



MoGua

com_zodtttd_quake-half-life 1.0.APK 分析报告



APP名称:

com_zodtttd_quake-half-life

包名:	com.software.application
域名线索:	17条
URL线索:	3条
邮箱线索:	4条
分析日期:	2025年6月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 0aa8e608f65414173829bfc633d5b5ca8c4a62892ca4f592c7a147768771d7ad.apk

文件大小: 0.46MB
MD5值: ffda6fd12e43ce79fa6af19d3baea3b8
SHA1值: f08dec43ed47266be516a39ffc395215b7723847
SHA256值: 0aa8e608f65414173829bfc633d5b5ca8c4a62892ca4f592c7a147768771d7ad

i APP 信息

App名称: com_zodttdd_quake-half-life
包名: com.software.application
主活动Activity: .Main
安卓版本名称: 1.0
安卓版本: 1

🔍 域名线索

域名	服务器信息
depositmobi.com	IP: 52.27.79.221 所属国家: United States of America 地区: Oregon 城市: Portland 纬度: 45.523460 经度: -122.676468
androids-market.ru	没有服务器地理信息.
www.mobi911.ru	IP: 31.28.24.244 所属国家: Russian Federation 地区: Moskva 城市: Moscow 纬度: 55.752258 经度: 37.615471
	IP: 104.21.48.161

www.android-app.ru	所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
fonts.gstatic.com	IP: 203.208.50.34 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.sms911.ru	IP: 78.108.80.33 所属国家: Russian Federation 地区: Sankt-Peterburg 城市: Saint Petersburg 纬度: 59.894440 经度: 30.264200
googleadapis.l.google.com	IP: 114.250.65.33 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
mc.yandex.ru	IP: 87.250.251.119 所属国家: Russian Federation 地区: Moskva 城市: Moscow 纬度: 55.752258 经度: 37.615471
s.w.org	IP: 192.0.77.48 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.748425

	经度: -122.413673
android-app.ru	IP: 104.21.48.161 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
adservice.google.com	IP: 114.250.70.38 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
googleads.g.doubleclick.net	IP: 114.250.67.38 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
counter.yadro.ru	IP: 88.212.201.198 所属国家: Russian Federation 地区: Moskva 城市: Moscow 纬度: 55.752258 经度: 37.615471
pagead2.google syndication.com	IP: 114.250.67.38 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 168.143.171.154 所属国家: Japan

adservice.google.fr	地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
pagead46.l.doubleclick.net	IP: 142.251.215.226 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
gstaticadssl.l.google.com	IP: 203.208.50.162 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

 URL线索

URL信息	Url所在文件
http://androids-market.ru/register/	com/software/application/DeviceRegistrar.java
http://androids-market.ru/unregister/	com/software/application/DeviceRegistrar.java
http://depositmobi.com/	摸瓜V1引擎
http://www.mobi911.ru/	摸瓜V1引擎
http://depositmobi.com/.	摸瓜V1引擎
http://www.mobi911.ru/	摸瓜V1引擎

http://www.mobi911.ru	摸瓜V1引擎
http://www.mobi911.ru/.	摸瓜V1引擎
http://www.sms911.ru	摸瓜V1引擎
http://www.sms911.ru/.	摸瓜V1引擎
fonts.googleapis.com	摸瓜V3引擎
www.android-app.ru	摸瓜V3引擎
gstaticadssl.l.google.com	摸瓜V3引擎
fonts.gstatic.com	摸瓜V3引擎
googleadapis.l.google.com	摸瓜V3引擎
mc.yandex.ru	摸瓜V3引擎
s.w.org	摸瓜V3引擎
android-app.ru	摸瓜V3引擎
googleads.g.doubleclick.net	摸瓜V3引擎
counter.yadro.ru	摸瓜V3引擎
pagead2.google syndication.com	摸瓜V3引擎
adservice.google.fr	摸瓜V3引擎
pagead46.l.doubleclick.net	摸瓜V3引擎

✉ 邮箱线索

邮箱地址	所在文件
noviigfastn@gmail.com	com/software/application/C2DMReceiver.java
noviigfastn@gmail.com	com/software/application/DeviceRegistrar.java
noviigfastn@gmail.com	com/software/application/Main.java
help@zerogravity.kz support@i-free.com zipwap.ru@gmail.com	摸瓜V1引擎

📱 手机线索

✳ 签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=SD, ST=WW, L=New York, O=Reti, OU=UI, CN=Code Coder
签名算法: rsassa_pkcs1v15
有效期自: 2011-07-17 19:29:30+00:00
有效期至: 2038-12-02 19:29:30+00:00
发行人: C=SD, ST=WW, L=New York, O=Reti, OU=UI, CN=Code Coder
序列号: 0x4e23381a

哈希算法: sha1
md5值: a91d613fb245e6e3cb1096ae7541035d
sha1值: 5cb0136d4f218b1d7a489024972f8aa4720f5e67
sha256值: 6c51d90fcaded4681fb96892222cfeec28eb30ed3edcd9e410c6dc2340666e70
sha512值: 940463fa8c60c156fc9b9928bfad26030b835ec41c0e0aa32e74b1a5a3be94b95a8781894f49046b4c0931c2ed1aff6ed503ca07c5839e86121fdbcd2756c066

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.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
com.software.application.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
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

应用内通信

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。