



MoGua

bad.news 0.0.42.APK 分析报告



APP名称:

bad.news

包名:	news.bad.app
域名线索:	26条
URL线索:	18条
邮箱线索:	3条
分析日期:	2025年8月2日
分析平台:	摸瓜APK反编译平台

文件名: 2_base.apk
文件大小: 26.11MB
MD5值: a63a9f89d8ebdac89a4b47635a790918
SHA1值: 7b6b0b732bce703f785ae44b9b3263f8eab74a84
SHA256值: c8b17e123659e9fb521cc2f858ff161e3dae234d872ddec1a72d95dd14779bdd

i APP 信息

App名称: bad.news
包名: news.bad.app
主活动Activity: news.bad.app.MainActivity
安卓版本名称: 0.0.42
安卓版本: 1

🔍 域名线索

域名	服务器信息
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
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
bad.news	IP: 108.160.170.44 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: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
www.ibm.com	IP: 104.84.146.202 所属国家: Germany 地区: Hamburg 城市: Hamburg 纬度: 53.575253 经度: 10.014778
pbs.twimg.com	IP: 151.101.88.159 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: 23.48.23.181 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
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
	IP: 199.36.158.100

flutter.dev	所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
ns.adobe.com	没有服务器地理信息.
s3.aaaaa.io	IP: 172.67.221.24 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
android.googleusercontent.com	IP: 108.177.98.82 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
docs.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
video.twimg.com	IP: 151.101.108.158 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
schemas.android.com	没有服务器地理信息.
	IP: 216.239.38.21

dartbug.com	所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
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
video-cloudflare.twimg.com	IP: 104.18.36.146 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
video.twimg.com.cdn.cloudflare.net	IP: 172.64.151.110 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
schemas.microsoft.com	IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903

www.unicode.org	IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204
img.lv2.com	IP: 202.160.129.37 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
exoplayer.dev	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
developer.android.com	IP: 142.251.215.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
dualstack.twimg.twitter.map.fastly.net	IP: 151.101.88.159 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	f6/s.java
https://exoplayer.dev/issues/cleartext-not-permitted	f4/f0.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	g2/k0.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	l2/i0.java
https://x</LA_URL>	l2/h0.java
https://x	l2/h0.java
http://ns.adobe.com/xap/1.0/	r2/a.java
http://dashif.org/guidelines/trickmode	n3/c.java
http://dashif.org/guidelines/trickmode	o3/e.java
http://dashif.org/guidelines/last-segment-number	o3/e.java
https://docs.flutter.dev/deployment/android	x1/r.java
https://developer.android.com/training/articles/direct-boot	y1/g.java
https://developer.android.com/guide/topics/permissions/overview	p3/u.java
https://aomedia.org/emsg/ID3	c3/a.java
https://developer.apple.com/streaming/emsg-id3	c3/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
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
bad.news	摸瓜V3引擎
https://docs.flutter.dev/deployment/android#what-are-the-supported-target-architectures	摸瓜V3引擎
https://github.com/richtr/NoSleep.js/issues/15	摸瓜V3引擎
http://dashif.org/guidelines/last-segment-number	摸瓜V3引擎
pbs.twimg.com	摸瓜V3引擎
https://api.flutter.dev/flutter/material/Scaffold/of.html	摸瓜V3引擎
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status	摸瓜V3引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released	摸瓜V3引擎
https://github.com/dart-lang/sdk/blob/master/runtime/docs/compiler/aot/entry_point_pragma.md	摸瓜V3引擎
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	摸瓜V3引擎
https://github.com/rodion-m/dio_smart_retry#retry-requests-with-multipartform-data	摸瓜V3引擎
http://dashif.org/guidelines/trickmode	摸瓜V3引擎
s3.aaaaa.io	摸瓜V3引擎
https://github.com/flutter/flutter/issues	摸瓜V3引擎
video.twimg.com	摸瓜V3引擎
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	摸瓜V3引擎

http://schemas.android.com/apk/res/android	摸瓜V3引擎
https://img.lv2.com	摸瓜V3引擎
video-cloudflare.twimg.com	摸瓜V3引擎
video.twimg.com.cdn.cloudflare.net	摸瓜V3引擎
http://www.unicode.org/copyright.html	摸瓜V3引擎
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android	摸瓜V3引擎
https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html	摸瓜V3引擎
img.lv2.com	摸瓜V3引擎
https://exoplayer.dev/issues/cleartext-not-permitted	摸瓜V3引擎
https://developer.android.com/guide/topics/permissions/overview	摸瓜V3引擎
https://dartbug.com/52121	摸瓜V3引擎
https://developer.android.com/training/articles/direct-boot	摸瓜V3引擎
https://bad.news	摸瓜V3引擎
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	摸瓜V3引擎
https://aomedia.org/emsg/ID3	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm-project	摸瓜V3引擎
dualstack.twimg.twitter.map.fastly.net	摸瓜V3引擎

http://www.unicode.org/copyright.html	lib/arm64-v8a/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	lib/arm64-v8a/libflutter.so
https://github.com/flutter/flutter/issues .	lib/arm64-v8a/libflutter.so
https://dartbug.com/52121 .	lib/arm64-v8a/libflutter.so
https://github.com/rodion-m/dio_smart_retry	lib/armeabi-v7a/libapp.so
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status	lib/armeabi-v7a/libapp.so
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://bad.news	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android .	lib/armeabi-v7a/libapp.so
http://www.unicode.org/copyright.html	lib/armeabi-v7a/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues .	lib/armeabi-v7a/libflutter.so
https://dartbug.com/52121 .	lib/armeabi-v7a/libflutter.so
http://www.unicode.org/copyright.html	lib/x86_64/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	lib/x86_64/libflutter.so
https://github.com/flutter/flutter/issues .	lib/x86_64/libflutter.so
https://dartbug.com/52121 .	lib/x86_64/libflutter.so



邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libflutter.so
_double@0150898.fromintege _growablelist@0150898._literal _growablelist@0150898.withcapaci _growablelist@0150898._literal6 _receivportimpl@1026248.fromrawrec _list@0150898._ofarray _timer@1026248.periodic _growablelist@0150898._literal2 _rawsocket@16069316._readpipe _list@0150898.empty _file@16069316.fromrawpat _nativesocket@16069316.normal _imagefilter@17065589.fromcolorf _invocationmirror@0150898._withtype storationinformation@135124995.fromserial authenticationscheme@15463476.fromstring _assetmanifestbin@48287047.fromstanda _growablelist@0150898._literal1 _uri@0150898.file _future@5048458.immediatee _compressednode@39137193.single _growablelist@0150898._literal4 _growablelist@0150898._ofgrowabl _growablelist@0150898.of _nativesocket@16069316.pipe _link@16069316.fromrawpat _list@0150898.of _list@0150898.generate _future@5048458.zonevalue _typeiderror@0150898._create _imagefilter@17065589.composed	lib/armeabi-v7a/libapp.so

🌸 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=Android Debug, O=Android, C=US
签名算法: rsassa_pkcs1v15
有效期自: 2023-04-05 00:32:51+00:00
有效期至: 2053-03-28 00:32:51+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha1
md5值: c40eb98f1fd3af88b279c6c9e5729183
sha1值: 94e44794e184f0b965f5c0a67bc1fed86c4931d5
sha256值: 72d9cd791aca3c6f2e58444628e2bd9098e2e4e06b157ee74869152bd48c9479
sha512值: 7afd8e355489f4c5cd8cb061a12b87037f780d05535d4dbd2a8db41db609c38765b4d7ffe4da59585d89fedfdd2090ffbfbab48f715807ca942dbecae9bea384
公钥算法: rsa
密钥长度: 2048
指纹: 6d08b2e66dcc82ad03faf7f39fcdab2e517466bcd9ccec11f2a2f00f2854acda

🔑 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.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.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.POST_NOTIFICATIONS	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.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.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

android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
news.bad.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
news.bad.app.MainActivity	Schemes: oauth2redirect://, Hosts: news.bad.app,

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。