MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Spotted 1.3.2.APK

APP名称:	Spotted
包名:	be.spotteds.app
域名线索:	7条
URL线索:	7条
邮箱线索:	1条
分析日期:	2022年1月28日 23:19

文件信息

文件名: spotted530409.apk
文件大小: 3.18MB
MD5值: 936b40954659cf565e6e4546330d23ee
SHA1值: b438df9ef7df241e34ef5506d025283ed7313310
SHA256值: 051aca40af8a9f97297e236579ccbe13888e0c7e9ad03a0bafc1da175f359ea1

APP 信息

App名称: Spotted
包名: be.spotteds.app
主活动**Activity:** io.flutter.embedding.android.FlutterActivity
安卓版本名称: 1.3.2
安卓版本: 18

域名线索

域名	是否危险域名	服务器信息
github.com	good	**IP:** 20.205.243.166 **所属国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看地图:** Google Map
schemas.android.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
pagead2.googlesyndication.com	good	**IP:** 220.181.174.230 **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
goo.gl	good	**IP:** 172.217.163.46 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map
developer.android.com	good	**IP:** 142.251.42.238 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map
app-measurement.com	good	**IP:** 220.181.174.225 **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
spotted-12f4c.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
http://schemas.android.com/apk/res/android	b/f/a/a/i.java
https://app-measurement.com/a	d/b/a/c/f/f/C0510kf.java
https://goo.gl/J1sWQy	d/b/a/c/f/f/C0473g.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	d/b/a/c/a/a/b.java
https://github.com/flutter/flutter/issues/2897).It	io/flutter/plugin/platform/n.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/f.java
https://spotted-12f4c.firebaseio.com	Android String Resource

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	d/b/a/c/d/v.java

数据库线索

FIREBASE链接地址	详细信息
https://spotted-12f4c.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.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

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: 2020-02-17 18:53:01+00:00
Valid To: 2050-02-17 18:53:01+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x4aec4e4ab27535747d893911a1dfc0daf5772b09
Hash Algorithm: sha256
md5: ddec79d5e4d01a7cda20df70ca62171b
sha1: adba90e467b66cb7d1dcabd7b64308bfa1696289
sha256: 9d4b813c09ebd817a6e216010aa129e6bec03864011b3443d09b77a87bc91189
sha512: de4dad4f5654f63bffabbca628da7b84584d907270cb0aac33a12b775f1a459249d7d294020213ca26ddb89fac8314decf40a191a3ed5fe4cc682bef3a85ada0
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: bb5c1e68d4f146e2209cc5e160773b3d136e902dd5bf2eff716b1d22ab585f41

Exodus威胁情报

名称	分类	URL链接
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
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://spotted-12f4c.firebaseio.com"
"google_api_key" : "AIzaSyAvCgXsOwvEdqYYrMIaZ1E66LitFfFnnR8"
"google_crash_reporting_api_key" : "AIzaSyAvCgXsOwvEdqYYrMIaZ1E66LitFfFnnR8"

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.flutter.embedding.android.FlutterActivity	Schemes: spotted://, https://, Hosts: spotteds.be,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.be.spotteds.app,

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
Build.TAGS check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
