MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

又开薪 2.0.APK

APP名称:	又开薪
包名:	cn.hlgrp.sqm
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2022年1月25日 22:58

文件信息

文件名: youkaixin486269.apk
文件大小: 7.01MB
MD5值: 1e714adb9a990fbd1b4be50b50d8df87
SHA1值: 8cae6cb8e42d12015f8ddf61c170c7dbf15d84be
SHA256值: 48d1c27522930df4aa1fbdc9d6883d3451fe4de45071cc03be67f2addb13c96b

APP 信息

App名称: 又开薪
包名: cn.hlgrp.sqm
主活动**Activity:** cn.hlgrp.sqm.HomeActivity
安卓版本名称: 2.0
安卓版本: 10

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

URL线索

URL信息	Url所在文件
https://github.com/vinc3m1	Android String Resource
https://github.com/vinc3m1/RoundedImageView	Android String Resource
https://github.com/vinc3m1/RoundedImageView.git	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
cn.hlgrp.sqm.permission.MIPUSH_RECEIVE	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.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
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.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

向手机申请的权限	是否危险	类型	详细情况
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。
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=86, ST=guangdong, L=shenzhen, O=hlgrp, OU=hlgrp, CN=leimin
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-11-04 07:04:31+00:00
Valid To: 2043-10-29 07:04:31+00:00
Issuer: C=86, ST=guangdong, L=shenzhen, O=hlgrp, OU=hlgrp, CN=leimin
Serial Number: 0x412fa716
Hash Algorithm: sha256
md5: 6c77e0cdeb8dea86e91379dbb089d750
sha1: 2ad8dd1e1b8d6eea63098f9cf4bf096739bd3d7c

sha256: c1fc62d065859d8b76a4537eb4db85deabd1a4dded4308232df38b58ae9dc584
sha512: 25f67408ecd5222f3294e39a4f5f0f878bdb80b901ffaad84379159c9aaff77117d75c7259da0623e790a2210bab9311d48228e9f21cd21bde69a8dc676a4392
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 57faaa17ede0c5aed98884972e8e245801241a9f3dd5b067cd8ce6133edee22c

Exodus威胁情报

名称	分类	URL链接
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116

硬编码敏感信息

可能的敏感信息
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"str_password" : "密码"

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></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>
<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.MANUFACTURER check
Build.BOARD check
possible Build.SERIAL check
SIM operator check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
