MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

怡信 1.42.APK

APP名称:	怡信
包名:	chatyi.com
域名线索:	5条
URL线索:	8条
邮箱线索:	0条
分析日期:	2022年1月29日 00:18

文件信息

文件名: yixing.apk

文件大小: 7.51MB
MD5值: a50aa9c961778e9b7808eac47a9f8934
SHA1值: c17e7614a862ede7999c0e27774d5a6af3890249
SHA256值: 4668ca996c9f7133f7665cf463402b65cfd7191733de28362cfb154bbdc16eec

APP 信息

App名称: 怡信
包名: chatyi.com
主活动Activity: chatyi.com.SplashScreen
安卓版本名称: 1.42
安卓版本: 142

域名线索

域名	是否危险域名	服务器信息
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
configapi-api.glqa.jpushoa.com	good	IP: 172.17.5.42 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map

域名	是否危险域名	服务器信息
ce3e75d5.jpush.cn	good	**IP:** 183.232.58.243 **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
chat-yi.com	good	没有服务器地理信息.
aphroditemessenger.com	good	**IP:** 172.105.6.203 **所属国家:** Canada **地区:** Ontario **城市:** Toronto **纬度:** 43.700111 **经度:** -79.416298 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
https://github.com/Bearded-Hen/Android-Bootstrap	com/beardedhen/androidbootstrap/TypefaceProvider.java
http://configapi-api.glqa.jpushoa.com/v1/status	cn/jiguang/ay/e.java
https://ce3e75d5.jpush.cn/wi/op8jdu	cn/jiguang/p/c.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/au/c.java

URL信息	Url所在文件
https://ce3e75d5.jpush.cn/wi/d8n3hj	cn/jiguang/au/c.java
https://chat-yi.com	Android String Resource
https://aphroditemessenger.com/terms	Android String Resource
https://aphroditemessenger.com/policy	Android String Resource
https://aphroditemessenger.com	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
chatyi.com.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
chatyi.com.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
com.huawei.android.launcher.permission.CHANGE_BADGE	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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.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.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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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。
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。
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.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_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.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.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_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
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
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
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=USA, ST=MA, L=Medford, O=aphroditemessenger.com, OU=aphroditemessenger.com, CN=William Santiago
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-11-03 08:10:31+00:00
Valid To: 2045-10-28 08:10:31+00:00
Issuer: C=USA, ST=MA, L=Medford, O=aphroditemessenger.com, OU=aphroditemessenger.com, CN=William Santiago
Serial Number: 0x6c6c1fde
Hash Algorithm: sha256
md5: 69fc8466d98845dbf7f967f9dcef01c7
sha1: 4554731aa9c1ae9cf6db51d3ade5cd62d07c94a3
sha256: 96bd423c77dfe1c05293d1a32aba120d6fbd1f1608c9c3063ccc462c6c4f9cd6
sha512: ce7955f8022137f5d42236386d43ae0c30cc83353f3657b232b55c995ed7c388158ecf0292c81e6611b916c02650f29e07dad3a84a4c748acc66746df8dd7527
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: d67d00e9edfd6fa624969fb762d32c19a24d5a05edb85b1dc647338c74cbbda2

Exodus威胁情报

名称	分类	URL链接
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343

硬编码敏感信息

可能的敏感信息
"channel_token" : "Channel Token : "
"login_username" : "Username"
"login_username" : "Nutzername"
"channel_token" : "聊天口令 : "
"login_username" : "用户名"
"login_username" : "tên tài khoản"
"login_username" : "ユーザー名"
"login_username" : "Nom d'utilisateur"
"channel_token" : "□□□ □□ : "

可能的敏感信息
"login_username" : "□□□ □□"
"login_username" : "Nombre de usuario"
"login_username" : "Имя пользователя"

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>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
Build.TAGS check
network operator name check
device ID check
subscriber ID 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>
