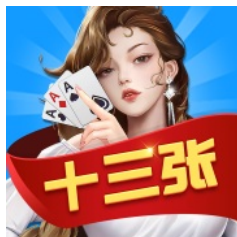




MoGua

财神十三张 1.0.4.APK 分析报告



APP名称:

财神十三张

包名:

com.hbl.caishen

域名线索:

75条

URL线索:	49条
邮箱线索:	1条
分析日期:	2025年4月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: caishen-website.apk
文件大小: 208.47MB
MD5值: 2193113d477c467d94716f2ebc2f5b24
SHA1值: 77496a2efa8cfcef3556dcd6b0093f9fa48daf12
SHA256值: ab7551b26c78a1e23a381e4c7b97ff7fd175303b1ca82a8151eb6b875d667a87

APP 信息

App名称: 财神十三张
包名: com.hbl.caishen
主活动Activity: com.cocos.game.AppActivity
安卓版本名称: 1.0.4

🔍 域名线索

域名	服务器信息
stuartk.com	IP: 99.83.231.61 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
alogsus.umeng.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
ai.login.umeng.com	IP: 59.82.31.154 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
oss.caishen13.com	IP: 47.106.74.31 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545673 经度: 114.068108
www.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
mobilegw.alipaydev.com	IP: 110.75.132.131 所属国家: China 地区: Zhejiang

	<p>城市: Hangzhou 纬度: 30.293650 经度: 120.161583</p>
jsperf.com	<p>IP: 104.16.227.18 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203</p>
www.w3.org	<p>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</p>
github.com	<p>IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281</p>
open.weixin.qq.com	<p>IP: 116.128.169.212 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948</p>
aspect-upush.umeng.com	<p>IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992</p>
h5.m.taobao.com	<p>IP: 125.39.135.147 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102</p>
	<p>IP: 223.109.148.178</p>

alogus.umeng.com	所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
mmbiz.qpic.cn	IP: 180.95.234.213 所属国家: China 地区: Gansu 城市: Lanzhou 纬度: 36.056690 经度: 103.792221
tools.ietf.org	IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
mobilegwpre.alipay.com	IP: 110.75.138.35 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
ttwhhttp.caishen13.com	IP: 121.40.69.50 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
ttwhhttp.caishentw.com	IP: 121.40.69.50 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
ccs.umeng.com	IP: 36.143.252.41 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

long.open.weixin.qq.com	IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
utoken.umeng.com	IP: 223.109.148.139 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
ttwhhttp.caishen.ai	IP: 121.41.17.113 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
sss.umeng.com	IP: 59.82.31.95 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mobile.umeng.com	IP: 59.82.31.210 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mcbgw.alipay.com	IP: 123.125.216.191 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501

	经度: 116.397102
api.weixin.qq.com	IP: 112.65.193.153 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
www.cocos.com	IP: 218.11.0.24 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
ofk4hc.xze589.com	IP: 60.28.220.199 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
purl.eligrey.com	IP: 104.236.163.66 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418
crbug.com	IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
guonei.xm6822.com	IP: 222.134.1.30 所属国家: China 地区: Shandong 城市: Binzhou 纬度: 37.366619 经度: 118.015182
	IP: 123.125.216.191 所属国家: China

wappaygw.alipay.com	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
cdn.jsdelivr.net	IP: 104.18.186.31 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
game.caishen.ai	IP: 113.6.79.154 所属国家: China 地区: Heilongjiang 城市: Suihua 纬度: 46.640614 经度: 126.996925
dragonbones.com	IP: 121.36.48.123 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
developer.umeng.com	IP: 59.82.60.44 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
h.trace.qq.com	IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi 纬度: 30.204170 经度: 115.077606
git.io	IP: 199.16.156.39 所属国家: United States of America 地区: Georgia 城市: Atlanta 纬度: 33.770844 经度: -84.377632

mobilegw.alipay.com	IP: 203.209.250.8 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
log.umsns.com	IP: 59.82.31.95 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
oss01.caishen13.com	IP: 116.142.235.206 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
192.168.9.151	IP: 192.168.9.151 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
www.apple.com	IP: 184.25.87.45 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul 纬度: 37.566311 经度: 126.977203
plbslog.umeng.com	IP: 36.156.202.78 所属国家: China 地区: Jiangsu 城市: Yangzhou 纬度: 32.397221 经度: 119.435600
ucc.umeng.com	IP: 203.119.169.82 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583

ulogs.umengcloud.com	IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
pre-c.umsns.com	IP: 203.119.204.32 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
www.caishen.ai	IP: 8.134.84.212 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
cgi.qplus.com	没有服务器地理信息.
eligrey.com	IP: 104.236.163.66 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418
imgcache.qq.com	IP: 42.231.138.50 所属国家: China 地区: Henan 城市: Nanyang 纬度: 32.994720 经度: 112.532784
nodejs.org	IP: 104.20.3.6 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
	IP: 59.82.31.210

c.umsns.com	所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mobilegw.dl.alipaydev.com	IP: 110.75.132.25 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mmocgame.qpic.cn	IP: 119.188.174.57 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
rxfile.xze589.com	没有服务器地理信息.
deeplink.umeng.com	IP: 59.82.112.112 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
appsupport.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
cgi.connect.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
www.umeng.com	IP: 59.82.31.95 所属国家: China 地区: Zhejiang 城市: Hangzhou

	纬度: 30.293650 经度: 120.161583
graph.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
ulogs.umeng.com	IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
loggw-exsdk.alipay.com	IP: 119.42.231.59 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
dom.spec.whatwg.org	IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
openmobile.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
render.alipay.com	IP: 122.156.129.94 所属国家: China 地区: Heilongjiang 城市: Heihe 纬度: 50.266670 经度: 127.466667
	IP: 185.199.108.133 所属国家: United States of America

raw.github.com	地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
stuk.github.io	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
www.saxproject.org	IP: 204.68.111.100 所属国家: United States of America 地区: California 城市: San Diego 纬度: 32.799797 经度: -117.137047
heycam.github.io	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
ttwhhttp.bangmangerp.com	没有服务器地理信息.
pslog.umeng.com	IP: 59.82.29.249 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mclient.alipay.com	IP: 116.142.235.203 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
oauth2.umeng.com	IP: 59.82.31.210 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650

URL线索

URL信息	Url所在文件
https://mobilegw.alipay.com/mgw.htm	b/a/a/c/w/a.java
https://mobilegw.alipaydev.com/mgw.htm	b/a/a/c/w/a.java
https://mobilegw.dl.alipaydev.com/mgw.htm	b/a/a/c/w/a.java
https://mcgw.alipay.com/sdklog.do	b/a/a/c/w/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	b/a/a/c/w/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	b/a/a/c/w/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	b/a/a/c/w/a.java
https://h5.m.taobao.com/mlapp/olist.html	b/a/a/c/y/a.java
https://mobilegwpre.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/b.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java

https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
https://www.caishen.ai/	com/cocos/game/MarketUtils.java
https://openmobile.qq.com/oauth2.0/me	com/tencent/connect/UnionInfo.java
https://cgi.qplus.com/report/report	com/tencent/connect/avatar/ImageActivity.java
https://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/connect/common/BaseApi.java
https://imgcache.qq.com/ptlogin/static/qzsjump.html?	com/tencent/connect/common/BaseApi.java
https://imgcache.qq.com/ptlogin/static/qzsjump.html?	com/tencent/connect/auth/a.java
https://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/v3/user/get_info	com/tencent/connect/auth/AuthAgent.java
https://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/user/user_login_statis	com/tencent/connect/auth/AuthAgent.java
https://imgcache.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/SocialApiml.java
https://imgcache.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/SocialApiml.java
https://imgcache.qq.com	com/tencent/open/SocialApiml.java
https://imgcache.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApiml.java
https://openmobile.qq.com/cgi-bin/qunopensdk/check_group	com/tencent/open/SocialOperation.java
https://openmobile.qq.com/cgi-bin/qunopensdk/unbind	com/tencent/open/SocialOperation.java
https://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utills/i.java
https://openmobile.qq.com/	com/tencent/open/utills/HttpUtils.java
https://appsupport.qq.com/cgi-bin/appstage/mstats_batch_report	com/tencent/open/b/h.java

https://h.trace.qq.com/kv	com/tencent/open/b/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s×tamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.java
https://aspect-upush.umeng.com/occa/v1/event/report	com/umeng/analytics/pro/an.java
https://ucc.umeng.com/v2/inn/fetch	com/umeng/analytics/pro/ao.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://developer.umeng.com/docs/119267/detail/182050	com/umeng/commonsdk/debug/UMLogCommon.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://alogus.umeng.com	com/umeng/commonsdk/stateless/a.java
https://log.umsns.com/	com/umeng/socialize/common/SocializeConstants.java
https://log.umsns.com/link/qq/download/	com/umeng/socialize/common/SocializeConstants.java
https://log.umsns.com/link/weixin/download/	com/umeng/socialize/common/SocializeConstants.java
http://www.umeng.com/social	com/umeng/socialize/common/SocializeConstants.java

https://c.umsns.com/ulink/getRTC	com/umeng/socialize/tracker/a.java
https://pre-c.umsns.com/ulink/getRTC	com/umeng/socialize/tracker/a.java
https://mobile.umeng.com/images/pic/home/social/img-1.png	com/umeng/socialize/net/LinkcardRequest.java
https://log.umsns.com/	com/umeng/socialize/net/base/SocializeRequest.java
https://ai.login.umeng.com/api/umed/event	com/umeng/socialize/net/analytics/SocialAnalytics.java
http://log.umsns.com/link/qq/download/	com/umeng/socialize/handler/QZoneSsoHandler.java
https://api.weixin.qq.com/sns/userinfo?access_token=	com/umeng/socialize/handler/UMWXHandler.java
https://api.weixin.qq.com/sns/oauth2/access_token?	com/umeng/socialize/handler/UMWXHandler.java
https://oauth2.umeng.com/oauth/token/acquire?	com/umeng/socialize/handler/UMWXHandler.java
https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=	com/umeng/socialize/handler/UMWXHandler.java
http://log.umsns.com/link/weixin/download/	com/umeng/socialize/handler/UMWXHandler.java
https://graph.qq.com/oauth2.0/me?access_token=	com/umeng/socialize/handler/UMQSSoHandler.java
https://ccs.umeng.com/sa	com/umeng/socialize/a/a.java
https://sss.umeng.com/api/v2/al	com/umeng/socialize/a/a.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/socialize/utills/UrlUtil.java
https://log.umsns.com/	com/umeng/socialize/view/OauthDialog.java
https://utoken.umeng.com	com/umeng/umzid/ZIDManager.java
https://deeplink.umeng.com/deeplink/match	com/umeng/umlink/MobclickLink.java
https://deeplink.umeng.com/deeplink/deviceFingerprint	com/umeng/umlink/MobclickLink.java
http://jsperf.com/call-apply-segu	摸瓜V2引擎
http://eligrey.com	摸瓜V2引擎

https://github.com/dsamarin	摸瓜V2引擎
https://github.com/eligrey/Blob.js/blob/master/LICENSE.md	摸瓜V2引擎
http://purl.eligrey.com/github/Blob.js/blob/master/Blob.js	摸瓜V2引擎
https://dom.spec.whatwg.org/	摸瓜V2引擎
https://heycam.github.io/webidl/	摸瓜V2引擎
https://tools.ietf.org/html/rfc7230	摸瓜V2引擎
https://github.com/taylorhakes	摸瓜V2引擎
https://github.com/taylorhakes/promise-polyfill/blob/master/LICENSE	摸瓜V2引擎
https://cdn.jsdelivr.net/npm/promise-polyfill@8/dist/polyfill.js	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/helpers/DefaultHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ContentHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ErrorHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ext/LexicalHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ext/DeclHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ext/EntityResolver2.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/DTDHandler.html	摸瓜V2引擎
https://www.cocos.com/	摸瓜V2引擎
http://www.cocos.com	摸瓜V2引擎
https://ttwhhttp.caishen.ai/	摸瓜V2引擎
https://ttwhhttp.bangmangerp.com/	摸瓜V2引擎
http://ttwhhttp.bangmangerp.com/	摸瓜V2引擎

http://192.168.9.151	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
https://rxfile.xze589.com/share/2022/12/12/freeroompoker_1670814224050.jpg	摸瓜V2引擎
https://git.io/jvFET	摸瓜V2引擎
http://stuartk.com/jszip	摸瓜V2引擎
https://raw.githubusercontent.com/Stuk/jszip/main/LICENSE.markdown	摸瓜V2引擎
https://github.com/nodeca/pako/blob/main/LICENSE	摸瓜V2引擎
https://stuk.github.io/jszip/documentation/howto/read_zip.html	摸瓜V2引擎
https://github.com/cocos-creator/engine/blob/develop/EngineErrorMap.md	摸瓜V2引擎
http://dragonbones.com/\nSource	摸瓜V2引擎
https://github.com/DragonBones/	摸瓜V2引擎
https://github.com/DragonBones/Tools/	摸瓜V2引擎
https://github.com/imaya/zlib.js	摸瓜V2引擎
https://ofk4hc.xze589.com/static/service	摸瓜V2引擎
https://www.caishen.ai	摸瓜V2引擎
https://oss01.caishen13.com/logo256-256(1).png	摸瓜V2引擎
http://127.0.0.1:8000/add_result?	摸瓜V2引擎
https://mmbiz.qpic.cn/sz_mmbiz_jpg/gZVPV3OJwygRehAzWQdh75XhVXjicUHJ6b5oQ9rfptW7rlc5JfjoOiatriciba5EC6djFia419Q3dOVzK5WovUZ1Mldw/0	摸瓜V2引擎
https://mmbiz.qpic.cn/sz_mmbiz_jpg/gZVPV3OJwygRehAzWQdh75XhVXjicUHJ6wH4ZkLdR0nYC8DwelUj8KiaycKH2R4xj6bTgrycd6ricoKT1Ria5tIVaA/0	摸瓜V2引擎
https://mmocgame.qpic.cn/wechatgame/gZhjxc9qfQdw9HraNqaLYb56AicnXB8vvOoJKs9VNQ0gpNUyBIROdhTJ4uY4TyicEO/0	摸瓜V2引擎
https://ofk4hc.xze589.com	摸瓜V2引擎

https://ttwhhttp.caishenttw.com/	摸瓜V2引擎
https://ttwhhttp.caishen13.com/	摸瓜V2引擎
https://oss01.caishen13.com/com	摸瓜V2引擎
https://oss.caishen13.com/com	摸瓜V2引擎
https://game.caishen.ai/com	摸瓜V2引擎
https://guonei.xm6822.com/native/ios/	摸瓜V2引擎
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/x86/libcocos.so
https://nodejs.org/static/favicon.ico	lib/x86/libcocos.so
https://nodejs.org/en/docs/inspector	lib/x86/libcocos.so
https://crbug.com/v8/8520	lib/x86/libcocos.so
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/armeabi-v7a/libcocos.so
https://nodejs.org/static/favicon.ico	lib/armeabi-v7a/libcocos.so
https://nodejs.org/en/docs/inspector	lib/armeabi-v7a/libcocos.so
https://crbug.com/v8/8520	lib/armeabi-v7a/libcocos.so

✉ 邮箱线索

邮箱地址	所在文件
jhruby.web@gmail.com	摸瓜V2引擎

☰ 手机线索

--	--

手机号	所在文件
17179869184	摸瓜V2引擎
16640753482	摸瓜V2引擎
14159265359	摸瓜V2引擎
15915494309	摸瓜V2引擎

🌸 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=cs, OU=hbl, O=hbl, L=xm, ST=xm, C=CN

签名算法: rsassa_pkcs1v15

有效期自: 2023-09-06 05:53:56+00:00

有效期至: 2053-08-29 05:53:56+00:00

发行人: CN=cs, OU=hbl, O=hbl, L=xm, ST=xm, C=CN

序列号: 0x1

哈希算法: sha256

md5值: 4d5bbba78d35a3aafd99a186c0586204

sha1值: a794de1afb29c1237a1bc1d04aa1c99ae2a42ac8

sha256值: c1a65e9ccb0bcacb84cad711f15ea966405c4a08f46576a5ecc58684cb6217ab

sha512值: fc3ee09ec5992f07433d1e888d42eaeafc49fe882116a38b35c809434358635c3a60c723f5da5d3bf96f7ff488af086ea2b8a31440153c1836d83db6b24a1739

公钥算法: rsa

密钥长度: 2048

指纹: bcd5261aeca839260b9771e294f28d963baea52f0189205f46f5bd296a63d0e8

🔑 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.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
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.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.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
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置(如果可用)。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位 (GPS)	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.BATTERY_STATS	合法	修改电池统计信息	允许修改收集的电池统计信息。不供普通应用程序使用

android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
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
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.cocos.game.AppActivity	Schemes: cs://, Hosts: com.hbl.caishen,
com.tencent.tauth.AuthActivity	Schemes:.tencent102070035://,

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。