MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Ace Scanner 2.13.0.APK

APP名称:	Ace Scanner
包名:	com.impressmedium.textscanner
域名线索:	0条
URL线索:	1条
邮箱线索:	0条
分析日期:	2022年2月2日 17:02

文件信息

文件名: acescanner589967.apk
文件大小: 8.47MB
MD5值: 08401291f093c4ddf78fadad70847f24
SHA1值: 6d6cb4f3bafeed4c1c4952e4ab00901917f361b7
SHA256值: af254146a5335a67527ec782174bd97b0446260f175e4729a6d61b0d9f174024

APP 信息

App名称: Ace Scanner
包名: com.impressmedium.textscanner
主活动**Activity:** com.impressmedium.textscanner.MainActivity
安卓版本名称: 2.13.0
安卓版本: 21300

URL线索

URL信息	Url所在文件

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

向手机申请的权限	是否危险	类型	详细情况
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.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_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
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。

向手机申请的权限	是否危险	类型	详细情况
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章

向手机申请的权限	是否危险	类型	详细情况
com.huawei.android.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
android.permission.READ_APP_BADGE	正常	显示应用程序通知	允许应用程序显示应用程序图标徽章
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.impressmedium.textscanner.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference

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: 2017-10-15 16:44:42+00:00
Valid To: 2047-10-15 16:44:42+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xb5dd4f2dcdc5abc2776031af61015a42dca99841
Hash Algorithm: sha256
md5: 40bcfe4002dc3cf4d82c2f06bde10232
sha1: 38c9a608334e3d8295bfa2ca76028b97a599ecb3
sha256: 4d7077ca48c0abc6c2dab0ad856b74b3a48cf7e2a305182570e99575195c4e92
sha512: b198d3fcb58c0bf6d541ad8807160f8168f06022063a7f456f70c3aed5b91743501a81e331a6044bde95be1946d00ed9f64ce192642ea73feec2d1c2a3fd4290
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: f0f269b3ee20b1d645a57e5c8816545d96f701df2bbfeaafbd1f0bfe3b90afd2

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

名称	分类	URL链接
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

🔑 硬编码敏感信息

可能的敏感信息
"billing_key_param" : "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtnr4TWQsu1Rkuj3B2qZ95QOVE68lKKuItEEzJISon+bKC3oT0+t9IDm+3hXI4Hm+v8xbFf0egX9zUstMqqY8SIZQC/LBk0mAS5MH8z3mfeOUXTW/znMpxDckYSms7O5/ITC7tXdrZ+dlfxQ9G7rIb+gTB36ep2QZuPUs8r+N7ZlYsVAF6zmDxaF7y7UeS5l8d8yDbEn6xEiPMpl0Svnx9N+Ub1MjCNqZogGLMYuMIjLHv3VhAxkbWQPWp7jYw7v/J4B+HiIGZgZeh8aMPs4FgONa//7hRb8b0aF7K2hniVnpsogkd9dnUgTj5ojVfdpvfXyFuox4CwOXFBZTVTnl1QIDAQAB"
"com_facebook_device_auth_instructions" : "Visit facebook.com/device and enter the code shown above."
"google_api_key" : "AIzaSyAXL5s0fVxu82biV1bhqZQst1CN2-N4Tok"
"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 '■■ ■■■■■ ■■■ ■■■ ■■■■ ■■■■■ ■■■ ■■■ ■■■■■ ■■■□"

可能的敏感信息
"com_facebook_device_auth_instructions" : "facebook.com/device ■■■ ■■■■■■■■■■■■,■■■■ ■■■■■■■■■■■ ■■■■■■■■■■ ■■■■■■■■■■■"
"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■■ ■■■■■■■■■■ ■■■■■ ■■■■■ ■■■■■■ ■■■■■ ■■■■■■■"
"com_facebook_device_auth_instructions" : "Besoek facebook.com/device en voer die kode wat hierbo gewys word, in."
"com_facebook_device_auth_instructions" : "■■■■■ facebook.com/device ■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"com_facebook_device_auth_instructions" : "Siirry osoitteeseen facebook.com/device ja anna oheinen koodi."
"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."

可能的敏感信息

"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."
"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."

可能的敏感信息
"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" : "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 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。"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.impressmedium.textscanner://,

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 Build.SERIAL check
network operator name check
possible VM check</td></tr>
<tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>编译器</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table>
</td></tr>
</table>
