MoGua

Monster789 2.1.3.5.APK 分析报告

APP名称: Monster789

包名:	com.lottery.monster
域名线索:	15条
URL线索:	16条
邮箱线索:	0条
分析日期:	2025年4月26日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: GP00-1.apk
文件大小: 21.12MB
MD5值: 5ca34106f31313943296c026626c9e08
SHA1值: 0c28ab7357a3505de036736a91fc2b18465bebf9
SHA256值: e6d61221c24b92fb8b136ec748a88e7d3f6e51d682cf6e54088ece97428cf858

APP 信息

App名称: Monster789
包名: com.lottery.monster
主活动Activity: com.lottery.monster.MainActivity
安卓版本名称: 2.1.3.5
安卓版本: 2135

域名线索

域名	服务器信息
download.garudalottery.com	**IP**: 163.181.23.224 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
47.243.17.51	**IP**: 47.243.17.51 **所属国家**: United Kingdom of Great Britain and Northern Ireland **地区**: England **城市**: Manchester **纬度**: 53.480949 **经度**: -2.237430
download.mybtlottery.com	**IP**: 163.181.164.242 **所属国家**: Singapore **地区**: Singapore

	城市: Singapore **纬度**: 1.289987 **经度**: 103.850281
ns.adobe.com	没有服务器地理信息.
pagead2.googlesyndication.com	IP: 114.250.65.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
bt-games-sg.oss-accelerate.aliyuncs.com	IP: 8.131.131.67 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
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
api.monsters789.com	IP: 104.21.78.147 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
btgame.win	没有服务器地理信息.
120.27.129.233	IP: 120.27.129.233 **所属国家**: China **地区**: Zhejiang

	城市: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
dashif.org	**IP**: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
plus.google.com	**IP**: 199.16.156.7 **所属国家**: United States of America **地区**: Georgia **城市**: Atlanta **纬度**: 33.770844 **经度**: -84.377632
schemas.android.com	没有服务器地理信息.
download.monsters789.com	**IP**: 65.9.189.115 **所属国家**: Croatia **地区**: Grad Zagreb **城市**: Zagreb **纬度**: 45.814396 **经度**: 15.978012
garudalottery.com	**IP**: 104.21.16.1 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

URL线索

URL信息	Url所在文件
https://download.monsters789.com/pro-resource/2025/03/04/abig2_20250304143259A001.webp	com/lottery/monster/MyApplication.java
https://download.garudalottery.com/pro-resource/2025/03/05/	com/lottery/monster/MyApplication.java
https://download.mybtlottery.com/app/GP00.apk	com/lottery/monster/MainActivity.java
https://download.monsters789.com/default/host.log	com/lottery/monster/service/MyJobIntentService.java
https://bt-games-sg.oss-accelerate.aliyuncs.com/pro-resource/2024/12/13/aicon_20241213135856A001.webp	com/lottery/monster/service/MyJobIntentService.java
http://120.27.129.233:5000/	com/lottery/monster/api/ApiConstant.java
http://47.243.17.51/prod-api/	com/lottery/monster/api/ApiConstant.java
https://api.monsters789.com	com/lottery/monster/api/ApiConstant.java
https://api.monsters789.com/	com/lottery/monster/api/ApiConstant.java
https://garudalottery.com/	com/lottery/monster/fragment/HomeOneFragment.java
https://btgame.win/	com/lottery/monster/activity/XHLoginActivity.java
https://btgame.win/	com/lottery/monster/activity/SattaActivity.java
https://btgame.win/	com/lottery/monster/activity/LiveActivity.java
https://garudalottery.com/	com/lottery/monster/activity/LiveActivity.java
https://btgame.win/	com/lottery/monster/activity/RummyActivity.java
https://garudalottery.com/	com/lottery/monster/activity/RummyActivity.java
https://btgame.win/	com/lottery/monster/activity/FishActivity.java

https://garudalottery.com/	com/lottery/monster/activity/FishActivity.java
https://garudalottery.com/	com/lottery/monster/activity/CasinoActivity.java
https://plus.google.com/	h5/j0.java
http://schemas.android.com/apk/res/android	j8/b.java
http://dashif.org/guidelines/last-segment-number	h4/d.java
http://dashif.org/guidelines/trickmode	h4/d.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	a5/b.java
http://ns.adobe.com/xap/1.0/	o3/a.java

邮箱线索

手机线索

手机号	所在文件
19849657605	com/lottery/monster/activity/XHLoginActivity.java

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: CN=zhejiang, OU=zhejiang, O=zhejiang, L=zhejiang, ST=zhejiang, C=zhejiang
签名算法: rsassa_pkcs1v15
有效期自: 2025-02-27 12:10:01+00:00
有效期至: 2055-02-20 12:10:01+00:00
发行人: CN=zhejiang, OU=zhejiang, O=zhejiang, L=zhejiang, ST=zhejiang, C=zhejiang
序列号: 0x1
哈希算法: sha256
md5值: cc820526d9c337f01f0679831f1aa705
sha1值: 89f657723fe2c78c7b77ea4bc8e30b8410b7ba42
sha256值: bc5bb1e5be1ce03fca912acea84bf0cdad08ea245b78f541aef369e67a120ea4
sha512值: fe51f29c262fa7920586b435be1565737bcd4b459457fc84c41c01d9410f7122bf34107aa4f2a28ba053183f064a644af123f1ad8bfadbd396b96738e239c29b
公钥算法: rsa
密钥长度: 2048
指纹: 33bdcde8b32fe453a3a27a33fa50656f9793ae7441c7df4dafb8d9f6aadd98c7

🔑 硬编码敏感信息

可能的敏感信息
"enter_password" : "Enter Password"
"google_api_key" : "AIzaSyDpFobGqlj3hxcwnxSdjKHyDX_eY8C9wck"
"google_crash_reporting_api_key" : "AIzaSyDpFobGqlj3hxcwnxSdjKHyDX_eY8C9wck"
"password" : "Password"
"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "Permanently denied authorization, please manually grant relevant permissions"
"please_enter_password" : "Please enter password"
"repeat_password" : "Repeat password"
"set_password" : "Set password"

"user" : "USER"

"enter_password" : "கடவுச்சொல் உள்ளிடவும்"

"password" : "கடவுச்சொல்"

"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "நிரந்தரமாக மறுக்கப்பட்ட அனுமதி, தயவுசெய்து சார்ந்த அனுமதிகளை கைமுறையாக அளிக்கவும்"

"please_enter_password" : "தயவுசெய்து கடவுச்சொல் உள்ளிடவும்"

"repeat_password" : "கடவுச்சொல் மீண்டும் உள்ளிடவும்"

"set_password" : "கடவுச்சொல் அமை"

"user" : "பயனர்"

"enter_password" : "गुप्तशब्द दर्ज करू"

"password" : "गुप्तशब्द"

"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "स्थायी रूप सँ अस्वीकृत प्राधिकरण, कृपया मैन्युअल रूप सँ प्रासंगिक अनुमति प्रदान करू"

"please_enter_password" : "कृपया पासवर्ड दर्ज करू"

"repeat_password" : "गुप्तशब्द दोहराउ"

"set_password" : "गुप्तशब्द सेट करू"

"user" : "उपयोगकर्ता"

"enter_password" : "ਪਾਸਵਰਡ ਦਰਜ ਕਰੋ"

"password" : "ਪਾਸਵਰਡ"

"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "ਸਥਾਈ ਤੌਰ 'ਤੇ ਅਧਿਕਾਰਤ ਤੌਰ 'ਤੇ ਅਸਵੀਕਾਰ ਕੀਤਾ ਗਿਆ ਹੈ, ਕਿਰਪਾ ਕਰਕੇ ਹੱਥੀਂ ਸੰਬੰਧਿਤ ਅਨੁਮਤੀਆਂ ਦਿਓ"

"please_enter_password" : "ਕਿਰਪਾ ਕਰਕੇ ਪਾਸਵਰਡ ਦਰਜ ਕਰੋ"

"repeat_password" : "ਪਾਸਵਰਡ ਦੁਹਰਾਓ"

"set_password" : "ਪਾਸਵਰਡ ਸੈੱਟ ਕਰੋ"

"user" : "USER"

"enter_password" : "पासवर्ड प्रविष्ट गर्नुहोस्"

"password" : "पासवर्ड"

"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "स्थायी रूपमा अस्वीकृत प्राधिकरण, कृपया म्यानुअल रूपमा सान्दर्भिक अनुमतिहरू दिनुहोस्"

"please_enter_password" : "कृपया पासवर्ड प्रविष्ट गर्नुहोस्"

"repeat_password" : "पासवर्ड दोहोर्याउनुहोस्"

"set_password" : "पासवर्ड सेट गर्नुहोस्"

"user" : "USER"

"enter_password" : "పాస్‌వర్డ్ నమోదు చేయండి"

"password" : "పాస్‌వర్డ్"

"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "శాశ్వతంగా అనుమతి నిరాకరించబడింది, దయచేసి సంబంధిత అనుమతులను చేతితో మంజూరు చేయండి"

"please_enter_password" : "దయచేసి పాస్‌వర్డ్‌ను నమోదు చేయండి"

"repeat_password" : "పాస్‌వర్డ్ మళ్ళీ నమోదు చేయండి"

"set_password" : "పాస్‌వర్డ్ సెట్ చేయండి"

"user" : "వినియోగదారు"

"enter_password" : "पासवर्ड दर्ज करें"

"password" : "पासवर्ड"

"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "स्थायी रूप से अस्वीकृति, कृपया संबंधित अनुमतियाँ मैन्युअली प्रदान करें"

"please_enter_password" : "कृपया पासवर्ड दर्ज करें"

"repeat_password" : "पासवर्ड दोहराएँ"

"set_password" : "पासवर्ड सेट करें"

"user" : "उपयोगकर्ता"

"enter_password" : "പാസ്‌വേഡ് നൽകുക"

"password" : "പാസ്‌വേഡ്"

"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "ശാശ്വതമായി അംഗീകാരം നിഷേധിച്ചു, ദയവായി പ്രസക്തമായ അനുമതികൾ നേരിട്ട് നൽകുക"

"please_enter_password" : "ദയവായി പാസ്‌വേഡ് നൽകുക"

"repeat_password" : "പാസ്‌വേഡ് ആവർത്തിക്കുക"

"set_password" : "പാസ്‌വേഡ് സജ്ജീകരിക്കുക"

"user" : "ഉപയോക്താവ്"

"enter_password" : "পাসওয়ার্ড লিখুন"

"password" : "পাসওয়ার্ড"

"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "স্থায়ীভাবে অনুমোদন অস্বীকার করা হয়েছে, অনুগ্রহ করে ম্যানুয়ালি প্রাসঙ্গিক অনুমতি দিন"

"please_enter_password" : "অনুগ্রহ করে পাসওয়ার্ড লিখুন"

"repeat_password" : "পাসওয়ার্ড পুনরাবৃত্তি করুন"

"set_password" : "পাসওয়ার্ড সেট করুন"

"user" : "USER"

"enter_password" : "ಪಾಸ್‌ವರ್ಡ್ ನಮೂದಿಸಿ"

"password" : "Password"

"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "ಶಾಶ್ವತವಾಗಿ ಅನುಮತಿಯನ್ನು ನಿರಾಕರಿಸಲಾಗಿದೆ, ದಯವಿಟ್ಟು ಸಂಬಂಧಿತ ಅನುಮತಿಗಳನ್ನು ಹಸ್ತಚಾಲಿತವಾಗಿ ನೀಡಿ"

"please_enter_password" : "ದಯವಿಟ್ಟು ಪಾಸ್‌ವರ್ಡ್ ನಮೂದಿಸಿ"

"repeat_password" : "ಪಾಸ್ವರ್ಡ್ ಪುನರಾವರ್ತಿಸಿ"

"set_password" : "ಪಾಸ್‌ವರ್ಡ್ ಹೊಂದಿಸಿ"

"user" : "USER"

"enter_password" : "पासवर्ड प्रविष्ट करा"

"password" : "पासवर्ड"

"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "कायमस्वरूपी अधिकृतता नाकारली, कृपया संबंधित परवानग्या व्यक्तिचलितपणे द्या"

"please_enter_password" : "कृपया संकेतशब्द प्रविष्ट करा"

"repeat_password" : "पासवर्ड पुन्हा करा"

"set_password" : "पासवर्ड सेट करा"

"user" : "USER"

"enter_password" : "پاس ورڈ درج کریں"

"password" : "پاس ورڈ"

"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "مستقل طور پر اجازت سے انکار کر دیا گیا، براہ کرم دستی طور پر متعلقہ اجازتیں دیں"

"please_enter_password" : "براہ کرم پاس ورڈ درج کریں"

"repeat_password" : "پاس ورڈ دہرائیں"

"set_password" : "پاس ورڈ سیٹ کریں"

"user" : "صارف"

"enter_password" : "গুপ্তশব্দ সুমুৱাওক"

"password" : "গুপ্তশব্দ"

"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "স্থায়ীভাৱে অস্বীকাৰ কৰা অনুমোদন, অনুগ্ৰহ কৰি প্ৰাসংগিক অনুমতিসমূহ হস্তচালিতভাৱে প্ৰদান কৰক"

"please_enter_password" : "অনুগ্ৰহ কৰি গুপ্তশব্দ দিয়ক"

"repeat_password" : "পাছৱৰ্ড পুনৰাবৃত্তি কৰক"

"set_password" : "গুপ্তশব্দ নিৰ্ধাৰণ কৰক"

"user" : "ব্যৱহাৰকাৰী"

"enter_password" : "પાસવર્ડ દાખલ કરો"

"password" : "પાસવર્ડ"
"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "કાયમી રૂપે અધિકૃતતા નકારી, કૃપા કરીને મેન્યુઅલી સંબંધિત પરવાનગીઓ આપો"
"please_enter_password" : "કૃપા કરીને પાસવર્ડ દાખલ કરો"
"repeat_password" : "પાસવર્ડ પુનરાવર્તિત કરો"
"set_password" : "પાસવર્ડ સેટ કરો"
"user" : "USER"
"enter_password" : "पासवर्ड दर्ज करो"
"password" : "पासवर्ड"
"permanently_denied_authorization_please_manually_grant_relevant_permissions" : "स्थायी रूप कन्नै मनाया गेआ प्राधिकरण, कृपा करियै मैन्युअल रूप कन्नै प्रासंगिक अनुमतियां देओ"
"please_enter_password" : "कृपया पासवर्ड दर्ज करो"
"repeat_password" : "पासवर्ड दोहराओ"
"set_password" : "पासवर्ड सेट करो"
"user" : "उपयोगकर्ता"

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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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
	危		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

android.permission.WRITE_SETTINGS	危险	修改全局系统设置	统的配置。
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.LAUNCH_APP	未知	Unknown permission	Unknown permission from android reference
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.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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
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_AUDIO	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
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
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕

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
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
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.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.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.lottery.monster.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信