MoGua

大时代资本 2.0.5.APK 分析报告

APP名称: 大时代资本

包名:	com.ymjdfa1231.wxhsus7130
域名线索:	18条
URL线索:	13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

文件信息

文件名: file_apk_20240613_dashidai-wxhsus7130-2.0.5_1718262511273_VFS (1).apk
文件大小: 45.39MB
MD5值: 825cdb13f4b6c2a2d4dcb492673b6927
SHA1值: babe7a08b22752debc93f4b89a8c0b6477cf8f6e
SHA256值: 15d5ae98b34e7beb922b27b5e973717cb355b7f3fd64a024a9bbccf08c7f5614

ℹ APP 信息

App名称: 大时代资本
包名: com.ymjdfa1231.wxhsus7130
主活动Activity: com.npcwdm5904.ecobmk0175.MainActivity
安卓版本名称: 2.0.5
安卓版本: 1

域名线索

域名	服务器信息
ns.adobe.com	没有服务器地理信息.
developer.apple.com	**IP**: 17.253.87.204 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
api.flutter.dev	**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

flutter.dev	**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
223.5.5.5	**IP**: 223.5.5.5 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
www.ibm.com	**IP**: 23.13.189.250 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
dashidai-pz-fc-srvice-sz-uujifigmca.cn-shenzhen.fcapp.run	**IP**: 39.108.69.25 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108
api.shorebird.devupdater	没有服务器地理信息.
developer.mozilla.org	**IP**: 34.111.97.67 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
	IP: 172.217.163.46 **所属国家**: United States of America

developer.android.com	**地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
dartbug.com	**IP**: 216.239.34.21 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
dashif.org	**IP**: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
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
www.unicode.org	**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
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

aomedia.org	**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
schemas.microsoft.com	**IP:** 13.107.246.74 **所属国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903
default.url	没有服务器地理信息.

URL线索

URL**信息**	Url**所在文件**
https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread	a1/c1.java
http://dashif.org/guidelines/last-segment-number	g2/d.java
http://dashif.org/guidelines/trickmode	g2/d.java
http://dashif.org/thumbnail_tile	g2/d.java
http://dashif.org/guidelines/thumbnail_tile	g2/d.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	e1/o0.java
https://x</LA_URL>	e1/n0.java

https://default.url	e1/n0.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/h.java
https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted	w2/z.java
http://ns.adobe.com/xap/1.0/	k1/a.java
https://aomedia.org/emsg/ID3	u1/a.java
https://developer.apple.com/streaming/emsg-id3	u1/a.java
https://github.com/richtr/NoSleep.js/issues/15	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)	摸瓜V2引擎
http://www.unicode.org/copyright.html	lib/arm64-v8a/libflutter.so
https://api.shorebird.devUpdater	lib/arm64-v8a/libflutter.so
http://://should	lib/arm64-v8a/libflutter.so
http://cookie2too	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://dashidai-pz-fc-srvice-sz-uujifigmca.cn-shenzhen.fcapp.run/v3/appHost/	lib/armeabi-v7a/libapp.so
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
https://github.com/dart-lang/language/issues/3488	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so

http://223.5.5.5/resolve	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues/new.	lib/armeabi-v7a/libapp.so
http://www.unicode.org/copyright.html	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
https://api.shorebird.devUpdater	lib/armeabi-v7a/libflutter.so
http://://should	lib/armeabi-v7a/libflutter.so
http://www.unicode.org/copyright.html	lib/x86_64/libflutter.so
http://://should	lib/x86_64/libflutter.so
http://cookie2too	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

_nativesocket@14069316.listen _httpparser@13463476.responsepa _internetaddress@14069316.fixed _double@0150898.fromintege _future@4048458.immediate _growablelist@0150898._literal _link@14069316.fromrawpat _growablelist@0150898.withcapaci _growablelist@0150898._literal6 _receiveportimpl@1026248.fromrawrec _imagefilter@15065589.composed _list@0150898._ofarray _timer@1026248.periodic _compressednode@54137193.single _growablelist@0150898._literal2 _bigintimpl@0150898.from _list@0150898.empty _pointerpanzoomdata@399213599.fromupdate _directory@14069316.fromrawpat _invocationmirror@0150898._withtype _colorfilter@15065589.lineartosr _growablelist@0150898._literal1 _uri@0150898.file _imagefilter@15065589.blur _growablelist@0150898._literal4 _growablelist@0150898._ofgrowabl _growablelist@0150898.of _nativesocket@14069316.pipe authenticationscheme@13463476.fromstring _list@0150898.of _hashcollisionnode@54137193.fromcollis _list@0150898.generate _typeerror@0150898._create _list@0150898._ofgrowabl _list@0150898._ofefficie _growablelist@0150898._ofarray _growablelist@0150898._literal3 _growablelist@0150898._ofother _timer@1026248._internal _growablelist@0150898._literal5 _rawsocket@14069316._readpipe _socket@14069316._readpipe	lib/armeabi-v7a/libapp.so

_list@0150898._ofother _bytebuffer@7027147._new ngstreamsubscription@4048458.zoned _assertionerror@0150898._create _nativesocket@14069316.normal _imagefilter@15065589.fromcolorf _assetmanifestbin@405287047.fromstanda _filestream@14069316.forstdin _colorfilter@15065589.srgbtoline _uri@0150898.directory _httpparser@13463476.requestpar _growablelist@0150898._literal8 _file@14069316.fromrawpat _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

手机号	所在文件
17512775099	c3/a.java

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=gd, L=st, O=gztuwy2040, OU=gztuwy2040, CN=gztuwy2040
签名算法: rsassa_pkcs1v15
有效期自: 2024-06-13 07:00:30+00:00
有效期至: 2049-06-07 07:00:30+00:00
发行人: C=CN, ST=gd, L=st, O=gztuwy2040, OU=gztuwy2040, CN=gztuwy2040
序列号: 0x48844bf7
哈希算法: sha256
md5值: 182bcc2a30a029551d2c7307371392ca
sha1值: 471a4ef3d024cabda521d78bfe3be7b211dd7830
sha256值: c184e6d65179972aaafc2e97ffacdf0bbff2f561dd9d48d4b9cfa7b8eb2bce1d
sha512值: d034e3d844f15402958d8f6dea6c59f486069f1e34ae1d31f86b36087d70def35168cb9c1646921a3ac59f28b323d4aab27d659e254222a84e28466fafe2217f
公钥算法: rsa
密钥长度: 1024
指纹: d44da6a16ad1c0dae2ab9083bc8282e45ade699d3c77a3478c13438db134723a

🔑 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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.Manifest.permission.READ_PRIVILEGED_PHONE_STATE	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
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。
com.ymjdfa1231.wxhsus7130.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.npcwdm5904.ecobmk0175.MainActivity	Schemes: dashidai205://,

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。