MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

KHAZANAY 1.2.APK

APP名称:	KHAZANAY
包名:	com.khazanay
域名线索:	6条
URL线索:	3条
邮箱线索:	0条
分析日期:	2022年1月22日 23:17

文件信息

文件名: khazanay579498.apk
文件大小: 2.66MB
MD5值: 4667f41a5c312c6efdf4aee8b43b36c5
SHA1值: d0ca1e8aff47f1b9792cecc2343c52cae2b2be62
SHA256值: 5e0bc1bdd5a0ec75b68b9bcc23cb3874c17edf95fcebdfa68455bb988168b597

APP 信息

App名称: KHAZANAY
包名: com.khazanay
主活动**Activity:** com.khazanay.SplashActivity
安卓版本名称: 1.2
安卓版本: 3

域名线索

域名	是否危险域名	服务器信息
www.instagram.com	good	**IP:** 162.125.32.5 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map

域名	是否危险域名	服务器信息
m.facebook.com	good	IP: 199.59.148.9 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
khazanay-4df05.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
www.khazanay.pk	good	IP: 23.227.38.74 所属国家: Canada 地区: Ontario 城市: Ottawa 纬度: 45.418877 经度: -75.696510 查看地图: Google Map
mobile.twitter.com	good	IP: 199.59.148.15 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

域名	是否危险域名	服务器信息
twitter.com	good	**IP:** 162.220.12.226 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683 查看地图: Google Map

URL线索

URL信息	Url所在文件
https://www.khazanay.pk/	com/khazanay/MainActivity.java
https://m.facebook.com	com/khazanay/MainActivity.java
https://twitter.com/khazanayalerts	com/khazanay/MainActivity.java
https://mobile.twitter.com/khazanayalerts	com/khazanay/MainActivity.java
https://www.instagram.com/khazanay	com/khazanay/MainActivity.java
https://khazanay-4df05.firebaseio.com	Android String Resource

数据库线索

FIREBASE链接地址	详细信息
https://khazanay-4df05.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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

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: 2019-07-08 06:39:30+00:00
Valid To: 2049-07-08 06:39:30+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x9d4ad173240bae482d130bdc53bcea00312f7a9d
Hash Algorithm: sha256
md5: 3ea84e0dddd3dd026346567e91730ba3
sha1: a695a90dbbc0c4402b88d308780ee97b1b809f10
sha256: 0da933bff86e3df609226be4810201a26dc87dc34162ce4342c54f0479064534
sha512: 1e31d21848dbee84cf27f2cd9601a44db7b80297d2c716659c424c188b2ebe82b2d6740de776d1b5033af70abcd8f3039fdf3300a7b37498e76d74c12ea6eec6
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 5a4632d14d5c87f9b77fd4d98cb15d00ee062b26c06ffe0cfb3ce30fabd82cd0

Exodus威胁情报

名称	分类	URL链接
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Places		https://reports.exodus-privacy.eu.org/trackers/69
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

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://khazanay-4df05.firebaseio.com"
"google_api_key" : "AIzaSyAargTSLAaQBmGZdT7dcRgjKUtnMAW0OAY"
"google_crash_reporting_api_key" : "AIzaSyAargTSLAaQBmGZdT7dcRgjKUtnMAW0OAY"
"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" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di atas."
"com_facebook_device_auth_instructions" : "Gehe zu facebook.com/device und gib den oben angezeigten Code ein."
"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."

可能的敏感信息
"com_facebook_device_auth_instructions" : "facebook.com/device ■■ ■■■■■■ ■■■■ ■■ ■■■ ■■■■■■ ■■■ ■■■ ■■■■■■"
"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 ■■■■ □■■■■■■ ■■■■■□ ■■■■■■■■■■■■■■■■■■ ■■■■■■ ■□■■■■"
"com_facebook_device_auth_instructions" : "Ga naar facebook.com/device en voer de bovenstaande code in."
"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 ■■■■■ ■■■■ ■■■■ ■■■■■■■■ ■■■■■■■■■ ■■■■■■■ ■■■■■■"
"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 ■■ ■■■■■ ■■■■■ ■■■■■ ■■■■■ ■■■■■■■■■■ ■■■■■■■ ■■■■ ■■■■■■■■■"
"com_facebook_device_auth_instructions" : "facebook.com/device□ □□□□ □ □□□ □□□□□."
"com_facebook_device_auth_instructions" : "تفضل بزيارة facebook.com/device وإدخال الرمز الموضح أعلاه."
"com_facebook_device_auth_instructions" : "Consultez facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "Posjetitw facebook.com/device i unesite gore prikazani kôd."

可能的敏感信息

"com_facebook_device_auth_instructions" : "facebook.com/device ■■■ ■■■■ ■■■ ■■■■ ■■■ ■■■■■■■■ ■■■■"
"com_facebook_device_auth_instructions" : "facebook.com/device adresine git ve yukarıda gösterilen kodu gir."
"com_facebook_device_auth_instructions" : "Přejděte na facebook.com/device a zadejte nahoře uvedený kód."
"com_facebook_device_auth_instructions" : "Ve a facebook.com/device e ingresa el código que se muestra arriba."
"com_facebook_device_auth_instructions" : "Lawati facebook.com/device dan masukkan kod yang ditunjukkan di atas."
"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" : "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" : "יש לבקר בכתובת facebook.com/device</b&gt ולהזין את הקוד המוצג למעלה"
"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。"

可能的敏感信息
"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 introduce el código que se muestra más arriba."
"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。"

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 VM check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
