli://, Hosts: main,
com.share.share.SplashActivity	Schemes: p2ev9m://,

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>assets/sharePlug!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>r8 without marker (suspicious)</td></tr>
</table>
</td></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
SIM operator check
network operator name check
subscriber ID check
possible ro.secure check
emulator file check</td></tr>
<tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
