MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

初见约会 1.0.0.APK

APP名称:	初见约会
包名:	com.chujian.yh
域名线索:	1条
URL线索:	1条
邮箱线索:	1条
分析日期:	2022年1月28日 23:59

文件信息

文件名: cjyh.apk
文件大小: 7.85MB
MD5值: 1fc24fd59348aefd8594addeaaebe78a
SHA1值: 84ea232842cd7917893831ec66de622a84dd9682
SHA256值: 4d3f9a86f9c3e01fa82c43453cb8f4455b22cdca7406a9d83e5095c0f5273b2e

APP 信息

App名称: 初见约会
包名: com.chujian.yh
主活动**Activity:** com.chujian.yh.jyj_activity.JYJLaunchActivity
安卓版本名称: 1.0.0
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
www.openssl.org	good	**IP:** 23.41.243.45 **所属国家:** United States of America **地区:** Massachusetts **城市:** Cambridge **纬度:** 42.363598 **经度:** -71.085205 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/librealm-jni.so

邮箱线索

邮箱地址	所在文件
help@realm.io	lib/armeabi-v7a/librealm-jni.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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=key172
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-05-14 07:54:03+00:00
Valid To: 2045-05-08 07:54:03+00:00
Issuer: CN=key172
Serial Number: 0x2e431934
Hash Algorithm: sha256
md5: 1a915d36135b2c9cb264f51af500cebd
sha1: 2d14efb059ba1ba5783906c2b124eb1d3e86e7f5
sha256: abbc07c8124bc874e00a450ab67c4b52f97f9c65d33f91c64861f8cbbae2edb2
sha512: 7aa94e1d6efe307bfa45b69c608023173b5bb3af45911fb7ef6907a0f2a40db1b1b585ed739e49142991948755b3d044688b549ca023dad40e4c19c399b15fdf
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: eeb7b791054ad7d9d58948b35237263110ff0da1b740ad38aa306733b93e3026

Exodus威胁情报

名称	分类	URL链接
TalkingData	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/293

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>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.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!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>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></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>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.BRAND check
Build.DEVICE check
Build.PRODUCT check
possible Build.SERIAL check
SIM operator check
network operator name check
subscriber ID check
possible VM 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>
