MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Love.ru Lite 1.0.3.APK

APP名称:	Love.ru Lite
包名:	com.dating.mylove.lite
域名线索:	10条
URL线索:	10条
邮箱线索:	0条
分析日期:	2022年1月28日 23:05

文件信息

文件名: loverulite515090.apk
文件大小: 4.43MB
MD5值: b5a6caa7cbf0cd224043e929df158626
SHA1值: 3c7b9f3d04adc3343eaee322af47efbde76c9219
SHA256值: 0d5e8c036b941c51d4aefef6b46da8a00610d15d3dfbc649c86725a1ddacddf6

APP 信息

App名称: Love.ru Lite
包名: com.dating.mylove.lite
主活动**Activity:** ru.mylove.android.ui.splash.SplashActivity
安卓版本名称: 1.0.3
安卓版本: 112063

域名线索

域名	是否危险域名	服务器信息
startup.mobile.yandex.net	good	**IP:** 213.180.204.244 **所属国家:** Russian Federation **地区:** Moskva **城市:** Moscow **纬度:** 55.752220 **经度:** 37.615559 **查看地图:** Google Map

域名	是否危险域名	服务器信息
vk.com	good	**IP:** 87.240.190.67 **所属国家:** Russian Federation **地区:** Sankt-Peterburg **城市:** Saint Petersburg **纬度:** 59.894440 **经度:** 30.264170 **查看地图:** Google Map
tech.yandex.com	good	**IP:** 213.180.204.242 **所属国家:** Russian Federation **地区:** Moskva **城市:** Moscow **纬度:** 55.752220 **经度:** 37.615559 **查看地图:** Google Map
oauth.vk.com	good	**IP:** 87.240.129.135 **所属国家:** Russian Federation **地区:** Sankt-Peterburg **城市:** Saint Petersburg **纬度:** 59.894440 **经度:** 30.264170 **查看地图:** Google Map
m.love.ru	good	**IP:** 136.243.161.204 **所属国家:** Germany **地区:** Bayern **城市:** Nuremberg **纬度:** 49.447781 **经度:** 11.068330 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.facebook.com	good	**IP:** 150.107.3.176 **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
love.ru	good	**IP:** 136.243.161.204 **所属国家:** Germany **地区:** Bayern **城市:** Nuremberg **纬度:** 49.447781 **经度:** 11.068330 **查看地图:** Google Map
api.damochka.ru	good	**IP:** 136.243.161.206 **所属国家:** Germany **地区:** Bayern **城市:** Nuremberg **纬度:** 49.447781 **经度:** 11.068330 **查看地图:** Google Map
www.google.com	good	**IP:** 174.37.54.20 **所属国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.939491 **经度:** -96.838730 **查看地图:** Google Map

域名	是否危险域名	服务器信息
api.love.ru	good	**IP:** 136.243.161.206 **所属国家:** Germany **地区:** Bayern **城市:** Nuremberg **纬度:** 49.447781 **经度:** 11.068330 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
https://startup.mobile.yandex.net/	com/yandex/metrica/impl/ob/su.java
https://tech.yandex.com/metrica-mobile-sdk/doc/mobile-sdk-dg/concepts/android-initialize-docpage/	com/yandex/metrica/impl/ob/yl.java
https://oauth.vk.com/blank.html	com/vk/sdk/dialogs/VKOpenAuthDialog.java
https://oauth.vk.com/authorize? client_id=%s&scope=%s&redirect_uri=%s&display=mobile&v=%s&response_type=token&revoke=%d	com/vk/sdk/dialogs/VKOpenAuthDialog.java
http://vk.com/images/s_noalbum.png	com/vk/sdk/api/model/VKApiPhotoAlbum.java
http://vk.com/images/m_noalbum.png	com/vk/sdk/api/model/VKApiPhotoAlbum.java
http://vk.com/images/x_noalbum.png	com/vk/sdk/api/model/VKApiPhotoAlbum.java
https://api.love.ru	ru/mylove/android/Application.java

URL信息	Url所在文件
http://www.google.com	ru/mylove/android/ui/AppWebActivity.java
https://api.damochka.ru/	ru/mylove/android/ui/AppWebActivity.java
https://m.love.ru	ru/mylove/android/ui/AppWebActivity.java
https://api.love.ru	ru/mylove/android/ui/AppDebugHelper.java
https://m.love.ru	ru/mylove/android/ui/AppDebugHelper.java
https://love.ru	ru/mylove/android/fcm/FcmService.java
https://api.love.ru	ru/mylove/android/operations/MultiOperation.java
www.facebook.com/	Android String Resource
https://m.love.ru/agreement/privacy/?action=simple	Android String Resource
https://m.love.ru/agreement/main/?action=simple	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.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
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
org.onepf.openiab.permission.BILLING	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-06-08 12:57:59+00:00
Valid To: 2051-06-08 12:57:59+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0xe14d0be815d876785c6c7666e13f8ddfc292fe14
Hash Algorithm: sha256
md5: c4917362275d841313bdb69cd83ecd93
sha1: 01f3a32afaae67b303a2ee3711246b8e88d34f53
sha256: 11e2fb5397961a51226e03f27056ed46e9606a27669dbf73ec565f196bb8536a
sha512: e67d65c59fb73092565cf3bfa7d0e6c5ec49c3e1f48d4f65be9c204d1dd54e8dc9c76799374f860a0ca417bdc99a8b6ad68fc001e482280a03edc03c41639f5d
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: f4c5b81d96cb60f83f1fcfacfa193808ea439b0e44261451344cfe80b32bc84c

Exodus威胁情报

名称	分类	URL链接
AppMetrica		https://reports.exodus-privacy.eu.org/trackers/140
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
VKontakte SDK	Identification	https://reports.exodus-privacy.eu.org/trackers/382

硬编码敏感信息

可能的敏感信息
"google_api_key" : "AIzaSyDdFqE2YMZYheGBnFcC4pIizqxRfU--M2w"

可能的敏感信息
"google_crash_reporting_api_key" : "AIzaSyDdFqE2YMZYheGBnFcC4pIizqxRfU--M2w"
"google_maps_key" : "AIzaSyAVhw0ps5oW0QGYXYvFWwrnDNvO114KZZ4"
"greeeting_auth" : "Dear, %s!"
"greeeting_noauth" : "Hello!"
"password" : "Password"
"restore_password" : "Send"
"settings_password" : "Change Password"
"vk_auth_canceled" : "Authorization was canceled"
"greeeting_auth" : "Уважаемый пользователь, %s!"
"greeeting_noauth" : "Здравствуйте!"
"password" : "Пароль"
"restore_password" : "Восстановить пароль"
"settings_password" : "Поменять пароль"
"vk_auth_canceled" : "Авторизация была отменена"
"greeeting_auth" : "Уважаемый пользователь, %s!"

可能的敏感信息
"greeeting_noauth" : "Здравствуйте!"
"password" : "Пароль"
"restore_password" : "Восстановить пароль"
"settings_password" : "Поменять пароль"
"vk_auth_canceled" : "Авторизация была отменена"
"greeeting_auth" : "Уважаемый пользователь, %s!"
"greeeting_noauth" : "Здравствуйте!"
"password" : "Пароль"
"restore_password" : "Восстановить пароль"
"settings_password" : "Поменять пароль"
"vk_auth_canceled" : "Авторизация была отменена"
"greeeting_auth" : "Уважаемый пользователь, %s!"
"greeeting_noauth" : "Здравствуйте!"
"password" : "Пароль"
"restore_password" : "Восстановить пароль"

可能的敏感信息
"settings_password" : "Поменять пароль"
"vk_auth_canceled" : "Авторизация была отменена"
"greeeting_auth" : "Уважаемый пользователь, %s!"
"greeeting_noauth" : "Здравствуйте!"
"password" : "Пароль"
"restore_password" : "Восстановить пароль"
"settings_password" : "Поменять пароль"
"vk_auth_canceled" : "Авторизация была отменена"
"greeeting_auth" : "Уважаемый пользователь, %s!"
"greeeting_noauth" : "Здравствуйте!"
"password" : "Пароль"
"restore_password" : "Восстановить пароль"
"settings_password" : "Поменять пароль"
"vk_auth_canceled" : "Авторизация была отменена"
"greeeting_auth" : "Уважаемый пользователь, %s!"

可能的敏感信息
"greeeting_noauth" : "Здравствуйте!"
"password" : "Пароль"
"restore_password" : "Восстановить пароль"
"settings_password" : "Поменять пароль"
"vk_auth_canceled" : "Авторизация была отменена"
"greeeting_auth" : "Уважаемый пользователь, %s!"
"greeeting_noauth" : "Здравствуйте!"
"password" : "Пароль"
"restore_password" : "Восстановить пароль"
"settings_password" : "Поменять пароль"
"vk_auth_canceled" : "Авторизация была отменена"

应用内通信

活动(ACTIVITY)	通信(INTENT)
ru.mylove.android.ui.splash.SplashActivity	Schemes: http://, https://, @string/app_scheme://, Hosts: love.ru, m.love.ru,

加壳分析

<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
SIM operator check
network operator name check</td></tr>
<tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>编译器</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

报告由 摸瓜平台 自动生成，并非包含所有检测结果，有疑问请联系管理员。

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析