MoGua

跑路科技 7.2.0.APK 分析报告

APP名称:	跑路科技

包名:	com.minecraftpe.plugin
域名线索:	6条
URL线索:	17条
邮箱线索:	0条
分析日期:	2024年10月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 跑路科技_7.2.0.apk
文件大小: 27.37MB
MD5值: daa1289e61ed4f05154a2c26399946f5
SHA1值: a784698395c35dfa0bf27a58b11160e0f66d0747
SHA256值: 1ab6a07b8b15b7dbfa13c351062cda1e2fbd87f873e68ceaaa31d77f51c5f5a6

APP 信息

App名称: 跑路科技
包名: com.minecraftpe.plugin
主活动Activity: com.mojang.minecraftpe.activity.MainActivity
安卓版本名称: 7.2.0
安卓版本: 20241014

域名线索

域名	服务器信息
g79mclobt.nie.netease.com	**IP**: 42.186.125.85 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
g79mcltransfer.nie.netease.com	**IP**: 42.186.192.81 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
aria.laoyuyu.me	没有服务器地理信息.
	IP: 42.186.122.125

g79mclobt.minecraft.cn	**所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
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
schemas.android.com	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://aria.laoyuyu.me/aria_doc/create/any_java.html	com/arialyy/aria/core/Aria.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/download/DownloadReceiver.java
https://github.com/AriaLyy/Aria/issues/597	com/arialyy/aria/core/download/m3u8/M3U8Option.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/upload/UploadReceiver.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Flowable.java

https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/rxjava3/exceptions/UndeliverableException.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/AbstractC1175.java
http://schemas.android.com/apk/res/android	··/AbstractC2660.java
https://g79mclobt.minecraft.cn/rental-server-world-enter/get	`'/DialogInterface$OnDismissListenerC1891.java
https://g79mclobt.minecraft.cn/rental-server/query/search-by-name	`'/DialogInterface$OnDismissListenerC1891.java
https://g79mclobt.nie.netease.com/online-lobby-room/query/search-by-name-v2	`'/DialogInterface$OnDismissListenerC1900.java
https://g79mclobt.nie.netease.com/online-lobby-room-enter/	`'/DialogInterface$OnDismissListenerC1900.java
https://g79mcltransfer.nie.netease.com/room-with-name	`'/DialogInterface$OnDismissListenerC1856.java

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
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: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+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: 0x936eacbe07f201df
哈希算法: sha1
md5值: e89b158e4bcf988ebd09eb83f5378e87
sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569
公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

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.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
moe.shizuku.manager.permission.API_V23	未知	Unknown permission	Unknown permission from android reference
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
com.minecraftpe.plugin.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信
