MoGua

駿河屋 2.1.1.APK 分析报告

APP名称: 駿河屋

包名:	jp.surugaya.android
域名线索:	28条
URL线索:	2条
邮箱线索:	0条
分析日期:	2025年6月19日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 駿河屋_2.1.1_APKPure.apk
文件大小: 1.57MB
MD5值: a386da70a7a6bbb453823b4475ad3751
SHA1值: a2b7fef6c65885213e962e5a861e7eb5f321a7a5
SHA256值: 7a55d10cef815bee160138ba947d835d22b6a3ea380ca784b71e65ec089cbe6c

APP 信息

App名称: 駿河屋
包名: jp.surugaya.android
主活动Activity: jp.surugaya.android.LauncherActivity
安卓版本名称: 2.1.1
安卓版本: 67

域名线索

域名	服务器信息
www.google.nl	**IP**: 98.159.108.71 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052986 **经度**: -118.263687
connectivitycheck.gstatic.com	**IP**: 203.208.43.98 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
t.co	**IP**: 172.66.0.227 **所属国家**: United States of America **地区**: California

	城市: San Francisco **纬度**: 37.775700 **经度**: -122.395203
stats.g.doubleclick.net	**IP**: 114.250.67.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
analytics.twitter.com	**IP**: 104.244.46.21 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
www.googletagmanager.com	**IP**: 114.250.70.41 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
media.tenor.com	**IP**: 173.252.105.21 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.713192 **经度**: -74.006065
platform.twitter.map.fastly.net	**IP**: 151.101.88.157 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
	IP: 203.208.39.226

www.gstatic.com	**所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
googleads.g.doubleclick.net	**IP**: 114.250.65.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
bat.bing.com	**IP**: 150.171.27.10 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
s.twitter.com	**IP**: 199.59.149.204 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
plusinbound.hachidori.io	**IP**: 35.72.71.210 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
plus.hachidori.io	**IP**: 3.165.11.110 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199

www.suruga-ya.jp	**IP**: 46.51.247.29 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
surugaya-f-s.snva.jp	**IP**: 35.73.234.141 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
surugaya2-f-s.snva.jp	没有服务器地理信息.
search-surugaya2-alb-front-1824450475.ap-northeast-1.elb.amazonaws.com	没有服务器地理信息.
googlehosted.l.googleusercontent.com	**IP**: 142.250.217.65 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
kitchen.juicer.cc	**IP**: 54.150.84.47 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
suruga-ya.jp	**IP**: 46.51.247.29 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322

blank.juicer.cc	**IP**: 3.165.102.69 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
static.ads-twitter.com	**IP**: 151.101.88.157 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
ads.twitter.com	**IP**: 199.96.59.95 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
edgedl.me.gvt1.com	**IP**: 34.104.35.123 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
lh3.googleusercontent.com	**IP**: 142.250.217.65 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
lh3-dz.googleusercontent.com	**IP**: 142.250.217.97 **所属国家**: United States of America **地区**: California **城市**: Mountain View

	纬度: 37.405991 **经度**: -122.078514
c.tenor.com	**IP**: 69.63.186.30 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.713192 **经度**: -74.006065

URL线索

URL信息	Url所在文件
https://www.suruga-ya.jp	摸瓜V1引擎
https://www.suruga-ya.jp/	摸瓜V1引擎
https://www.suruga-ya.jp/pwa?utm_source=pwa&utm_medium=none&utm_campaign=home_screen	摸瓜V1引擎
https://www.suruga-ya.jp/manifest.json	摸瓜V1引擎
www.google.nl	摸瓜V3引擎
connectivitycheck.gstatic.com	摸瓜V3引擎
t.co	摸瓜V3引擎
growth-pa.googleapis.com	摸瓜V3引擎
stats.g.doubleclick.net	摸瓜V3引擎
analytics.twitter.com	摸瓜V3引擎

www.googletagmanager.com	摸瓜V3引擎
content-autofill.googleapis.com	摸瓜V3引擎
https://www.suruga-ya.jp/pwa?utm_source=pwa&utm_medium=none&utm_campaign=home_screen	摸瓜V3引擎
android.googleapis.com	摸瓜V3引擎
media.tenor.com	摸瓜V3引擎
gugqrzdzvnjzo	摸瓜V3引擎
platform.twitter.map.fastly.net	摸瓜V3引擎
https://www.suruga-ya.jp	摸瓜V3引擎
https://www.suruga-ya.jp/manifest.json	摸瓜V3引擎
www.gstatic.com	摸瓜V3引擎
googleads.g.doubleclick.net	摸瓜V3引擎
bat.bing.com	摸瓜V3引擎
s.twitter.com	摸瓜V3引擎
plusinbound.hachidori.io	摸瓜V3引擎
plus.hachidori.io	摸瓜V3引擎
surugaya-f-s.snva.jp	摸瓜V3引擎
www.suruga-ya.jp	摸瓜V3引擎

surugaya2-f-s.snva.jp	摸瓜V3引擎
qalqhvldvo	摸瓜V3引擎
search-surugaya2-alb-front-1824450475.ap-northeast-1.elb.amazonaws.com	摸瓜V3引擎
googlehosted.l.googleusercontent.com	摸瓜V3引擎
kitchen.juicer.cc	摸瓜V3引擎
www.googleapis.com	摸瓜V3引擎
enxhwsb	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
blank.juicer.cc	摸瓜V3引擎
static.ads-twitter.com	摸瓜V3引擎
instantmessaging-pa.googleapis.com	摸瓜V3引擎
clientservices.googleapis.com	摸瓜V3引擎
https://suruga-ya.jp/	摸瓜V3引擎
ads.twitter.com	摸瓜V3引擎
update.googleapis.com	摸瓜V3引擎
edgedl.me.gvt1.com	摸瓜V3引擎
lh3.googleusercontent.com	摸瓜V3引擎

lh3.googleusercontent.com	摸瓜V3引擎
gnpfesdk-pa.googleapis.com	摸瓜V3引擎
https://www.suruga-ya.jp/&&https://www.suruga-ya.jp/manifest.jsonTThttps://www.suruga-ya.jp/pwa?utm_	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
lh3-dz.googleusercontent.com	摸瓜V3引擎
https://www.suruga-ya.jp/	摸瓜V3引擎
c.tenor.com	摸瓜V3引擎

邮箱线索

手机线索

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=jp, ST=Unknown, L=Tokyo, O=Digital Circus, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2010-11-09 13:04:25+00:00
有效期至: 2038-03-27 13:04:25+00:00
发行人: C=jp, ST=Unknown, L=Tokyo, O=Digital Circus, OU=Unknown, CN=Unknown
序列号: 0x4cd946d9
哈希算法: sha1
md5值: bbdec5d3f32e5f6a3511f2b8c3606119

sha1值: 6ddb1482eb1ad029e1fba55af0d0e723927c6598
sha256值: 085253f4979132899458213c102382a8c47f0daeb1376aba7632c257150de0cb
sha512值: 43a883f1b2deb29eeff5e7e49d54f4abbcc28f64d099e085ae68e231d042260dfefcdaffd71f66a87535a208d53eb94b528d5e42f861af6fb52a7ff46f82952e
公钥算法: rsa
密钥长度: 1024
指纹: c1bc6e609beea7a2da87d6e4b4ab7a2da35008209df5e0df04874d64df59f0f0

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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference

		permission	
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
jp.surugaya.android.LauncherActivity	Schemes: https://, Hosts: @string/hostName,

---

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。