MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Joromi 3.2.APK

APP名称:	Joromi
包名:	joromi.ajef
域名线索:	1条
URL线索:	1条
邮箱线索:	2条
分析日期:	2022年1月28日 22:21

文件信息

文件名: joromi528268.apk
文件大小: 10.14MB
MD5值: 9ac134423234dc9c97bd41995ded0885
SHA1值: 5fb8c82043813c253d57a5a907bac4a9bd1222bf
SHA256值: 5a616616aaf90834763e3fda4d5ec5e3393759eb8db7615c8581b077bdfc201b

APP 信息

App名称: Joromi
包名: joromi.ajef
主活动**Activity:** joromi.ajef.preinicio
安卓版本名称: 3.2
安卓版本: 4

域名线索

域名	是否危险域名	服务器信息
api-project-751842291101.firebaseio.com	good	**IP:** 35.201.97.85 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568 查看地图: Google Map

URL线索

URL信息	Url所在文件
https://api-project-751842291101.firebaseio.com	Android String Resource

邮箱线索

邮箱地址	所在文件
o@netstream.failed	lib/x86_64/librtmp-jni.so
o@netstream.failed	lib/x86/librtmp-jni.so

数据库线索

FIREBASE链接地址	详细信息
https://api-project-751842291101.firebaseio.com	info App talks to a Firebase Database.

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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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
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
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度

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: 2021-07-15 09:24:02+00:00
Valid To: 2051-07-15 09:24:02+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xf9933da6e0f469e2e6e7916100b63fd87af17725
Hash Algorithm: sha256
md5: 1a28583aeff2eab4e7710af96d7231b8
sha1: 322397b0ac5cf3baf7ea2c08164b6de61986c433
sha256: c131c31c600d6329fdaf488548d53382e5f43820e0af181c4e9540640c8dde6f
sha512: d6fefd33f9325cdf2e3786d521a68d9b74a60f0d49da5b025d236a1571eba3429ccd61d35047b4301662d226260b220efc1d9d0d5bbfbc8a868e8c1926eaf124
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 7ce22b27553424966c93b2ddd8137fd3a5b0f65150b3544c91c2fee0667b65bc

Exodus威胁情报

名称	分类	URL链接
AdColony	Advertisement	https://reports.exodus-privacy.eu.org/trackers/90
Appnext		https://reports.exodus-privacy.eu.org/trackers/184
Facebook Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/65
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67

名称	分类	URL链接
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Startapp	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/195
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121

🔑 硬编码敏感信息

可能的敏感信息
"com_facebook_device_auth_instructions" : "Visit facebook.com/device and enter the code shown above."
"firebase_database_url" : "https://api-project-751842291101.firebaseio.com"
"google_api_key" : "AIzaSyCtzGwdiM8t6R6Ff6uCwEYggQECaFdCcFA"
"google_crash_reporting_api_key" : "AIzaSyCtzGwdiM8t6R6Ff6uCwEYggQECaFdCcFA"
"com_facebook_device_auth_instructions" : "Gehe zu facebook.com/device und gib den oben angezeigten Code ein."
"com_facebook_device_auth_instructions" : "Ga naar facebook.com/device en voer de bovenstaande code in."
"com_facebook_device_auth_instructions" : "تفضل بزيارة facebook.com/device وإدخال الرمز الموضح أعلاه."

可能的敏感信息
"com_facebook_device_auth_instructions" : "Consultez facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "facebook.com/device adresine git ve yukarıda gösterilen kodu gir."
"com_facebook_device_auth_instructions" : "Ve a facebook.com/device e ingresa el código que se muestra arriba."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e inserisci il codice mostrato qui sotto."
"com_facebook_device_auth_instructions" : "Acesse facebook.com/device e insira o código mostrado acima."
"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og indtast koden, som er vist ovenfor."
"com_facebook_device_auth_instructions" : "facebook.com/deviceにアクセスして、上のコードを入力してください。"
"com_facebook_device_auth_instructions" : "facebook.com/device '[redacted]"
"com_facebook_device_auth_instructions" : "facebook.com/device [redacted]"
"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og skriv inn koden som vises over."
"com_facebook_device_auth_instructions" : "facebook.com/device[redacted]"
"com_facebook_device_auth_instructions" : "Besoek facebook.com/device en voer die kode wat hierbo gewys word, in."
"com_facebook_device_auth_instructions" : "[redacted] facebook.com/device [redacted]"
"com_facebook_device_auth_instructions" : "Siirry osoitteeseen facebook.com/device ja anna oheinen koodi."
"com_facebook_device_auth_instructions" : "facebook.com/device [redacted]"

可能的敏感信息
"com_facebook_device_auth_instructions" : "Truy cập facebook.com/device và nhập mã được hiển thị bên trên."
"com_facebook_device_auth_instructions" : "Navštívte stránku facebook.com/device a zadajte kód zobrazený vyššie."
"com_facebook_device_auth_instructions" : "Πηγαίνετε στη διεύθυνση facebook.com/device και εισαγάγετε τον παραπάνω κωδικό."
"com_facebook_device_auth_instructions" : "facebook.com/device [redacted]"
"com_facebook_device_auth_instructions" : "Odwiedź stronę facebook.com/device i wprowadź powyższy kod."
"com_facebook_device_auth_instructions" : "Puntahan ang facebook.com/device at ilagay ang code na ipinapakita sa itaas."
"com_facebook_device_auth_instructions" : "facebook.com/device [redacted]"
"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di bawah ini."
"com_facebook_device_auth_instructions" : "facebook.com/device [redacted]"
"com_facebook_device_auth_instructions" : "facebook.com/device[redacted]."
"com_facebook_device_auth_instructions" : "Vizitează facebook.com/device şi introdu codul de mai sus."
"com_facebook_device_auth_instructions" : "Posjetitw facebook.com/device i unesite gore prikazani kôd."
"com_facebook_device_auth_instructions" : "facebook.com/device [redacted]"
"com_facebook_device_auth_instructions" : "Přejděte na facebook.com/device a zadejte nahoře uvedený kód."
"com_facebook_device_auth_instructions" : "Lawati facebook.com/device dan masukkan kod yang ditunjukkan di atas."

可能的敏感信息

"com_facebook_device_auth_instructions" : "facebook.com/device</b&gt ■■ ■■■■■■ ■■;■■■ ■■■ ■■■■■ ■■■ ■■■■ ■■■■"
"com_facebook_device_auth_instructions" : "Keresd fel a facebook.com/device címet, és írd be a fent megjelenített kódot."
"com_facebook_device_auth_instructions" : "Откройте facebook.com/device и введите код, показанный выше."
"com_facebook_device_auth_instructions" : "Gå till facebook.com/device och skriv in koden som visas ovan."
"com_facebook_device_auth_instructions" : "ולהזין את הקוד המוצג למעלה facebook.com/device</b&gt יש לבקר בכתובת"
"com_facebook_device_auth_instructions" : "Accédez à facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "前往facebook.com/device</b&gt，並輸入上方顯示的代碼。"
"com_facebook_device_auth_instructions" : "请访问facebook.com/device并输入以上验证码。"
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e insere o código apresentado abaixo."
"com_facebook_device_auth_instructions" : "前往facebook.com/device</b&gt，並輸入上方顯示的代碼。"
"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di atas."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e introduce el código que se muestra más arriba."

应用内通信

活动(ACTIVITY)	通信(INTENT)
joromi.ajef.preinicio	Schemes: http://, https://, Hosts: www.appcreator24.com, join-app.net, Path Prefixes: /open1580707/, /a1580707/,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.joromi.ajef,

加壳分析

文件列表	分析结果
assets/audience_network.dex	壳列表 / 详细情况 反调试 — Debug.isDebuggerConnected() check 反虚拟机 — possible Build.SERIAL check 编译器 — unknown (please file detection issue!)

文件列表	分析结果
classes.dex	<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.TAGS check SIM operator check network operator name check</td></tr><tr><td>编译器</td><td>r8</td></tr></table>

<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>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
subscriber ID check
ro.product.device check
ro.kernel.qemu check
possible ro.secure check
emulator file check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
