MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

ACGN社区 1.9.73.APK

APP名称:	ACGN社区
包名:	niming360.acgnsq.bd
域名线索:	6条
URL线索:	9条
邮箱线索:	2条
分析日期:	2022年1月28日 21:59

文件信息

文件名: acgshequ.apk
文件大小: 5.66MB
MD5值: 9f3ca83f6154e61ef2260a1ef1bf566c
SHA1值: f96b1e70d9e369098f65b18514f53ec10518f81b
SHA256值: ce3e493f50a0c121ef9c06b833f6843c5f2c9eb740d8c811c645aff80607c0a3

APP 信息

App名称: ACGN社区
包名: niming360.acgnsq.bd
主活动**Activity:** nimingban.acgnsq.tv.MainActivity
安卓版本名称: 1.9.73
安卓版本: 109750

域名线索

域名	是否危险域名	服务器信息
ap.cpatrk.net	good	**IP:** 116.198.14.30 **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

域名	是否危险域名	服务器信息
dns.qq.com	good	**IP:** 119.29.29.229 **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
cloud.cpatrk.net	good	**IP:** 116.198.14.47 **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
api.whatsapp.com	good	**IP:** 104.244.43.208 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.773968 **经度:** -122.410446 **查看地图:** Google Map
www.talkingdata.net	good	**IP:** 116.196.122.26 **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

域名	是否危险域名	服务器信息
me.cpatrk.net	good	**IP:** 116.198.14.136 **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
https://dns.qq.com	com/tendcloud/tenddata/al.java
https://cloud.cpatrk.net/configcloud/rest/sdk/gdprCheck	com/tendcloud/tenddata/aa.java
https://ap.cpatrk.net/u/a/v1	com/tendcloud/tenddata/aa.java
https://cloud.cpatrk.net/configcloud/rest/sdk/match	com/tendcloud/tenddata/aa.java
www.talkingdata.net	com/tendcloud/tenddata/u.java
https://me.cpatrk.net	com/tendcloud/tenddata/a.java
https://api.whatsapp.com/send?phone=	nl/xservices/plugins/SocialSharing.java

邮箱线索

邮箱地址	所在文件
test@test.com	com/mopgame/netdiagno/LDNetDiagnoPlugin.java
someone@domain.com	nl/xservices/plugins/SocialSharing.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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
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.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
android.permission.EXPAND_STATUS_BAR	正常	展开/折叠状态栏	允许应用程序展开或折叠状态栏
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.RECEIVE_USER_PRESENT	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
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.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.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.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.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_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.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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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

向手机申请的权限	是否危险	类型	详细情况
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=acgnshequ, ST=acgnshequ, L=acgnshequ, O=acgnshequ, OU=acgnshequ, CN=sign.acgnshequ.keystore
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-06-22 08:21:24+00:00
Valid To: 3846-09-29 08:21:24+00:00
Issuer: C=acgnshequ, ST=acgnshequ, L=acgnshequ, O=acgnshequ, OU=acgnshequ, CN=sign.acgnshequ.keystore
Serial Number: 0x51eaec8e
Hash Algorithm: sha256
md5: d16914b3896bee92a041bf20d9a43b67
sha1: d50f30484177c7d9464fbd9c733dcae2826bf18e
sha256: 25156d60bafde6ff817af7aa3f47c57d66667d0a37fd06141e690b8fb929fe83
sha512: 306839723f1efa44fe270226f8850d84ff7bd2d8c34201503aa53f9bf0ca888210fe071dab39a54c02c067bc05bfc02d256ef8953e681f977223c215b715f274
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: a1e8fd6d8cbab03a2c383afbde7cdde2dd834ee25a7f805600ecb6a6abbcca80

Exodus威胁情报

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

应用内通信

活动(ACTIVITY)	通信(INTENT)
nimingban.acgnsq.tv.MainActivity	Schemes: adnmb://, tnmb://, https://, Hosts: adnmb.com, adnmb2.com, adnmb3.com, tnmb.org, Mime Types: text/plain, image/*, Path Patterns: /t/.*,

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>APK包</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
possible Build.SERIAL check
SIM operator check
network operator name check
subscriber ID check
network interface name check</td></tr>
<tr><td>编译器</td><td>dexlib 2.x</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>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

<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
Build.BOARD check
possible Build.SERIAL check
SIM operator check
network operator name check
subscriber ID check
network interface name check</td></tr>
<tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>
