



MoGua

Bebulay 3.3.6.APK 分析报告



APP名称:

Bebulay

包名:	plus.H5EF8EC9D
域名线索:	19条
URL线索:	34条
邮箱线索:	45条
分析日期:	2025年6月7日
分析平台:	摸瓜APK反编译平台

文件名: android.apk
文件大小: 21.98MB
MD5值: 63a8f6dc56b4d7a2449cbfd8c0d15b4d
SHA1值: 93c8ca528123532482f4a9acdbba9b1489fe697d
SHA256值: 17e30349fa1b6ea8f42840e67b20d948a8d427ff8c05587cb4797828a8545541

i APP 信息

App名称: Bebulay
包名: plus.H5EF8EC9D
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 3.3.6
安卓版本: 336

🔍 域名线索

域名	服务器信息
www.huobi.com	IP: 185.60.216.169 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
www.xxx.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
	IP: 15.197.167.90 所属国家: United States of America 地区: Washington

next.vuex.vuejs.org	城市: Seattle 纬度: 47.627499 经度: -122.346199
hertzen.com	IP: 172.67.140.170 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
clipboardjs.com	IP: 104.21.80.1 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
m3w.cn	IP: 119.188.174.58 所属国家: China 地区: Shandong 城市: jinan 纬度: 36.668331 经度: 116.997223

html2canvas.hertzen.com	IP: 172.67.140.170 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
ask.dcloud.net.cn	IP: 101.72.254.86 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
www.coinbase.com	IP: 31.13.95.35 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
schemas.android.com	没有服务器地理信息.
www.binance.com	IP: 3.170.229.66 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
er.dcloud.io	没有服务器地理信息.

ns.adobe.com	没有服务器地理信息.
www.crypto.com	IP: 67.230.169.182 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052986 经度: -118.263687
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
vuejs.org	IP: 3.33.186.135 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199

 URL线索

URL信息	Url所在文件
http://ns.adobe.com/xap/1.0/u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java

https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://er.dcloud.io/rv	io/dcloud/e/c/h/c.java
https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/c.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/e/b/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/e/b/a.java
https://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
http://www.xxx.com	摸瓜V2引擎
http://www.xxx.com	摸瓜V2引擎
https://next.vuex.vuejs.org/	摸瓜V2引擎
https://vuejs.org/images/icons/favicon-96x96.png	摸瓜V2引擎
https://github.com/emn178/js-md5	摸瓜V2引擎
https://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎

https://clipboardjs.com/	摸瓜V2引擎
https://clipboardjs.com/	摸瓜V2引擎
https://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
https://next.vuex.vuejs.org/	摸瓜V2引擎
https://vuejs.org/images/icons/favicon-96x96.png	摸瓜V2引擎
https://github.com/emn178/js-md5	摸瓜V2引擎
https://github.com/ecomfe/zrender/blob/master/LICENSE.txt	摸瓜V2引擎
https://github.com/ecomfe/zrender/blob/master/LICENSE.txt	摸瓜V2引擎
https://github.com/zloirock/core-js/blob/v3.30.2/LICENSE	摸瓜V2引擎
https://github.com/zloirock/core-js	摸瓜V2引擎
https://github.com/systemjs/systemjs/blob/main/docs/errors.md	摸瓜V2引擎
https://www.huobi.com/en-us/	摸瓜V2引擎
https://www.binance.com/en	摸瓜V2引擎
https://www.coinbase.com/	摸瓜V2引擎
https://www.crypto.com/	摸瓜V2引擎
https://www.huobi.com/en-us/	摸瓜V2引擎
https://www.binance.com/en	摸瓜V2引擎

https://www.coinbase.com/	摸瓜V2引擎
https://www.crypto.com/	摸瓜V2引擎
http://www.xxx.com	摸瓜V2引擎
http://www.xxx.com	摸瓜V2引擎
https://html2canvas.hertzen.com>	摸瓜V2引擎
https://hertzen.com>	摸瓜V2引擎
https://html2canvas.hertzen.com>	摸瓜V2引擎
https://hertzen.com>	摸瓜V2引擎
http://a	摸瓜V2引擎
http://a/c%20d?a=1&c=3	摸瓜V2引擎
https://a@b	摸瓜V2引擎
http://x	摸瓜V2引擎
http://a	摸瓜V2引擎
http://a/c%20d?a=1&c=3	摸瓜V2引擎
https://a@b	摸瓜V2引擎
http://x	摸瓜V2引擎

邮箱地址	所在文件
23@3x1-c85f317e.png	摸瓜V2引擎
23@3x1-c85f317e.png	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
flags@2x-e21becc4.png	摸瓜V2引擎
c2c@binance.com emn178@gmail.com jhruby.web@gmail.com	摸瓜V2引擎
23@3x1.png	摸瓜V2引擎

23@3x1.png	摸瓜V2引擎
flags@2x-e21becc4.png	摸瓜V2引擎
23@3x1.png	摸瓜V2引擎
flags@2x-e21becc4.png	摸瓜V2引擎
c2c@binance.com emn178@gmail.com jhruby.web@gmail.com	摸瓜V2引擎
flags@2x-e21becc4.png	摸瓜V2引擎
23@3x1.png	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com c2c@binance.com으로	摸瓜V2引擎
c2c@binance.com c2c@binance.com으로	摸瓜V2引擎
flags@2x-e21becc4.png	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎

c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
trash@rubaxa.org owen23355@gmail.com	摸瓜V2引擎
trash@rubaxa.org owen23355@gmail.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
c2c@binance.com	摸瓜V2引擎
23@3x1-c85f317e.png	摸瓜V2引擎
23@3x1-c85f317e.png	摸瓜V2引擎

🌸 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=, L=, O=Android, OU=Android, CN=jFHKxfNy0YzlaEGwPzQgdxlYpDVrPY3DekLJRX7qp4BNsBJpi25%2FQ74NRsqSTeMb9DHWGVaiWAeZUHZNhlqx5Q%3D%3D

签名算法: rsassa_pkcs1v15

有效期自: 2025-04-11 14:18:15+00:00

有效期至: 2125-03-18 14:18:15+00:00

发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=jFHKxfNy0YzlaEGwPzQgdxlYpDVrPY3DekLJRX7qp4BNsBJpi25%2FQ74NRsqSTeMb9DHWGVaiWAeZUHZNhlqx5Q%3D%3D

序列号: 0x6dfc12fc

哈希算法: sha256

md5值: 7025783577884b88f9ee54278732c2e8

sha1值: 7b2ff7dee7794655282ed723c41fa461b4e76211

sha256值: 293f921174a97fe43ebdfaf7686c5893a339f41397a20765c70d47240d5e5529

sha512值: 26f9844753b74d73b10f07c48fc19f83b1e00fbe062f88819e46c143cb5ff74f55bf6e618c1d0d6bf46c52b068fddea18bd01d8bae90591be7d4fb65a34210bd

公钥算法: rsa

密钥长度: 2048

指纹: f88597011f6004b241857ebd114fc7cbb2a007ff72d70fffe4ecb6991d112d3d

🔑 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.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.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_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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: h596eaafb://,

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。