

APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



♣ 店小伙 1.2.APK

APP名称: 店小伙

包名: com.dianxiaohuo.storemanager

域名线索: 1条

URL线索: 4条

邮箱线索: 0条

分析日期: 2022年2月2日 19:43

文件名: dianxiaohuo.apk

文件大小: 4.04MB

MD5值: 9e1795805250dd7e05ac3366b08eff01

SHA1值: 7a975bd911883dca14baac464a7df7873d8f8ec5

SHA256值: c5e4a2890525bc908bb80255bdc336916da7d696a7da3f676341dfce19f9611d

i APP 信息

App名称: 店小伙

包名: com.dianxiaohuo.storemanager

主活动**Activity:** com.dianxiaohuo.storemanager.GuideActivity

安卓版本名称: 1.2

安卓版本: 3

0 域名线索

域名	是否危险域名	服务器信息
app.dxherp.com	good	IP: 47.95.127.60 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map



URL信息	Url所在文件
http://app.dxherp.com/h5/	com/dianxiaohuo/storemanager/MainActivity.java
https://)(com/huawei/hms/scankit/p/C0061kb.java

₩ 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.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.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

*签名证书

APK is signed v1 signature: True v2 signature: True v3 signature: False

Found 1 unique certificates

Subject: ST=BJ, L=BJ, O=DXH, OU=GS, CN=BJ Signature Algorithm: rsassa_pkcs1v15 Valid From: 2021-06-10 09:12:27+00:00 Valid To: 2046-06-04 09:12:27+00:00 Issuer: ST=BJ, L=BJ, O=DXH, OU=GS, CN=BJ Serial Number: 0x661cf184 Hash Algorithm: sha256

md5: b651f852b6e200179590e918f9e9c6a6

sha1: ffba426a168229e4f708a4566d3e9e15697657c4

sha256: 969e7e468616385a952517775093fb33c61ab972a01f536ee56797852e539f07

sha512: b94bdab8f71787430e369f00d8fc340f687af84e768ff735c720abaca5c669e395b474bcf8fce19bd2b33c835057a0c7f22d33b5c2be1e924cd12a5a937a0c36

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: b66fd238bfcca2dfaf42e3c3a543b7a9f9a60d0db4acf6eded5c386de073b2b3

Exodus威胁情报

名称	分类	URL链接
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333

₽ 硬编码敏感信息

可能的敏感信息

"maintain_user":"隐私政策"

命加壳分析

文件列表	分析结果
------	------

文件列表	分析结果			
	壳列表	详细情况		
classes.dex	反虚拟机	Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check		
	编译器	r8		
	<u> </u>			

报告由 摸瓜平台 自动生成,并非包含所有检测结果,有疑问请联系管理员。

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析