MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

一米社区 1.0.APK

APP名称:	一米社区
包名:	io.dcloud.H50F23A94
域名线索:	2条
URL线索:	2条
邮箱线索:	0条
分析日期:	2022年1月28日 23:23

文件信息

文件名: yimishequ521411.apk
文件大小: 6.17MB
MD5值: 1845c1a351b549d316cdaa05741ccf05
SHA1值: 833ff78438b373088f444e9c6c3bb59ddbada53b
SHA256值: a27288d9e33f437246b6f6a531a23529c9a3af8387da006014a0666674adbba0

APP 信息

App名称: 一米社区
包名: io.dcloud.H50F23A94
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 1.0
安卓版本: 101

域名线索

域名	是否危险域名	服务器信息
rqd.uu.qq.com	good	**IP:** 182.254.88.185 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
android.bugly.qq.com	good	**IP:** 109.244.244.35 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
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/lejiagu/crashreport/common/strategy/StrategyBean.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/lejiagu/crashreport/common/strategy/StrategyBean.java
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

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.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.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.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.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.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.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.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.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

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.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
android.permission.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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.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

向手机申请的权限	是否危险	类型	详细情况
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher2.permission.READ_SETTINGS	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.android.launcher3.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.yulong.android.launcherL.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.bbk.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.qiku.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.READ_SETTINGS	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
com.zte.mifavor.launcher.permission.READ_SETTINGS	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.lenovo.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.google.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.yulong.android.launcher3.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adw.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.qihoo360.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.lge.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
net.qihoo.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adwfreak.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adw.launcher_donut.permission.READ_SETTINGS	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.launcher3.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.fede.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.sec.android.app.twlauncher.settings.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.tencent.qqlauncher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.ebproductions.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.nd.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.yulong.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.mylauncher.permission.READ_SETTINGS	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.ztemt.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
cn.nubia.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.gionee.amisystem.permission.READ_SHORTCUT	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=86, ST=shanxi, L=taiyuan, O=shengdun, OU=shengdun, CN=mipengfei
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-09-03 06:46:38+00:00
Valid To: 2043-08-28 06:46:38+00:00
Issuer: C=86, ST=shanxi, L=taiyuan, O=shengdun, OU=shengdun, CN=mipengfei
Serial Number: 0x49fe4103
Hash Algorithm: sha256
md5: 19aee0de9bfb8d0ad67e08753fa7fafc
sha1: 559f806cfbd43889f437a849354ac7288f3c3d8d
sha256: 8120ab440057b9d67b610db9a4a310fcddc6ba2f8f44cd0bdb9e6f666aefcd3b
sha512: 1e63637ca6a5760ee4e75707401c5db1ab0d4311159a7a9b2bcc17a3a796067c15b5a940c3376d1cdc09e1cb3424cf057729852757b4c950e93d0518421b4876

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntryActivity	Schemes: h50f23a94://,

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
Build.PRODUCT check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
device ID check
subscriber ID check
possible VM check</td></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi-v7a/libshella-2.9.0.2.so</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>
</table>
</td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>lib/armeabi/libshella-2.9.0.2.so</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></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>
<tr><td>lib/x86/libshellx-2.9.0.2.so</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></table></td></tr>
</table>
