MoGua

皇马 3.4.2216708.APK 分析报告

APP名称:	皇马

包名:	com.emplre.hellogg.pkz
域名线索:	4条
URL线索:	4条
邮箱线索:	1条
分析日期:	2025年7月14日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 1683883912304.apk
文件大小: 58.97MB
MD5值: bd293b364e68bd72eda73c916c028872
SHA1值: 8cf1adaf3aa214b6b921969454ee756f33fa9abf
SHA256值: a3a1c78fa24dc7f60ed5b81f636289c5e7d68db2724eff20130f5317a40cb68c

APP 信息

App名称: 皇马
包名: com.emplre.hellogg.pkz
主活动Activity: com.empire.ggwin.app.FullscreenActivity
安卓版本名称: 3.4.2216708
安卓版本: 1

域名线索

域名	服务器信息
log-server-local.goodgaming.org	没有服务器地理信息.
d.alipay.com	**IP**: 203.209.245.120 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
local.ggwin.nocold.tw	没有服务器地理信息.
nocold.tw	**IP**: 172.105.204.41 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689507 **经度**: 139.691696

URL线索

URL信息	Url所在文件
https://d.alipay.com	com/empire/ggwin/app/s.java
https://app-buildin	com/empire/ggwin/app/FullscreenActivity.java
https://app-buildin/	com/empire/ggwin/app/FullscreenActivity.java
http://local.ggwin.nocold.tw/	com/empire/ggwin/app/FullscreenActivity.java
https://nocold.tw/	com/empire/ggwin/app/FullscreenActivity.java
https://log-server-local.goodgaming.org	com/empire/ggwin/app/MainApplication.java
https://log-server-local.goodgaming.org	com/empire/ggwin/net/c/c.java

邮箱线索

邮箱地址	所在文件
your.account@domain.com	org/acra/sender/DefaultReportSenderFactory.java

手机线索

手机号	所在文件
17598214793	Mogua Engine V2
14091739973	Mogua Engine V2
19823191819	Mogua Engine V2
13803106315	Mogua Engine V2

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=CN, O=7fb0733b64c0, OU=a98e477a4ebd, CN=pkw
签名算法: rsassa_pkcs1v15
有效期自: 2022-07-11 04:06:32+00:00
有效期至: 2047-07-05 04:06:32+00:00
发行人: C=CN, O=7fb0733b64c0, OU=a98e477a4ebd, CN=pkw
序列号: 0x6a7b6b0c
哈希算法: sha256
md5值: 3046ce899c45d0a844cab2caf2639d39
sha1值: 17fb98a1d6bb87441976108353fe8d2b604f9023
sha256值: 98224123ddda478e603daa23afb4b287d06ce48330957acb5278167ba81fcb03
sha512值: cd68351e9920acb8038b0dfe184458c81f6f6cace47d61e9bfedffecfd0895b9cb5d6066e7212c116dc3cbfcf8873dd8028283b5fabfe4d7a816f028578ed7c5
公钥算法: rsa
密钥长度: 2048
指纹: 1f8d3ec8c493e8441d919b4f29731dc7a458c272052801ba8996fafbdec1f1c1

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.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.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_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

应用内通信