MoGua

黑神话 24.10.151.APK 分析报告

APP名称:	黑神话

包名:	com.example.haijiao_shequ
域名线索:	24条
URL线索:	12条
邮箱线索:	2条
分析日期:	2024年10月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: hsh-24.10.081 (2).apk
文件大小: 18.09MB
MD5值: 9864b056934a8d87bb50c0a408edab91
SHA1值: f9b11c65ead32517e892eb20b5907c12b2eb2af4
SHA256值: 69907f5388b368254d65154825223f69e766da5b3cf1a36e289c11123990db12

APP 信息

App名称: 黑神话
包名: com.example.haijiao_shequ
主活动Activity: com.example.haijiao_shequ.MainActivity
安卓版本名称: 24.10.151
安卓版本: 1

域名线索

域名	服务器信息
cdr.pjnxuivy.shop	**IP**: 147.92.41.226 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
xbn.pzfxxyox.lat	**IP**: 147.92.41.226 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
bby.nlbaumko.cfd	**IP**: 147.92.41.226 **所属国家**: Hong Kong **地区**: Hong Kong

	城市: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
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
flutter.dev	IP: 199.36.158.100 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
jkt.pjnxuivy.lat	IP: 147.92.41.227 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
pkg.pzfxxyox.beauty	IP: 147.92.41.226 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
tbp.nyesimlv.pics	IP: 147.92.41.226 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
	IP: 185.199.110.153

aomedia.org	**所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
ns.adobe.com	没有服务器地理信息.
dashif.org	IP: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
developer.apple.com	IP: 17.253.85.203 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
xpt.cmkcaiof.lat	IP: 147.92.41.226 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
api.flutter.dev	IP: 199.36.158.100 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
default.url	没有服务器地理信息.

schemas.microsoft.com	**IP**: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
vcn.nyesimlv.lol	**IP**: 147.92.41.227 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
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
developer.android.com	**IP**: 142.250.69.206 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
developer.mozilla.org	**IP**: 34.111.97.67 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
lgh.nyesimlv.lat	**IP**: 147.92.41.226 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521

	经度: 114.157692
pbm.cmkcaiof.pics	**IP**: 147.92.41.226 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
xzn.pjnxuivy.pics	**IP**: 147.92.41.226 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
www.ibm.com	**IP**: 23.47.130.88 **所属国家**: Japan **地区**: Osaka **城市**: Osaka **纬度**: 34.694218 **经度**: 135.502228

URL线索

URL**信息**	Url**所在文件**
https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted	c2/z.java
https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread	g0/c1.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/h.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	k0/o0.java

https://x</LA_URL>	k0/n0.java
https://default.url	k0/n0.java
http://dashif.org/guidelines/last-segment-number	m1/d.java
http://dashif.org/guidelines/trickmode	m1/d.java
http://dashif.org/thumbnail_tile	m1/d.java
http://dashif.org/guidelines/thumbnail_tile	m1/d.java
https://developer.android.com/reference/javax/net/ssl/SSLSocket	t4/t.java
http://ns.adobe.com/xap/1.0/	q0/a.java
https://aomedia.org/emsg/ID3	a1/a.java
https://developer.apple.com/streaming/emsg-id3	a1/a.java
https://github.com/richtr/NoSleep.js/issues/15	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)	摸瓜V2引擎
https://jkt.pjnxuivy.lat	lib/armeabi-v7a/libapp.so
https://xbn.pzfxxyox.lat	lib/armeabi-v7a/libapp.so
https://bby.nlbaumko.cfd	lib/armeabi-v7a/libapp.so
https://cdr.pjnxuivy.shop	lib/armeabi-v7a/libapp.so
https://xpt.cmkcaiof.lat	lib/armeabi-v7a/libapp.so
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so

https://xzn.pjnxuivy.pics	lib/armeabi-v7a/libapp.so
https://lgh.nyesimlv.lat	lib/armeabi-v7a/libapp.so
https://pkg.pzfxxyox.beauty	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://pbm.cmkcaiof.pics	lib/armeabi-v7a/libapp.so
https://tbp.nyesimlv.pics	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues/new.	lib/armeabi-v7a/libapp.so
https://vcn.nyesimlv.lol	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues.	lib/armeabi-v7a/libflutter.so

邮箱线索

邮箱地址	所在文件
_nativesocket@14069316.listen _httpparser@13463476.responsepa _internetaddress@14069316.fixed _double@0150898.fromintege _future@4048458.immediate _growablelist@0150898._literal _link@14069316.fromrawpat _growablelist@0150898.withcapaci _growablelist@0150898._literal6	

_receiveportimpl@1026248.fromrawrec _colorfilter@15065589.mode _imagefilter@15065589.composed _list@0150898._ofarray _timer@1026248.periodic _growablelist@0150898._literal2 _bigintimpl@0150898.from _list@0150898.empty _directory@14069316.fromrawpat _invocationmirror@0150898._withtype _colorfilter@15065589.lineartosr _growablelist@0150898._literal1 _uri@0150898.file _imagefilter@15065589.blur _growablelist@0150898._literal4 _growablelist@0150898._ofgrowabl _growablelist@0150898.of _pointerpanzoomdata@481213599.fromupdate _nativesocket@14069316.pipe _cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring _list@0150898.of _list@0150898.generate _typeerror@0150898._create _assetmanifestbin@275287047.fromstanda _list@0150898._ofgrowabl _list@0150898._ofefficie _growablelist@0150898._ofarray _growablelist@0150898._literal3 _hashcollisionnode@367137193.fromcollis _growablelist@0150898._ofother _timer@1026248._internal _growablelist@0150898._literal5 _rawsocket@14069316._readpipe _socket@14069316._readpipe _list@0150898._ofother _bytebuffer@7027147._new ngstreamsubscription@4048458.zoned _assertionerror@0150898._create _nativesocket@14069316.normal _imagefilter@15065589.fromcolorf _filestream@14069316.forstdin	lib/armeabi-v7a/libapp.so

_colorfilter@15065589.srgbtoline _uri@0150898.directory _httpparser@13463476.requestpar _growablelist@0150898._literal8 _compressednode@367137193.single _growablelist@0150898.generate _uri@0150898.notsimple _growablelist@0150898._literal7 _future@4048458.zonevalue _growablelist@0150898._ofefficie _future@4048458.immediatee	
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

手机线索

手机号	所在文件
17512775099	i2/a.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: C=CA, ST=None, L=SHV, O=None, OU=None, CN=Wikky C
签名算法: rsassa_pkcs1v15
有效期自: 2023-06-09 03:39:58+00:00
有效期至: 2050-10-25 03:39:58+00:00
发行人: C=CA, ST=None, L=SHV, O=None, OU=None, CN=Wikky C
序列号: 0x35b37ea0
哈希算法: sha256

md5值: 9b91931ff2d154517acc60ab2e33c238
sha1值: 51bf171defbb6a3b4846f78a179f0c823cc48294
sha256值: cb641b208b6c97ddb14b0dab53d797b7bf797745e143a6d7eb1da85410519615
sha512值: 5bafd4f61bbc678b23c5efdb6a4cbe6c3f54f44fab69c5e729942646d6b9c4d41129f73fbd2feaa402285099e09cc7ae58578288317143b74ddc23468104915c
公钥算法: rsa
密钥长度: 2048
指纹: 5a1876f72fbd99be511379065c2219cfe83d4bb93e3a4c17bed583b14e4cd557

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	类型	详细情况

	险		
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.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.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.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_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.example.haijiao_shequ.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信