MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

阅享 1.3.0.APK

APP名称:	阅享
包名:	com.ashuaq88s.app
域名线索:	5条
URL线索:	2条
邮箱线索:	0条
分析日期:	2022年1月23日 00:22

文件信息

文件名: yuexiang.apk
文件大小: 3.63MB
MD5值: c90b41c85afcdbcafbebb73329be3bf3
SHA1值: f13bcec4661414ec9211c1a284a309c0a31e8d36
SHA256值: 5dacac1a0f8f8d66b49bd220b9016cfcc9a0f229215a2e2c04240c7a509bc38e

APP 信息

App名称: 阅享
包名: com.ashuaq88s.app
主活动**Activity:** com.gowanli.activity.SplashActivity
安卓版本名称: 1.3.0
安卓版本: 191080

域名线索

域名	是否危险域名	服务器信息
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
www.w3.org	good	**IP:** 128.30.52.100 **所属国家:** United States of America **地区:** Massachusetts **城市:** Cambridge **纬度:** 42.365078 **经度:** -71.104523 **查看地图:** Google Map
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
www.mob.com	good	**IP:** 116.62.130.46 **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
www.jinzhichi.cn	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/legu/crashreport/common/strategy/StrategyBean.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/legu/crashreport/common/strategy/StrategyBean.java
http://www.w3.org/2000/svg	Android String Resource
http://www.mob.com	Android String Resource
http://www.jinzhichi.cn	Android String Resource

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.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
com.ashuaq88s.app.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
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.VIBRATE	正常	可控震源	允许应用程序控制振动器

向手机申请的权限	是否危险	类型	详细情况
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
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_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.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
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.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.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

向手机申请的权限	是否危险	类型	详细情况
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.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.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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。

签名证书

APK is signed

v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=Zhejiang, L=Hangzhou, O=Weckey, OU=HuoNiu, CN=阿帅哦11
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-01-27 07:36:12+00:00
Valid To: 2039-01-22 07:36:12+00:00
Issuer: C=CN, ST=Zhejiang, L=Hangzhou, O=Weckey, OU=HuoNiu, CN=阿帅哦11
Serial Number: 0x59b3ba70
Hash Algorithm: sha256
md5: 05461380257773ced108d08483a52af0
sha1: 87c86e0af46622a6ec903f08b1ab94a927a7f632
sha256: 5c99a2cdb444d6bcde4bc104df87c46f101306ed32f1f80e64d2944625fb55a2
sha512: 4450b20eededfe27e84f1f30f1adc5ac1136dc30a209891655e42d099fd555664033ee971d68cf50a34979c956c74a9e108ad82d36fcf4acc5b9e44322821b36

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
"aliyun_app_key" : "25622635"
"aliyun_app_secret" : "7ae5d43d7fa8d35a92a2a72987e4b831"
"huawei_app_secret" : "9de01d5b9fd15837a08aafdcd0a1b3d7"

可能的敏感信息
"xiaomi_app_key" : "5591794226582"
"xiaomi_app_secret" : "oUu/arU1GcTkqWVIkBIk0Q=="
"mob_app_key" : "29f53b96520b0"
"mob_app_secret" : "ce8677fdbff31cc933d4d491de026781"
"wechat_app_secret" : "ce7e43bbe3c2d102944f4338e5243403"
"sina_app_key" : "3823540414"
"sina_app_secret" : "ab12ca6edaa93aeb718d115dee5dab0c"
"tencent_app_key" : "96hwdtf35jvlJnyX"
"baidu_lbs_key" : "gozZ2VcjCA6iP1rE4q1GliyF8QbVSizc"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"ssdk_instapaper_pwd" : "密码"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.gowanli.activity.MainActivity	Schemes: com.ashuaq88s.app://,

活动(ACTIVITY)	通信(INTENT)
cn.sharesdk.tencent.qq.ReceiveActivity	Schemes: @string/tencent_scheme://,

加壳分析

文件列表	分析结果
APK包	壳列表 / 详细情况 打包 / Mobile Tencent Protect

<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>打包</td><td>Mobile Tencent Protect</td></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
subscriber ID check
possible ro.secure check
emulator file check</td></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi/mix.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi/mixz.dex!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>dx</td></tr>
</table>
</td></tr>
</table>