



MoGua

GoldenWOW 23.12.14.APK 分析报告



APP名称:	GoldenWOW
包名:	com.H551DD09A.MPC_GAME
域名线索:	28条
URL线索:	24条
邮箱线索:	2条
分析日期:	2025年6月19日
分析平台:	摸瓜APK反编译平台

📁 文件信息

文件名: 2_base.apk
文件大小: 8.75MB
MD5值: 3e62ab154e247e89e847cf85ddf6439a
SHA1值: a62d4fe64cbe2c89e59b9c8bac678c1501d44f46
SHA256值: 86da9d1bf456aa777d8f7c61c32000925619012e2bb39f4b8dd74fcb59b12c04

i APP 信息

App名称: GoldenWOW
包名: com.H551DD09A.MPC_GAME
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 23.12.14
安卓版本: 231214

🔍 域名线索

域名	服务器信息
connectivitycheck.gstatic.com	IP: 203.208.49.130 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
clipboardjs.com	IP: 104.21.48.1 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

sketch.com	IP: 13.249.160.98 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
m3w.cn	IP: 221.204.20.165 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
share.theotc.cc	没有服务器地理信息.
momentjs.com	IP: 104.17.63.214 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
s1.dcloud.net.cn	IP: 150.158.3.107 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
ossby.oss-cn-hongkong.aliyuncs.com	IP: 47.79.66.76 所属国家: United States of America 地区: California 城市: San Mateo 纬度: 37.547424 经度: -122.330589
schemas.android.com	没有服务器地理信息.
oss-mp.oss-cn-hangzhou.aliyuncs.com	IP: 101.67.62.63 所属国家: China 地区: Zhejiang 城市: Huzhou 纬度: 30.870550 经度: 120.093300
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
gac1.dcloud.net.cn	IP: 121.40.128.37 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583

ask.dcloud.net.cn	IP: 101.72.227.61 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
opensource.org	IP: 104.22.65.197 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
er.dcloud.io	没有服务器地理信息.
sdk.api.oaid.wocloud.cn	没有服务器地理信息.
er.dcloud.net.cn	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
ns.adobe.com	没有服务器地理信息.
encrypted-tbn0.gstatic.com	IP: 142.251.215.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
sdk.api.oaid.wocloud.cn.local	没有服务器地理信息.
ati.mypayapi.pro	IP: 18.140.43.118 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
android.googlesource.com	IP: 192.178.163.82 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
timgsa.baidu.com	没有服务器地理信息.
img.yzcdn.cn	IP: 202.108.29.171 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

api.ipify.org	IP: 172.67.74.152 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
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
edgedl.me.gvt1.com	IP: 34.104.35.123 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514

 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://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://er.dcloud.io/rv	io/dcloud/e/c/h/b.java
https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/b.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://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
https://github.com/emn178/js-md5	摸瓜V2引擎
https://github.com/Tencent/vConsole	摸瓜V2引擎
http://opensource.org/licenses/MIT	摸瓜V2引擎
https://github.com/Tencent/vConsole	摸瓜V2引擎
https://github.com/Tencent/vConsole.git	摸瓜V2引擎
https://clipboardjs.com/	摸瓜V2引擎
https://img.yzcdn.cn/vant/coupon-empty.png	摸瓜V2引擎
https://img.yzcdn.cn/vant/empty-image-	摸瓜V2引擎
https://img.yzcdn.cn/vant/share-icon-	摸瓜V2引擎
https://img.yzcdn.cn/upload_files/2020/06/24/FmKWDg0bN9rMcTp9ne8MXiQWGtLn.png	摸瓜V2引擎
https://img.yzcdn.cn/upload_files/2020/07/02/Fu4_ya0l0aAt4Mv4PL9jzPzfZnDX.png	摸瓜V2引擎
http://momentjs.com/guides/	摸瓜V2引擎
https://share.theotc.cc/	摸瓜V2引擎
https://oss-mp.oss-cn-hangzhou.aliyuncs.com/MPC_GAME_v2/version-MPC.json	摸瓜V2引擎
https://ati.mypayapi.pro/common/common/index	摸瓜V2引擎
https://oss-mp.oss-cn-hangzhou.aliyuncs.com/MPC_GAME_v2/MPC.apk	摸瓜V2引擎
https://ati.mypayapi.pro/merchant/login/verifyGoogleAuthOpen	摸瓜V2引擎
https://ati.mypayapi.pro/common/common/uploadsV	摸瓜V2引擎
https://github.com/think2011/localResizeIMG/issues/7	摸瓜V2引擎
">http://feross.org>	摸瓜V2引擎
https://img.yzcdn.cn/vant/apple-1.jpg	摸瓜V2引擎
https://img.yzcdn.cn/vant/apple-1.jpg	摸瓜V2引擎

https://api.ipify.org/?format=json	摸瓜V2引擎
https://timgsa.baidu.com/timg?image&quality=80&size=b9999_10000&sec=1595434761460&di=362dae11080d82692bd0bafba1bdca07&imgtype=0&src=http%3A%2F%2Fa1.att.hudong.com%2F05%2F00%2F01300000194285122188000535877.jpg	摸瓜V2引擎
connectivitycheck.gstatic.com	摸瓜V3引擎
http://schemas.android.com/apk/res-auto00androidx.appcompat.widget.ActionBarOverlayLayout	摸瓜V3引擎
https://er.dcloud.net.cn/sc	摸瓜V3引擎
https://sketch.com	摸瓜V3引擎
https://ask.dcloud.net.cn/article/282	摸瓜V3引擎
https://clipboardjs.com/	摸瓜V3引擎
http://feross.org	摸瓜V3引擎
http://schemas.android.com/apk/res-auto((androidx.appcompat.widget.ActionMenuView	摸瓜V3引擎
s1.dcloud.net.cn	摸瓜V3引擎
http://schemas.android.com/apk/res/android00androidx.appcompat.widget.FitWindowsLinearLayout((androi	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm-project	摸瓜V3引擎
http://opensource.org/licenses/MIT	摸瓜V3引擎
https://ask.dcloud.net.cn/article/35627	摸瓜V3引擎
gmscompliance-pa.googleapis.com	摸瓜V3引擎
oss-mp.oss-cn-hangzhou.aliyuncs.com	摸瓜V3引擎
gac1.dcloud.net.cn	摸瓜V3引擎
https://er.dcloud.net.cn/rv	摸瓜V3引擎
update.googleapis.com	摸瓜V3引擎
https://ask.dcloud.net.cn/article/283	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
https://img.yzcdn.cn/vant/apple-1.jpg	摸瓜V3引擎
sdk.api.oaid.wocloud.cn	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm	摸瓜V3引擎
https://ossby.oss-cn-hongkong.aliyuncs.com/\$	摸瓜V3引擎
https://github.com/Tencent/VConsole	摸瓜V3引擎

http://schemas.android.com/apk/res/android	摸瓜V3引擎
encrypted-tbn0.gstatic.com	摸瓜V3引擎
https://er.dcloud.io/rv	摸瓜V3引擎
sdk.api.oaid.wocloud.cn.local	摸瓜V3引擎
https://android.googlesource.com/toolchain/clang	摸瓜V3引擎
ati.mypayapi.pro	摸瓜V3引擎
clientservices.googleapis.com	摸瓜V3引擎
android.googleapis.com	摸瓜V3引擎
https://er.dcloud.io/sc	摸瓜V3引擎
api.ipify.org	摸瓜V3引擎
edgedl.me.gvt1.com	摸瓜V3引擎
https://ask.dcloud.net.cn/article/35877	摸瓜V3引擎
https://oss-mp.oss-cn-hangzhou.aliyuncs.com/MPC_GAME_v2/MPC23.13.23.wgt	摸瓜V3引擎
http://schemas.android.com/apk/res-autoAAio.dcloud.feature.gallery.imageedit.view.WindowInsertLinear	摸瓜V3引擎
https://m3w.cn/s/	摸瓜V3引擎
https://ask.dcloud.net.cn/article/35058	摸瓜V3引擎

 邮箱线索

邮箱地址	所在文件
emn178@gmail.com	摸瓜V2引擎
hilogjw@gmail.com	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=, L=, O=Android, OU=Android, CN=y%2BHWvgraAhymfDhVHvtlnhDL7UL%2BldRChS0oXOsDCZKPWaFskEVogTRgbzvfjRyqa9yiO0cYN0yXpzlSEz6xqQ%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2023-12-14 11:02:05+00:00
有效期至: 2123-11-20 11:02:05+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=y%2BHWvgraAhymfDhVHvtlnhDL7UL%2BldRChS0oXOsDCZKPWaFskEVogTRgbzvfjRyqa9yiO0cYN0yXpzlSEz6xqQ%3D%3D
序列号: 0x505bc20d
哈希算法: sha256
md5值: e6dbe17a16a365df4faff7bc3e0d1a4a
sha1值: b68048b5b8255aa6790e4adcea46354ee147eeb7
sha256值: 53ce235c3fc819be5e9b671d061f8951f14976ca21542a6676b46afc5040ce7c
sha512值: 0e50f381ebe7b018c323e83571994cb812ceda19acafb895d7147159826ae3df41a179e1c1bdb8840f0c4f55f55622288a211d28aa36bca7568b43cdaaa1216f
公钥算法: rsa
密钥长度: 2048
指纹: 31e1dbf824bc72918108804e64af55b1e15e006d67af1d3ad9b1e3d10acb6b62

 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_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"

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.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.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.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_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.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.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
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: xpay://, h551dd09a://,