



缅北禁地 1.1.0.APK 分析报告



APP名称:

缅北禁地

包名:	myakkw.hqphiy.xojdbf
域名线索:	24条
URL线索:	19条
邮箱线索:	2条
分析日期:	2024年9月19日
分析平台:	摸瓜APK反编译平台

文件名: 202401101003_mbjd.apk
文件大小: 20.16MB
MD5值: d36c3a7f96b5aeaa26734c69dc4116c1
SHA1值: 4e1c00ddb41d04d0f1ed33a9d3633ac9f2cd8788
SHA256值: 1bbfb8a350e119b3afbe53f3514131e7585e4ba6b78d99236f7f454045163e1f

i APP 信息

App名称: 缅北禁地
包名: myakkw.hqphiy.xojdbf
主活动Activity: com.tbone.mbjd.MainActivity
安卓版本名称: 1.1.0
安卓版本: 1002

🔍 域名线索

域名	服务器信息
www.google.cn	IP: 58.254.137.162 所属国家: China 地区: Guangdong 城市: Yunfu 纬度: 22.930559 经度: 112.037300
www.ibm.com	IP: 23.13.189.250 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
exoplayer.dev	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
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
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
raw.githubusercontent.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
proton.flurry.com	没有服务器地理信息.
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000

	经度: 0.000000
gitee.com	IP: 180.76.198.77 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
vyxgsc.pjvhyfx.com	IP: 172.67.164.196 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
data.flurry.com	IP: 69.147.88.7 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.731323 经度: -73.990089
	IP: 104.21.23.24 所属国家: United States of America 地区: California

www.jsdelivr.com	城市: San Francisco 纬度: 37.775700 经度: -122.395203
wvseee.jsbacjr.com	IP: 104.21.31.88 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: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
vyxgsc.vqmfrb.com	IP: 172.67.190.16 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
ns.adobe.com	没有服务器地理信息.
staff.tea123.me	IP: 172.67.169.1 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700

	经度: -122.395203
aomedia.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
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
vyxgsc.ttvhhcx.com	IP: 104.21.54.139 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
http://ns.adobe.com/xap/1.0/\u0000	b/c/a/a.java
https://data.flurry.com/pcr.do	c/d/b/a0.java
https://data.flurry.com/aap.do	c/d/b/k0.java
http://data.flurry.com/aap.do	c/d/b/k0.java

https://proton.flurry.com/sdk/v1/config	c/d/b/s.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	c/e/a/a/g2.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	c/e/a/a/p2/k0.java
<a href="https://x</LA_URL>">https://x</LA_URL>	c/e/a/a/p2/j0.java
https://x	c/e/a/a/p2/j0.java
http://ns.adobe.com/xap/1.0/	c/e/a/a/q2/h0/a.java
https://aomedia.org/emsg/ID3	c/e/a/a/s2/j/a.java
https://developer.apple.com/streaming/emsg-id3	c/e/a/a/s2/j/a.java
http://www.w3.org/ns/ttml	c/e/a/a/v2/s/c.java
https://exoplayer.dev/issues/cleartext-not-permitted	c/e/a/a/x2/z.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/e.java
https://github.com/flutter/flutter/issues/2897).It	io/flutter/plugin/platform/l.java
https://developer.android.com/reference/javax/net/ssl/SSLSocket	io/flutter/plugins/d/t.java
https://www.google.cn/intl/zh-CN/chrome	Mogua Engine V2
https://www.jsdelivr.com/using-sri-with-dynamic-files	Mogua Engine V2
https://github.com/apvarun/toastify-js	Mogua Engine V2
https://github.com/richttr/NoSleep.js/issues/15	Mogua Engine V2
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released	Mogua Engine V2

http://www.w3.org/1998/Math/MathML	lib/armeabi-v7a/libapp.so
http://www.w3.org/2000/svg	lib/armeabi-v7a/libapp.so
https://vyxgsc.pjvhyfx.com/api.php	lib/armeabi-v7a/libapp.so
http://www.w3.org/2000/xmlns/	lib/armeabi-v7a/libapp.so
http://127.0.0.1:	lib/armeabi-v7a/libapp.so
https://vyxgsc.ttvhcx.com/api.php	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://raw.githubusercontent.com/little-5/backup/master/mbjd.txt	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html	lib/armeabi-v7a/libapp.so
https://wvsee.jsbacjr.com/mb.txt	lib/armeabi-v7a/libapp.so
https://staff.tea123.me/e.jpg	lib/armeabi-v7a/libapp.so
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
https://gitee.com/fdsaw/ffewelmcxww/raw/master/mb.txt	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android	lib/armeabi-v7a/libapp.so
https://vyxgsc.vqmfrb.com/api.php	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues/new	lib/armeabi-v7a/libapp.so
http://www.w3.org/XML/1998/namespace	lib/armeabi-v7a/libflutter.so

http://www.w3.org/2000/xmlns/	lib/armeabi-v7a/libflutter.so
https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues.	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues/73620.	lib/armeabi-v7a/libflutter.so

 邮箱线索

邮箱地址	所在文件
l@_dashoffsettype.percentage _growablelist@0150898._withdata n_typeerror@0150898._create _double@0150898.fromintege _growablelist@0150898._literal _immutablemap@0150898._create eo_bytebuffer@7027147._new l@boxwidthstyle.tight _casterror@0150898._create _assertionerror@0150898._create _immutablelist@0150898._dbb	lib/armeabi-v7a/libapp.so
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

 手机线索

手机号	所在文件
17512775099	c/e/b/c/a.java

🌸 签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=chengdu, ST=chengdu, L=chengdu, O=vg1704852144324, OU=nz1704852144324, CN=whri
签名算法: rsassa_pkcs1v15
有效期自: 2024-01-10 02:02:24+00:00
有效期至: 2073-12-28 02:02:24+00:00
发行人: C=chengdu, ST=chengdu, L=chengdu, O=vg1704852144324, OU=nz1704852144324, CN=whri
序列号: 0x34c4cd21
哈希算法: sha1
md5值: bdd1e87be7d9968a03f3ff465ac156e6
sha1值: bbc82c482e7bc31c0b63e8f8c1d3da3586f0a674
sha256值: 8529ec0e7704fcbdd228a47a71324edce7f67928b47ca4b1bfa8f889421bd83d
sha512值: 130360b9d85461f5c31c6926b7588d303fe492e2af53ff2c74a234e63dfa5dcd9bb63ee5576bb333b830425d072041879a96a7e183fd9fcefb438ca14fe58f79
公钥算法: rsa
密钥长度: 1024
指纹: c19b14fc900194cee2be7e5a85004788f600850fb38690da4f18fe5d53c21f9b

🔑 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.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.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.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.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
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.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference

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
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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度

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。