



MoGua

BOME 2.0.4.APK 分析报告



APP名称:

BOME

包名:	com.project.mkb
域名线索:	19条
URL线索:	17条
邮箱线索:	3条
分析日期:	2024年10月18日
分析平台:	摸瓜APK反编译平台

文件名: bome_204+(2).apk

文件大小: 33.98MB

MD5值: acaa866eebf25dc42fe2321e3628b85a

SHA1值: c502caf36973417b4adfbe2f289aaa94bcd6cc5e

SHA256值: e146e36f5658bfa9962694e3a85d8900ad65d2db73d64c7b42ccdf058e5b4399

i APP 信息

App名称: BOME

包名: com.project.mkb

主活动Activity: com.project.mkb.MainActivity

安卓版本名称: 2.0.4

安卓版本: 204

🔍 域名线索

域名	服务器信息
server.bomeapp.org	IP: 104.21.25.77 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
crash.163.com	IP: 45.254.50.146 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore

	<p>城市: Singapore 纬度: 1.289987 经度: 103.850281</p>
flutter.dev	<p>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</p>
docs.flutter.dev	<p>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</p>
ns.adobe.com	<p>没有服务器地理信息.</p>
wanproxy.127.net	<p>IP: 223.252.196.41 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572</p>
api.flutter.dev	<p>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</p>
server.bomeapp.net	<p>IP: 43.199.54.242 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692</p>

wannos.127.net	IP: 223.252.196.42 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
verify.dun.163.com	IP: 59.111.211.180 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
developer.android.com	IP: 142.250.69.206 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
da.dun.163.com	IP: 59.111.211.178 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City

	<p>纬度: 39.099731 经度: -94.578568</p>
issuetracker.google.com	<p>IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514</p>
dartbug.com	<p>IP: 216.239.36.21 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514</p>
www.unicode.org	<p>IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204</p>
223.252.196.38	<p>IP: 223.252.196.38 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572</p>

URL线索

URL信息	Url所在文件
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/g.java

http://wanproxy.127.net	com/netease/cloud/nos/yidun/monitor/MonitorConfig.java
https://wannos.127.net/lbs;https://wannos-hz.127.net/lbs;https://wannos-bj.127.net/lbs;https://wannos-oversea.127.net/lbs	com/netease/cloud/nos/yidun/core/AcceleratorConf.java
http://223.252.196.38/lbs	com/netease/cloud/nos/yidun/core/AcceleratorConf.java
https://wannos.127.net	com/netease/cloud/nos/yidun/core/AcceleratorConf.java
https://verify.dun.163.com/v1/liveperson/check	com/netease/nis/alivedetected/a.java
https://verify.dun.163.com/v1/liveperson/getConf	com/netease/nis/alivedetected/a.java
https://da.dun.163.com/sn.gif?d=	com/netease/nis/alivedetected/e/d.java
https://crash.163.com/uploadCrashLogInfo.do	com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java
https://crash.163.com/client/api/uploadStartUpInfo.do	com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java
https://crash.163.com/uploadCrashLogInfo.do	com/netease/nis/crashreport/BaseNdkHandler.java
https://crash.163.com/client/api/uploadStartUpInfo.do	com/netease/nis/crashreport/BaseNdkHandler.java
https://docs.flutter.dev/deployment/android	o2/d.java
https://github.com/Baseflow/flutter-permission-handler/issues	t0/u.java
https://developer.android.com/reference/com/google/android/play/core/install/model/InstallErrorCode	q1/a.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	v/m.java
http://ns.adobe.com/xap/1.0/\u0000	a0/a.java
https://github.com/nodeca/pica	摸瓜V2引擎

http://www.unicode.org/copyright.html	lib/arm64-v8a/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	lib/arm64-v8a/libflutter.so
https://github.com/flutter/flutter/issues	lib/arm64-v8a/libflutter.so
https://dartbug.com/52121	lib/arm64-v8a/libflutter.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://server.bomeapp.net	lib/armeabi-v7a/libapp.so
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android	lib/armeabi-v7a/libapp.so
https://server.bomeapp.org	lib/armeabi-v7a/libapp.so
http://www.unicode.org/copyright.html	lib/armeabi-v7a/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues	lib/armeabi-v7a/libflutter.so
https://dartbug.com/52121	lib/armeabi-v7a/libflutter.so
http://www.unicode.org/copyright.html	lib/x86_64/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	lib/x86_64/libflutter.so
https://github.com/flutter/flutter/issues	lib/x86_64/libflutter.so
https://dartbug.com/52121	lib/x86_64/libflutter.so

✉ 邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libflutter.so
authenticationscheme@13463476.fromstring _list@0150898.of _httparser@13463476.responsepa _list@0150898.generate _typeerror@0150898._create storationinformation@265124995.fromserial _list@0150898._ofgrowabl _list@0150898._ofefficie _compressednode@78137193.single _growablelist@0150898._ofarray _double@0150898.fromintege _growablelist@0150898._literal3 _future@4048458.immediate t@gmail.com _growablelist@0150898._literal _assetmanifestbin@30287047.fromstanda _growablelist@0150898._ofother _link@14069316.fromrawpat _growablelist@0150898.withcapaci _timer@1026248._internal _growablelist@0150898._literal6 _growablelist@0150898._literal5 _receiveportimpl@1026248.fromrawrec _imagefilter@15065589.composed _list@0150898._ofarray _timer@1026248.periodic _hashcollisionnode@78137193.fromcollis _growablelist@0150898._literal2 _list@0150898.empty _list@0150898._ofother _bytebuffer@7027147._new _directory@14069316.fromrawpat	lib/armeabi-v7a/libapp.so

_invocationmirror@0150898._withtype ngstreamssubscription@4048458.zoned _assertionerror@0150898._create _nativesocket@14069316.normal _colorfilter@15065589.lineartosr _imagefilter@15065589.fromcolorf _colorfilter@15065589.srgbtoline _growablelist@0150898._literal1 _uri@0150898.file _uri@0150898.directory _imagefilter@15065589.blur _growablelist@0150898._literal8 _file@14069316.fromrawpat _growablelist@0150898._literal4 _growablelist@0150898._ofgrowabl _growablelist@0150898.of _growablelist@0150898.generate _uri@0150898.notsimple _growablelist@0150898._literal7 _future@4048458.zonevalue _growablelist@0150898._ofefficie _future@4048458.immediatee	
appro@openssl.org	lib/x86_64/libflutter.so

手机线索

签名证书

APK已签名

v1 签名: True

v2 签名: True

v3 签名: False

找到 1 个唯一证书

主题: CN=Android Debug, O=Android, C=US

签名算法: rsassa_pkcs1v15

有效期自: 2024-03-05 03:24:11+00:00

有效期至: 2054-02-26 03:24:11+00:00

发行人: CN=Android Debug, O=Android, C=US

序列号: 0x1

哈希算法: sha256

md5值: c1c4a5b32ebd07b12e63638cc8f97445

sha1值: feefb7ef05c82e26ad6df04bfd4e7a07f8b4c64c

sha256值: db3dfa9f6a245a65e345c6b0730c964b29006f34eb4e22927008ad49d72fad4f

sha512值: ed0af7d8bd64571796cc494d42e7df71c7a17d8d3dc5de60ef69a1a772b2b3d39a85f14685eadb359b1f3fa51722c966b5c71a84e15021d14a819fa18f601e6b

公钥算法: rsa

密钥长度: 2048

指纹: b7cbe703226eccc226a436a51769530afb88b90e886b2fd5f7330e30467b597c

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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.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.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
com.project.mkb.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。