



MoGua

游戏更新器 1.0.8.APK 分析报告



APP名称:

游戏更新器

包名: `com.palmpai.gameupdater`

域名线索: 3条

URL线索: 10条

邮箱线索: 0条

分析日期: 2025年2月22日

分析平台: [摸瓜APK反编译平台](#)

文件名: GameUpdater_yd_v1000008.apk

文件大小: 10.23MB

MD5值: 4276d9fa802dd665f0d781ed255929de

SHA1值: f0fa56e6f948376597c316372a654c5de85c665f

SHA256值: 112be5452543296ed69d45496dea4b025e6a1b734db7e44ba8f40d9e6b610212

i APP 信息

App名称: 游戏更新器

包名: com.palmpai.gameupdater

主活动Activity: com.palmpai.gameupdater.ui.MainActivity

安卓版本名称: 1.0.8

安卓版本: 1000008

🔍 域名线索

域名	服务器信息
www.baidu.com	IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
games.yoodacloud.com	没有服务器地理信息.
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

URL线索

URL信息	Url所在文件
http://www.baidu.com	com/cphone/network/util/URLUtil.java
http://games.yoodacloud.com/	com/palmpai/gameupdater/BuildConfig.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java

邮箱线索

手机线索

签名证书

v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2014-12-23 06:43:41+00:00
有效期至: 2042-05-10 06:43:41+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0xff0641323cf95512
哈希算法: sha256
md5值: 0eba50a45c15b35d977d04d84379b355
sha1值: 41791c9b8faf15e1acd5aaf59210fd42467d8277
sha256值: 2d370c21f5dfd553d2a796314b70925fb38adeef90864c920bbbb12887d3522
sha512值: 94c59dcb36747368e23b13d0fea3f611cf4c632691e27a961047ae5d0e4ce7abbd3bc6d2280eb55275feb9733c47364a54ac1a21f9447e7e140adb6ebf7acb8e
公钥算法: rsa
密钥长度: 2048
指纹: bc1007e81b79d89bac41c9da38a9c6d7b5c63e546d35b8f83ed44c5102c7e0e3

硬编码敏感信息

可能的敏感信息

"toast_session_expired_403" : "会话失效了,请重试或联系客服喔 (859) "

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
登录摸瓜网站后查看		

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.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.DELETE_PACKAGES	系统需要	删除应用程序	允许应用程序删除 Android 包。恶意应用程序可以使用它来删除重要的应用程序
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.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

android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.ACCESS_MEDIA_LOCATION	危险	访问的任何地理位置	允许应用程序访问的任何地理位置持久保存在用户的共享集合
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。
com.android.launcher.permission.ACCESS_DOWNLOAD_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.palmpai.gameupdater.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

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。