MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

潮盒

潮盒 1.1.3.APK

APP名称:	潮盒
包名:	com.dcqkj.chaohe
域名线索:	6条
URL线索:	6条
邮箱线索:	0条
分析日期:	2022年1月18日 23:13

文件信息

文件名: e3563f378cbf49696747c59b48bdf651.apk
文件大小: 22.11MB
MD5值: e3563f378cbf49696747c59b48bdf651
SHA1值: 867d9501abf5f22a539931fc3246a837715640f6
SHA256值: f45f1afc02abb525a4bbf73c7655da87b48bbc740a00a8fa258557428554b040

APP 信息

App名称: 潮盒
包名: com.dcqkj.chaohe
主活动**Activity:** com.dcqkj.chaohe.ui.activity.SplashActivity
安卓版本名称: 1.1.3
安卓版本: 113

域名线索

域名	是否危险域名	服务器信息
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

域名	是否危险域名	服务器信息
eco.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
opencloud.wostore.cn	good	**IP:** 116.128.209.136 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
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
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

域名	是否危险域名	服务器信息
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

URL线索

URL信息	Url所在文件
https://wap.cmpassport.com/resources/html/contract.html	lib/armeabi-v7a/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so
https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true	lib/armeabi-v7a/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so
https://e.189.cn/sdk/agreement/detail.do?isWap=true&hidetop=true&appKey=8138111118	lib/armeabi-v7a/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so
https://eco.taobao.com/router/rest	lib/armeabi-v7a/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so

URL信息	Url所在文件
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://wap.cmpassport.com/resources/html/contract.html	lib/arm64-v8a/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so
https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true	lib/arm64-v8a/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so
https://e.189.cn/sdk/agreement/detail.do?isWap=true&hidetop=true&appKey=8138111118	lib/arm64-v8a/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so
https://eco.taobao.com/router/rest	lib/arm64-v8a/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlog.umeng.com	lib/arm64-v8a/libcrashsdk.so
https://errlogos.umeng.com	lib/arm64-v8a/libcrashsdk.so
https://wap.cmpassport.com/resources/html/contract.html	lib/armeabi/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so
https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true	lib/armeabi/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so
https://e.189.cn/sdk/agreement/detail.do?isWap=true&hidetop=true&appKey=8138111118	lib/armeabi/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so

URL信息	Url所在文件
https://eco.taobao.com/router/rest	lib/armeabi/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi/libcrashsdk.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.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_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

向手机申请的权限	是否危险	类型	详细情况
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.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.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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.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
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何

向手机申请的权限	是否危险	类型	详细情况
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
com.dcqkj.chaohe.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
com.dcqkj.chaohe.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	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.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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。

向手机申请的权限	是否危险	类型	详细情况
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=cn, ST=gd, L=sz, O=lzyd, OU=lzyd, CN=lzyd
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-08-22 02:22:58+00:00
Valid To: 2044-08-15 02:22:58+00:00
Issuer: C=cn, ST=gd, L=sz, O=lzyd, OU=lzyd, CN=lzyd
Serial Number: 0x3927262
Hash Algorithm: sha256
md5: 7de8c6c1adddd516491477d22911c500
sha1: f4db4ca48f58f0205ce91bf27baad924957a7df2
sha256: 105bbf3768b1926e60e4b7d84589ff7ef7896d009b9f0953769583debdae9538
sha512: d79a840ec8ad12bb9599bab4de702788de6b91893025cba86127cd4e24cbdf1933ace580cdf42007d7f92daadc0d879b73552b65f34a43e44ad7968dce9aeb4b

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: e9c23d6371a63cb6b6e8921ea1149f6ad27aa52cc895551ddff6d91b3afe31b4

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>APK包</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>打包</td><td>Tencent's Legu</td></tr>
</table>
</td></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!assets/yaq3_0.sec</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.MODEL check</td></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!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
subscriber ID check</td></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!lib/arm64-v8a/libturingau.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version unknown</td></tr>
</table>
</td></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!lib/armeabi/libturingau.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version unknown</td></tr>
</table>
</td></tr>
<tr><td>lib/arm64-v8a/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>possible VM check</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>lib/armeabi-v7a/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>possible VM check</td></tr></table></td></tr>
<tr><td>lib/armeabi/libauth_number_product-2.12.1-nolog-online-standard-channel_alijtca_plus.so</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>possible VM check</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>unknown (please file detection issue!)</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>防止反汇编</td><td>non-zero link size
non-zero link offset</td></tr><tr><td>打包</td><td>Mobile Tencent Protect</td></tr><tr><td>编译器</td><td>dexlib 2.x</td></tr></table></td></tr>
</table>