MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

AllRewards 1.0.5.APK

APP名称:	AllRewards
包名:	ph.com.allrewards.android
域名线索:	3条
URL线索:	4条
邮箱线索:	0条
分析日期:	2022年1月25日 21:38

文件信息

文件名: allrewards560473.apk
文件大小: 2.79MB
MD5值: 730cd6b0687fc441fefe085d8aa68a20
SHA1值: d868221d33c184cca1a84cacd7109b43e5d09783
SHA256值: 4dd14718cdde5734aa4b088d7139aa701ffabb9975d1366676dfedb14cee4c5c

APP 信息

App名称: AllRewards
包名: ph.com.allrewards.android
主活动**Activity:** ph.com.allrewards.android.SplashActivity
安卓版本名称: 1.0.5
安卓版本: 6

域名线索

域名	是否危险域名	服务器信息
www.google.com	good	**IP:** 199.59.148.8 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
allrewardstest.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
allrewards.com.ph	good	**IP:** 198.54.116.253 所属国家: United States of America 地区: Georgia 城市: Atlanta 纬度: 33.727291 经度: -84.425377 查看地图: Google Map

URL线索

URL信息	Url所在文件
https://allrewards.com.ph/user-home.php	ph/com/allrewards/android/MainActivity.java
www.google.com	ph/com/allrewards/android/MainActivity.java
www.google.com	ph/com/allrewards/android/SplashActivity.java
https://allrewardstest.firebaseio.com	Android String Resource

数据库线索

FIREBASE链接地址	详细信息
https://allrewardstest.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
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.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	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: 2019-05-24 04:56:03+00:00
Valid To: 2049-05-24 04:56:03+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x6d5f2eecaa32174bf6c5ddc57b342d2d89cd01a6
Hash Algorithm: sha256
md5: dab11c69e334691ebd7cd5d04b3ca2f3
sha1: 7fda4ba5d18d4bf59e03685fbf9887d3e59026c0
sha256: c99a69a578499594637a246caa65250655d2e11f561d8b2f4b18ab34fa26da0b
sha512: 952c84f268c424e5d7ed4ba48dcff8e0c51299f78d310142c019985d0e6d8f2600a0b631d1ac5f35aa0bb367cfd0f0bb878e28da6491f7e749fe4f4b262ab75c
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: f3a6dd1d44ac8f00e39b56df4861c1e4d3586334f2ee6d2d1b0b9479cf54163f

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://allrewardstest.firebaseio.com"
"google_api_key" : "AIzaSyAl0u0-XuvAfiqIKWnPUbYnfzKs-7XyaKc"
"google_crash_reporting_api_key" : "AIzaSyAl0u0-XuvAfiqIKWnPUbYnfzKs-7XyaKc"
"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" : "Vizitează facebook.com/device şi introdu codul de mai sus."
"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."

可能的敏感信息

"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."
"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."

可能的敏感信息
"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.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.ph.com.allrewards.android,

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>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>
