MoGua

众腾 2.1.0.APK 分析报告

APP名称:	众腾
包名:	plus.H5E1611EE
域名线索:	77条
URL线索:	32条
邮箱线索:	1条
分析日期:	2025年1月24日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: Zhongteng.apk
文件大小: 17.39MB
MD5值: 75f742e5033b51b12eabe7bf469f22e9
SHA1值: 2d0eb231890d3ae1c56526372949a4e36ff3d089
SHA256值: 942087f8b87f3c3d77d3995f2f0d467192e6edd833c487bd6de119ebfa9b3556

APP 信息

App名称: 众腾
包名: plus.H5E1611EE
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 2.1.0
安卓版本: 210

域名线索

域名	服务器信息
socket.zt82.vip	没有服务器地理信息.
npms.io	**IP**: 104.21.64.1 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
g.alicdn.com	**IP**: 125.38.11.59 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
socket.zt66.org	**IP**: 104.21.27.59 **所属国家**: United States of America **地区**: California **城市**: San Francisco

	纬度: 37.775700 **经度**: -122.395203
m3w.cn	IP: 124.163.195.101 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
momentjs.com	IP: 104.16.32.155 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
login.greenjade88.com	IP: 113.212.181.210 **所属国家**: Philippines **地区**: National Capital Region **城市**: Manila **纬度**: 14.604200 **经度**: 120.982201
www.gamblingtherapy.org	IP: 80.82.114.233 **所属国家**: United Kingdom of Great Britain and Northern Ireland **地区**: England **城市**: Manchester **纬度**: 53.480949 **经度**: -2.237430
android.googlesource.com	IP: 74.125.135.82 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
cube.meituan.com	IP: 101.236.69.20 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.zt66.org	IP: 172.67.169.6 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
data-api.binance.vision	IP: 57.180.121.33 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
zt.cdn.84dns.com	没有服务器地理信息.
	IP: 34.104.35.123 **所属国家**: United States of America

edgedl.me.gvt1.com	**地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
img01.yzcdn.cn	IP: 27.221.54.107 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
underscorejs.org	IP: 172.67.134.18 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
en.wikipedia.org	IP: 103.102.166.224 **所属国家**: United States of America **地区**: Indiana **城市**: Francisco **纬度**: 38.333290 **经度**: -87.447083
github.com	IP: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
lodash.com	IP: 52.76.120.174 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
schemas.android.com	没有服务器地理信息.
acjs.aliyun.com	IP: 203.119.145.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
wikipredia.net	IP: 104.21.6.223 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
feross.org	IP: 50.116.11.184 **所属国家**: United States of America **地区**: California **城市**: Fremont **纬度**: 37.548271 **经度**: -121.988571
	IP: 101.34.244.49

t1.dcloud.net.cn	**所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
static.sanbanye.com	IP: 83.229.44.135 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
api.zt82.vip	IP: 61.147.96.188 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221 **经度**: 119.435600
h5.zt66.win	IP: 156.59.152.141 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
solscan.io	IP: 104.22.53.159 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
raydium.io	IP: 93.179.102.140 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.043240 **经度**: -118.250916
www.galottery.com	IP: 151.101.91.52 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
baike.baidu.com	IP: 111.206.208.229 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
s.tradingview.com	IP: 128.242.240.157 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
	IP: 180.178.32.2

api.zt88.win	**所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
etherscan.io	IP: 154.83.14.134 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
service.hshsin.com	IP: 104.21.112.1 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.taiwanlottery.com	IP: 104.244.43.6 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
gac1.dcloud.net.cn	IP: 124.223.210.113 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.zt88888.com	IP: 104.21.17.13 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
zh.wikipedia.org	IP: 103.102.166.224 **所属国家**: United States of America **地区**: Indiana **城市**: Francisco **纬度**: 38.333290 **经度**: -87.447083
sdk.api.oaid.wocloud.cn	没有服务器地理信息.
tronscan.org	IP: 172.66.43.46 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
bscscan.com	IP: 172.67.72.93 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

g.alicdn.com.danuoyi.alicdn.com	IP: 125.38.11.59 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
f.m.suning.com	IP: 202.108.15.155 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
na61-na62.wagbridge.alibaba.aliyun.com.gds.alibabadns.com	IP: 203.119.145.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.zt66.win	IP: 156.59.152.141 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
st-tw.maitoo998.com	没有服务器地理信息.
api.m.taobao.com	没有服务器地理信息.
ask.dcloud.net.cn	IP: 220.194.123.111 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
m1.openfpcdn.io	IP: 99.84.55.31 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
popular.gitbook.io	IP: 172.64.147.209 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
xg-def-cn.xcdn.global	IP: 89.187.160.82 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
	IP: 104.233.161.49 **所属国家**: United States of America **地区**: California

api.zt00.win	**城市**: San Jose **纬度**: 37.333698 **经度**: -121.889297
www.opap.gr	IP: 184.29.238.153 **所属国家**: United Arab Emirates **地区**: Dubayy **城市**: Dubai **纬度**: 25.258471 **经度**: 55.304722
www.xarg.org	IP: 185.244.195.154 **所属国家**: Germany **地区**: Baden-Wurttemberg **城市**: Karlsruhe **纬度**: 49.004719 **经度**: 8.385830
m.baidu.com	IP: 110.242.71.103 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
guoneia.starlinkdp.top	没有服务器地理信息.
images.b728484.com	IP: 216.225.165.167 **所属国家**: United States of America **地区**: California **城市**: Westlake Village **纬度**: 34.192921 **经度**: -118.822617
1119378012870022401.zga.globalconnetct.com	IP: 156.59.152.141 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
gac2.dcloud.net.cn	IP: 124.222.75.101 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
sgm-m.jd.com	IP: 111.206.227.216 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ns.adobe.com	没有服务器地理信息.
er.dcloud.io	没有服务器地理信息.
bgac.dcloud.net.cn	IP: 43.135.130.85 **所属国家**: United States of America **地区**: California **城市**: Santa Clara

	纬度: 37.354111 **经度**: -121.955490
www.playnow.com	IP: 23.55.107.19 **所属国家**: United States of America **地区**: Florida **城市**: Miami **纬度**: 25.774269 **经度**: -80.193604
fpjs.dev	IP: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
element.eleme.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
openjsf.org	IP: 76.76.21.21 **所属国家**: United States of America **地区**: California **城市**: Walnut **纬度**: 34.015400 **经度**: -117.858223
www.gstatic.com	IP: 203.208.39.194 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
er.dcloud.net.cn	IP: 43.142.57.168 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
zenorocha.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.taiwanlottery.com.tw	IP: 34.80.76.78 **所属国家**: Taiwan (Province of China) **地区**: Taipei **城市**: Taipei **纬度**: 25.038172 **经度**: 121.563599
apps.apple.com	IP: 121.22.227.5 **所属国家**: China **地区**: Hebei **城市**: Qinhuangdao **纬度**: 39.932541

	经度: 119.588226
popular1.blob.core.windows.net	IP: 20.60.200.161 **所属国家**: Korea (Republic of) **地区**: Seoul-teukbyeolsi **城市**: Seoul **纬度**: 37.566311 **经度**: 126.977203
s1.dcloud.net.cn	IP: 122.51.205.36 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.w3.org	IP: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
atlas-postgraphile.public.main.prod.cldev.sh	没有服务器地理信息.

URL线索

URL信息
http://ns.adobe.com/xap/1.0/\u0000
https://m3w.cn/s/
https://ask.dcloud.net.cn/article/282
https://er.dcloud.io/sc
https://er.dcloud.net.cn/sc
https://ask.dcloud.net.cn/article/35058
https://er.dcloud.io/rv
https://er.dcloud.net.cn/rv
https://ask.dcloud.net.cn/article/35627
https://ask.dcloud.net.cn/article/35877
https://ask.dcloud.net.cn/article/283
https://ask.dcloud.net.cn/article/287
http://schemas.android.com/apk/res/android
http://schemas.android.com/apk/res/android

http://schemas.android.com/apk/res/android
https://ask.dcloud.net.cn/article/36199
https://etherscan.io/'
https://etherscan.io/
https://tronscan.org/
https://bscscan.com/'
https://bscscan.com/
https://www.taiwanlottery.com/lotto/result/bingo_bingo'
https://www.taiwanlottery.com/lotto/result/bingo_bingo
https://en.wikipedia.org/wiki/British_Columbia_Lottery_Corporation
https://www.playnow.com/keno/winning-numbers/'
https://www.playnow.com/keno/winning-numbers/
https://www.galottery.com/en-us/games/draw-games/keno.html
https://en.wikipedia.org/wiki/OPAP'
https://en.wikipedia.org/wiki/OPAP
https://www.opap.gr/en/kino-draw-results'
https://www.opap.gr/en/kino-draw-results
https://baike.baidu.com/item/
https://www.opap.gr/en/super3-draw-results'
https://www.opap.gr/en/super3-draw-results
https://zh.wikipedia.org/zh-hans/%E4%BB%A5%E5%A4%AA%E5%9D%8A
https://zh.wikipedia.org/zh-hans/%E6%B3%A2%E5%A0%B4
https://zh.wikipedia.org/zh-my/%E5%B9%A3%E5%AE%89
https://en.wikipedia.org/wiki/Chainlink_(blockchain)
https://zh.wikipedia.org/wiki/%E5%8F%B0%E7%81%A3%E5%BD%A9%E5%88%B8
https://en.wikipedia.org/wiki/OPAP
https://wikipredia.net/zh/Georgia_Lottery
https://atlas-postgraphile.public.main.prod.cldev.sh/graphql

https://m.baidu.com/from=1000969a/s?word=%E8%B0%B7%E6%AD%8C%E8%BA%AB%E4%BB%BD%E9%AA%8C%E8%AF%81%E5%99%A8%E4%B8%8B%E8%BD%BD&sa=tb&ts=1542211&t_kt=0&ie=utf-8&rsv_t=33e70%252FJVhUh23eFAV799X70L28RJtVITm188tQZFszJDGtxExkUVonzZatCFP3E&rsv_pq=10879009814157754031&ss=100&tj=1&rqlang=zh&rsv_sug4=5057&inputT=3529&oq=guge%E8%BA%AB%E4%BB%BD%E9%AA%8C%E8%AF%81%E5%99%A8%E4%B8%8B%E8%BD%BD
https://fpjs.dev/pro
https://m1.openfpcdn.io/fingerprintjs/v
https://api.zt66.win/public/last_version
https://popular1.blob.core.windows.net/statics/apk/GoogleAuthenticator.apk
https://apps.apple.com/cn/app/google-authenticator/id388497605
https://fpjs.dev/pro
https://m1.openfpcdn.io/fingerprintjs/v
https://h5.zt66.win
https://www.zt88888.com/
https://solscan.io/tx/
https://solscan.io/account/
https://raydium.io/
https://cube.meituan.com/ipromotion/cube/toc/component/base/getServerCurrentTime
https://sgm-m.jd.com/h5/
https://api.m.taobao.com/rest/api3.do?api=mtop.common.getTimestamp
https://f.m.suning.com/api/ct.do
https://www.gamblingtherapy.org
https://service.hshsin.com/chatIndex?ent_id=14
https://images.b728484.com:42666/TCG_GAME_ICONS/
https://s.tradingview.com/widgetembed/?frameElementId=tradingview_b239c&symbol=BINANCE%3ABTCUSDT&interval=5&hidesidetoolbar=0&symboledit=1&saveimage=1&toolbarbg=f1f3f6&studies=%5B%5D&theme=light&style=1&studies_overrides=%7B%7D&overrides=%7B%7D&enabled_features=%5B%22header_fullscr
https://popular.gitbook.io/popular/prediction
https://popular1.blob.core.windows.net/statics/zhongteng/gameIcon/wap/
https://popular1.blob.core.windows.net/statics/common/media/dida.mp3
https://popular1.blob.core.windows.net/statics/common/media/lottery.mp3
https://etherscan.io/block/
https://tronscan.org/
https://bscscan.com/block/

https://zh.wikipedia.org/wiki/
https://www.taiwanlottery.com.tw/lotto/BINGOBINGO/drawing.aspx
https://www.taiwanlottery.com.tw/lotto/BINGOBINGO/drawing.aspx</p>\n
https://en.wikipedia.org/wiki/British_Columbia_Lottery_Corporation
https://www.playnow.com/keno/winning-numbers/
https://en.wikipedia.org/wiki/British_Columbia_Lottery_Corporation \n
https://www.playnow.com/keno/winning-numbe
https://www.playnow.com/keno/winning-numbe </p>\n
https://wikipredia.net/zh/Georgia_Lottery
https://www.galottery.com/en-us/games/draw-games/keno.html
https://en.wikipedia.org/wiki/Georgia_Lottery
https://en.wikipedia.org/wiki/Georgia_Lottery \n
https://en.wikipedia.org/wiki/OPAP
https://www.opap.gr/en/kino-draw-results
https://www.opap.gr/en/kino-draw-results</p>\n
https://etherscan.io/
https://etherscan.io/</p>\n
https://tronscan.org/</p>\n
https://etherscan.io/</p>\n\t\t'
https://en.wikipedia.org/wiki/British_Columbia_Lottery_Corporation</p>\n
https://www.playnow.com/keno/winning-numbe
https://en.wikipedia.org/wiki/OPAP
https://www.playnow.com/keno/winning-numbers/</p>\n
https://en.wikipedia.org/wiki/OPAP</p>\n
https://www.opap.gr/en/super3-draw-results
https://www.opap.gr/en/super3-draw-results</p>\n
https://www.playnow.com/keno/winning-numbe</p>\n

https://api.zt66.org

https://api.zt66.win

https://api.zt88.win

https://api.zt00.win

https://api.zt82.vip:4435

https://api.zt66.win/public/last_version

https://static.sanbanye.com/

https://st-tw.maitoo998.com/v6/public/GetNewVersion

https://data-api.binance.vision/api/v3/klines?symbol=

https://socket.zt66.org

https://socket.zt82.vip:4435

https://feross.org>

http://www.xarg.org/2014/03/rational-numbers-in-javascript/

https://img01.yzcdn.cn/vant/coupon-empty.png

https://img01.yzcdn.cn/vant/empty-image-

https://img01.yzcdn.cn/vant/share-sheet-

https://img01.yzcdn.cn/upload_files/2020/06/24/FmKWDg0bN9rMcTp9ne8MXiQWGtLn.png

https://lodash.com/>

https://openjsf.org/>

https://lodash.com/license>

http://underscorejs.org/LICENSE>

https://npms.io/search?q=ponyfill.

http://momentjs.com/guides/

https://zenorocha.github.io/clipboard.js

http://element.eleme.io/

https://github.com/MikeMcl/decimal.js/LICENCE

https://service.hshsin.com/chatIndex?ent_id=14

https://api.zt66.win/public/last_version

g.alicdn.com
https://tronscan.org/
login.greenjade88.com
https://m3w.cn/s/
https://www.playnow.com/keno/winning-numbe
http://schemas.android.com/apk/res/android
api.zt66.org
https://socket.zt66.org
https://f.m.suning.com/api/ct.do
http://schemas.android.com/apk/res/android00androidx.appcompat.widget.FitWindowsLinearLayout((androi
zt.cdn.84dns.com
edgedl.me.gvt1.com
https://www.galottery.com/en-us/games/draw-games/keno.html#tab-winningNumbers
https://socket.zt82.vip:4435
acjs.aliyun.com
t1.dcloud.net.cn
api.zt82.vip
firebaseinstallations.googleapis.com
https://solscan.io/account/
api.zt88.win
https://api.zt88.win
https://sgm-m.jd.com/h5/
gac1.dcloud.net.cn
https://bscscan.com/
https://baike.baidu.com/item/
https://ask.dcloud.net.cn/article/35877
sdk.api.oaid.wocloud.cn
https://www.opap.gr/en/super3-draw-results

https://solscan.io/tx/
https://static.sanbanye.com/shengtu/common/images/loading.gif
https://android.googlesource.com/toolchain/llvm-project
https://android.googlesource.com/toolchain/clang
g.alicdn.com.danuoyi.alicdn.com
https://api.zt82.vip:4435
http://schemas.android.com/apk/res-auto
update.googleapis.com
https://er.dcloud.net.cn/rv
https://cube.meituan.com/ipromotion/cube/toc/component/base/getServerCurrentTime
https://login.greenjade88.com/jswrapper/integration.js.php?casino=greenjade88
https://www.taiwanlottery.com.tw/lotto/BINGOBINGO/drawing.aspx
infinitedata-pa.googleapis.com
na61-na62.wagbridge.alibaba.aliyun.com.gds.alibabadns.com
api.zt66.win
https://wikipredia.net/zh/Georgia_Lottery
https://etherscan.io/
https://ask.dcloud.net.cn/article/35627
https://api.zt66.org
https://api.zt00.win
https://atlas-postgraphile.public.main.prod.cldev.sh/graphql
xg-def-cn.xcdn.global
api.zt00.win
https://data-api.binance.vision/api/v3/klines?symbol=
https://er.dcloud.net.cn/sc
https://api.m.taobao.com/rest/api3.do?api=mtop.common.getTimestamp
https://tronscan.org/#/
https://raydium.io/

guoneia.starlinkdp.top
https://static.sanbanye.com/shengtu/common/images/loading.png);
http://schemas.android.com/apk/res-auto00androidx.appcompat.widget.ActionBarOverlayLayout
1119378012870022401.zga.globalconnetct.com
https://ask.dcloud.net.cn/article/35058
https://g.alicdn.com/AWSC/AWSC/awsc.js
https://er.dcloud.io/sc
gac2.dcloud.net.cn
bgac.dcloud.net.cn
clientservices.googleapis.com
https://android.googlesource.com/toolchain/llvm
www.gstatic.com
er.dcloud.net.cn
https://ask.dcloud.net.cn/article/283
https://er.dcloud.io/rv
instantmessaging-pa.googleapis.com
s1.dcloud.net.cn
https://ask.dcloud.net.cn/article/282
https://api.zt66.win
https://www.playnow.com/keno/winning-numbers/
https://www.taiwanlottery.com/lotto/result/bingo_bingo
https://www.opap.gr/en/kino-draw-results

邮箱线索

邮箱地址	所在文件
robert@xarg.org	摸瓜V2引擎

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=CN, ST=BJ, L=HD, O=Android, OU=Android, CN=Android Debug
签名算法: rsassa_pkcs1v15
有效期自: 2021-04-12 08:27:53+00:00
有效期至: 2121-03-19 08:27:53+00:00
发行人: C=CN, ST=BJ, L=HD, O=Android, OU=Android, CN=Android Debug
序列号: 0x363bc393
哈希算法: sha256
md5值: 06838cc840093b9d4689fc419ba1a3f3
sha1值: 97c84101b9141c130dd75d7428a2922518c36dcd
sha256值: b01d06180d003e79c7b9088993b8e5ae7a19b0da1161aa097c7f398a6f514fa7
sha512值: 67720eb20639d1f5f9c8b7b201b185ea4364f6a89bedd35aa1d273002c16d65a7739f59679510d3b96c1f2c3dd3136d9a34451cb679251a86ff4cafdc18314bf
公钥算法: rsa
密钥长度: 2048
指纹: b27ac6d7a4586417c251be6e44179616262379e57da2d1e19db0995be0ddf509

硬编码敏感信息

可能的敏感信息
"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_tips_certificate" : "certificate"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"
"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"

"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"
"dcloud_tips_certificate" : "证书"

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.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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由

android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
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.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
io.dcloud.PandoraEntry	Schemes: h5e1611ee://,