MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Bee Todo 1.0.1.APK

APP名称:	Bee Todo
包名:	pub.hanks.bee.todo
域名线索:	10条
URL线索:	14条
邮箱线索:	2条
分析日期:	2022年2月2日 21:55

文件信息

文件名: mifenqd.apk
文件大小: 2.41MB
MD5值: c41f36185b672e7543787a97dd7151a6
SHA1值: eb2f7bc65a9c3393e634f35306c7f9a78b4f6244
SHA256值: 60208bb79e7d67e65d8f215d99c4cbfc229718964afcccac0d97505a7e8b5971

APP 信息

App名称: Bee Todo
包名: pub.hanks.bee.todo
主活动**Activity:** pub.hanks.beetodo.MainActivity
安卓版本名称: 1.0.1
安卓版本: 4

域名线索

域名	是否危险域名	服务器信息
app-measurement.com	good	**IP:** 220.181.174.33 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
firebase.google.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
goo.gl	good	IP: 172.217.160.110 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
pagead2.googlesyndication.com	good	IP: 220.181.174.166 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
hanks.pub	good	IP: 104.21.18.95 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
www.google.com	good	**IP:** 185.45.7.189 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London 纬度: 51.508530 经度: -0.125740 查看地图: Google Map
play.google.com	good	**IP:** 142.251.43.14 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
google.com	good	**IP:** 142.251.43.14 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
www.googleadservices.com	good	**IP:** 220.181.174.166 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
schemas.android.com	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://firebase.google.com/support/privacy/init-options.	f/c/b/p/e.java
https://app-measurement.com/a	f/c/a/a/e/c/bb.java
https://goo.gl/J1sWQy	f/c/a/a/e/c/l2.java
https://app-measurement.com/a	f/c/a/a/f/b/c3.java
https://firebase.google.com/support/guides/disable-analytics	f/c/a/a/f/b/g3.java
https://goo.gl/NAOOOI.	f/c/a/a/f/b/v9.java
https://goo.gl/NAOOOI	f/c/a/a/f/b/v9.java
https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s	f/c/a/a/f/b/x5.java
https://google.com/search?	f/c/a/a/f/b/t6.java
www.google.com	f/c/a/a/f/b/u6.java
https://www.google.com	f/c/a/a/f/b/u6.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	f/c/a/a/a/a/b.java
http://schemas.android.com/apk/res/android	d/h/c/b/h.java
http://hanks.pub/apps/redirect.html?type=	g/a/a/c.java

URL信息	Url所在文件
https://play.google.com/store/apps/details?id=	g/a/a/a.java
https://play.google.com/store/apps/details?id=${packageName}	g/a/a/a.java

邮箱线索

邮箱地址	所在文件
zhangyuhan2014@gmail.com	l/a/a/o.java
u0013android@android.com0 u0013android@android.com	f/c/a/a/b/v.java

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.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
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference

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.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: False
Found 1 unique certificates
Subject: C=100000, ST=bj, L=bj, O=z, OU=z, CN=z
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-07-05 06:51:27+00:00
Valid To: 2071-06-23 06:51:27+00:00
Issuer: C=100000, ST=bj, L=bj, O=z, OU=z, CN=z
Serial Number: 0x178a2e8f
Hash Algorithm: sha256
md5: 6de7f0491db220e64e09e8631794ffbb
sha1: c5420dd3307cc5de87550f022cf5ebe59ab5a088
sha256: 572103bcc6bef87a0d2d0e9c5d000a78758fb3b2b2e810e5052413c21af41976
sha512: 95411aab47e194e37212dc60fba4b3c9aa9d1cc1a6574960cb423222638ffa8173b0cbe483357544c4817f7360572d9077a7068a07837c9ef550b5d348f6cda2
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 2f5dfff77f2c2f9c3d08933fd321852f48fe1202c19242fd41cb00b4e4843af6

Exodus威胁情报

名称	分类	URL链接
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
"google_api_key" : "AIzaSyDc1-Y36LmUkOhy_-pc4Dol9K_jYkLbFZQ"
"google_crash_reporting_api_key" : "AIzaSyDc1-Y36LmUkOhy_-pc4Dol9K_jYkLbFZQ"

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 反虚拟机: Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check 编译器: r8