MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Snooker Scoreboard 0.0.6.APK

APP名称:	Snooker Scoreboard
包名:	com.yolo.snookerscoreboard
域名线索:	28条
URL线索:	36条
邮箱线索:	1条
分析日期:	2022年1月26日 19:43

文件信息

文件名: snookerscoreboard566765.apk
文件大小: 4.63MB
MD5值: 2bfd9d5d43e55192fc747b2467206b8e
SHA1值: 65f4c1627a8745b207a1559ed2dd9a865db218b5
SHA256值: 0e57a2bce4c2f3d29b0aba9738495d942bca215fca2564a9f30c49fbc677dff2

APP 信息

App名称: Snooker Scoreboard
包名: com.yolo.snookerscoreboard
主活动**Activity:** com.yolo.snookerscoreboard.MainActivity
安卓版本名称: 0.0.6
安卓版本: 6

域名线索

域名	是否危险域名	服务器信息
yolo.blue	good	**IP:** 172.67.201.178 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
docs.yolo.blue	good	IP: 199.36.158.100 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
developers.google.com	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
admob-gmats.uc.r.appspot.com	good	IP: 69.171.224.36 所属国家: United States of America 地区: California 城市: Menlo Park 纬度: 37.436935 经度: -122.193604 查看地图: Google Map
firebase.google.com	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

域名	是否危险域名	服务器信息
zhuanlan.zhihu.com	good	IP: 182.254.61.202 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
play.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
issuetracker.google.com	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
www.google.com	good	IP: 104.244.46.186 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
app-measurement.com	good	**IP:** 220.181.174.97 **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
googlemobileadssdk.page.link	good	**IP:** 172.217.160.78 **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
ns.adobe.com	good	没有服务器地理信息.
csi.gstatic.com	good	**IP:** 220.181.174.34 **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
exoplayer.dev	good	**IP:** 185.199.110.153 **所属国家:** United States of America **地区:** Pennsylvania **城市:** California **纬度:** 40.065632 **经度:** -79.891708 **查看地图:** Google Map

域名	是否危险域名	服务器信息
schemas.android.com	good	没有服务器地理信息.
google.com	good	IP: 59.24.3.174 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul 纬度: 37.568260 经度: 126.977829 查看地图: Google Map
support.google.com	good	IP: 172.217.160.78 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: 220.181.174.38 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
www.example.com	good	IP: 93.184.216.34 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.043720 经度: -77.487488 查看地图: Google Map

域名	是否危险域名	服务器信息
goo.gle	good	IP: 67.199.248.12 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.739288 经度: -73.984955 查看地图: Google Map
plus.google.com	good	IP: 75.126.33.156 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.939491 经度: -96.838730 查看地图: Google Map
reports.crashlytics.com	good	没有服务器地理信息.
googleads.g.doubleclick.net	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
update.crashlytics.com	good	IP: 220.181.174.226 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
goo.gl	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
firebase-settings.crashlytics.com	good	IP: 220.181.174.226 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
www.googleadservices.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
imasdk.googleapis.com	good	IP: 220.181.174.97 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

URL线索

URL信息	Url所在文件
https://update.crashlytics.com/spi/v1/platforms/android/apps	l0/d.java
https://update.crashlytics.com/spi/v1/platforms/android/apps/%s	l0/d.java
https://reports.crashlytics.com/spi/v1/platforms/android/apps/%s/reports	l0/d.java
https://reports.crashlytics.com/sdk-api/v1/platforms/android/apps/%s/minidumps	l0/d.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	k5/b.java
https://zhuanlan.zhihu.com/p/374922754	i9/d1.java
https://play.google.com/store/apps/details?id=com.yolo.snookerscoreboard	i9/d1.java
https://yolo.blue/	i9/a.java
https://developers.google.com/admob/android/test-ads#enable_test_devices	t/u.java
https://app-measurement.com/a	t6/v2.java
www.google.com	t6/w4.java
https://www.google.com	t6/w4.java
https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s	t6/p4.java
https://plus.google.com/	c6/a1.java

URL信息	Url所在文件
http://www.example.com	e/b.java
http://schemas.android.com/apk/res/android	l2/h.java
https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	c8/b.java
www.google.com	m5/p.java
https://app-measurement.com/a	p6/p9.java
https://goo.gl/J1sWQy	p6/r1.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	a3/p.java
https://support.google.com/dfp_premium/answer/7160685#push	o5/p.java
https://google.com/search?	k6/df.java
https://googlemobileadssdk.page.link/admob-interstitial-policies	k6/cp0.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	k6/g4.java
https://googlemobileadssdk.page.link/admob-interstitial-policies	k6/pk0.java
http://www.google.com	k6/b11.java
http://www.example.com	k6/b11.java
https://googlemobileadssdk.page.link/admob-android-update-manifest	k6/pn.java

URL信息	Url所在文件
https://googlemobileadssdk.page.link/ad-manager-android-update-manifest.	k6/pn.java
http://www.google.com	k6/c10.java
http://ns.adobe.com/xap/1.0/	k6/py1.java
https://csi.gstatic.com/csi	k6/sp.java
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html	k6/gq.java
https://developers.google.com/admob/android/test-ads#enable_test_devices	k6/xr0.java
https://googlemobileadssdk.page.link/admob-interstitial-policies	k6/qc0.java
http://www.example.com	k6/lp.java
https://exoplayer.dev/issues/cleartext-not-permitted	k6/vb.java
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/mraid/v3/mraid_app_banner.js	k6/to.java
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/mraid/v3/mraid_app_expanded_banner.js	k6/to.java
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/mraid/v3/mraid_app_interstitial.js	k6/to.java
https://www.google.com/dfp/linkDevice	k6/to.java
https://admob-gmats.uc.r.appspot.com/	k6/to.java
https://www.google.com/dfp/inAppPreview	k6/to.java

URL信息	Url所在文件
https://www.google.com/dfp/debugSignals	k6/to.java
https://www.google.com/dfp/sendDebugData	k6/to.java
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/native_ads.html	k6/to.java
https://imasdk.googleapis.com/admob/sdkloader/native_video.html	k6/to.java
https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html	k6/to.java
https://firebase.google.com/support/privacy/init-options.	a9/b.java
https://goo.gle/compose-feedback	f0/n.java
https://docs.yolo.blue/projects/snooker-scoreboard/privacy-policy/en.html	Android String Resource
https://docs.yolo.blue/projects/snooker-scoreboard/terms-and-conditions/en.html	Android String Resource
https://docs.yolo.blue/projects/snooker-scoreboard/privacy-policy/zh.html	Android String Resource
https://docs.yolo.blue/projects/snooker-scoreboard/terms-and-conditions/zh.html	Android String Resource

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	z5/t.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.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
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
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
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, CN=Lei Wang
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-06-14 13:38:50+00:00
Valid To: 2051-06-07 13:38:50+00:00
Issuer: C=CN, CN=Lei Wang
Serial Number: 0x592b44b0
Hash Algorithm: sha256
md5: 7d32fdd1876c1d8e6c325bf36a38c0e1
sha1: 5445cbea365503f3f1e142cbfd3e2c3912c05d1a
sha256: 9f99dd495c204e6c74e0fdee539d5a83423dbe04ac4be79bff7e7fe4369f46e2
sha512: c5fc08b659ee369fb736e9df20e3a5cb5b199ca03bc87da93f58e4e5ec580ab959020219153e6b1467ab9ff9a9e625ad00b29305a5f18dc93581d7963bb9514e
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: bcbfb240b1f53c6210286d6e1504e0cf492764a386c6f7c6644dcb27ab78ff1f

Exodus威胁情报

名称	分类	URL链接
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
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" : "AIzaSyDXid-rrKiVD3-9gGgpu6XRUEIWLQ7vHhA"
"google_crash_reporting_api_key" : "AIzaSyDXid-rrKiVD3-9gGgpu6XRUEIWLQ7vHhA"

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
Build.HARDWARE check
Build.TAGS check
SIM operator 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>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
