```
print (“Hello,
Bread&Net!”);
project.att(){
/*
// protection =
// rights +
// tech +
// tools;
```

## كشف برامج التجسس في التطبيقات اليومية

# ورشة عملية للصحفيين والناشطين

المدة دقيقة 75

المكان بيروت، لبنان

30 OCT 2025

جوسا

خبز ونت ‘٢٥
bread&net ‘25

# المحاور الرئيسية

1. ما هي برامج التجسس؟
2. لماذا يُعدّ هذا الأمر مهمًا؟
3. بعض الأمثلة من الواقع
4. تدرّيب عملي على كيفية تحليل تطبيقات الأندرويد

# مـاذا ستـتـعـلـم

1. فهم ما هي برامج التجسس ومخاطرها
2. فحص التطبيقات باستخدام آداة Pithus – أداة تحليل مفتوحة المصدر
3. اكتشاف الأذونات المشبوهة والمتتبعات المخفية داخل التطبيق
4. شرح ومشاركة النتائج لحماية مجتمعك

# ما هي برامج التجسس؟

1. برنامج التجسس تقوم بجمع البيانات من هاتفك بشكل سري
2. يمكن لهذه البرامج تتبع الرسائل والمكالمات والموقع والنشاط عبر الإنترنت
3. يتم تثبيتها على جهازك من دون علمك

# لماذا يُعدّ هذا الأمر مهمًا؟

يمكن لبرامج التجسس أن تكشف عن مصادر معلوماتك وجهات اتصالك السرية

قد تؤدي ايضا إلى تسريب القصص أو المضايقة أو التهديدات القانونية

يمكن لهذه البرامج تتبّع موقعك أثناء رحلات التغطية الصحفية

لذلك يجب عليك ان تصبح المحقق الرقمي الخاص بك

# أمثلة من الواقع

The Guardian

## WhatsApp says journalists and civil society members were targets of Israeli spyware

Nearly 100 journalists and other members of civil society using WhatsApp, the popular messaging app owned by Meta, were targeted by spyware owned by Paragon...

Jan 31, 2025


The Hacker News

## New ClayRat Spyware Targets Android Users via Fake WhatsApp and TikTok Apps

ClayRat Android spyware uses fake apps and Telegram to steal data and spread via contacts.

4 days ago

Al Jazeera

## Journalists, activists targeted in Jordan with Israeli-made Pegasus spyware

The mobile phones of more than 30 people in Jordan, including journalists, lawyers and activists, were hacked with the Israeli-made Pegasus...

Feb 1, 2024

BBC

## Pegasus: Spyware sold to governments 'targets activists'

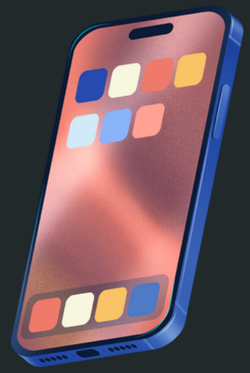
An Israeli woman uses her iPhone in front of the building housing the Israeli NSO group, on August 28, 2016, in Herzliya, near Tel Aviv.

Jul 19, 2021

# المحاور الرئيسية

1. ما هي برامج التجسس؟
2. لماذا يُعدّ هذا الأمر مهمًا؟
3. بعض الأمثلة من الواقع
4. تدرّيب عملي على كيفية تحليل تطبيقات الأندرويد

# خطوات تحليل التطبيق؟

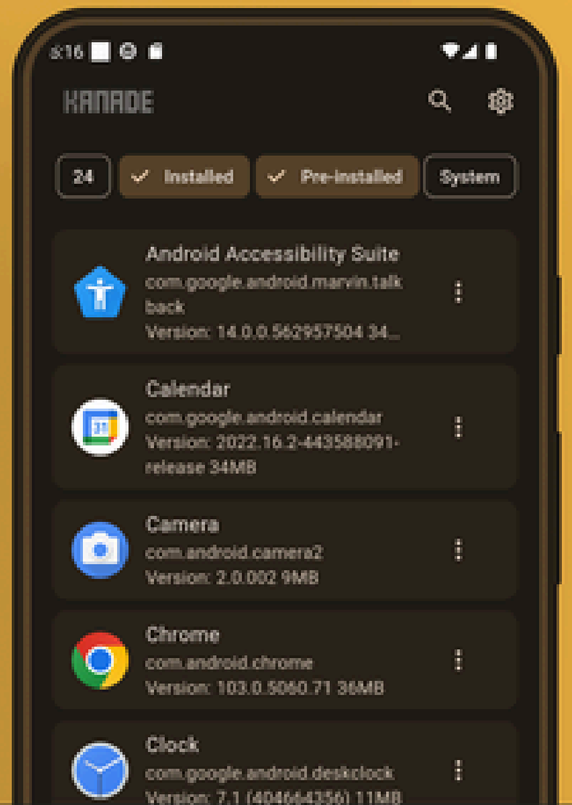


اختيار تطبيق
مشبوه

استخراج التطبيق
من الهاتف

استعمال آداة
لتحليل المخاطر

# استخراج التطبيق من هاتفك

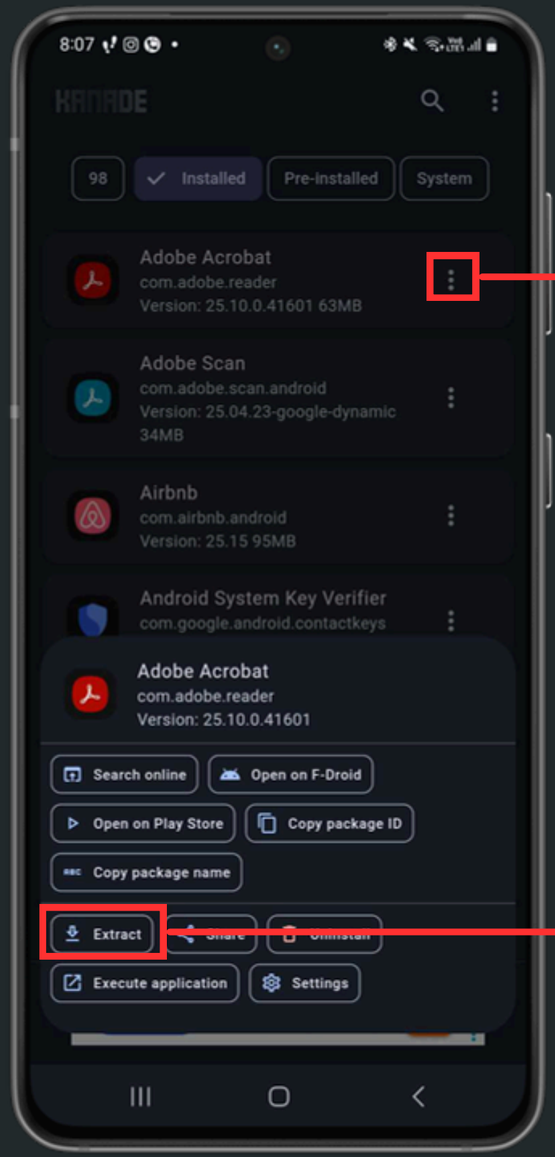



KANADE

Open source apk extractor app.

Download The App
via Play Store

# استخراج التطبيق من هاتفك



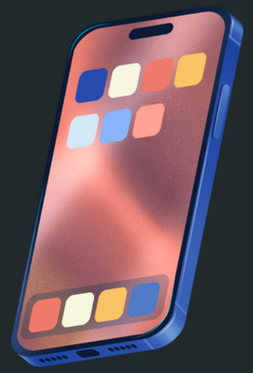

اختر التطبيق الذي تريد استخراجه عن طريق الضغط على النقاط، ثم قم بأستخراج التطبيق عن طريق زر Extract.

بعد حفظ التطبيق المستخرج (APK) يمكنك نقله على جهاز الحاسوب عن طريق اي USB Cable بسهولة للقيام بعملية التحليل.

# خطوات تحليل التطبيق؟

استعمال آداة
لتحليل المخاطر

استخراج التطبيق
من الهاتف



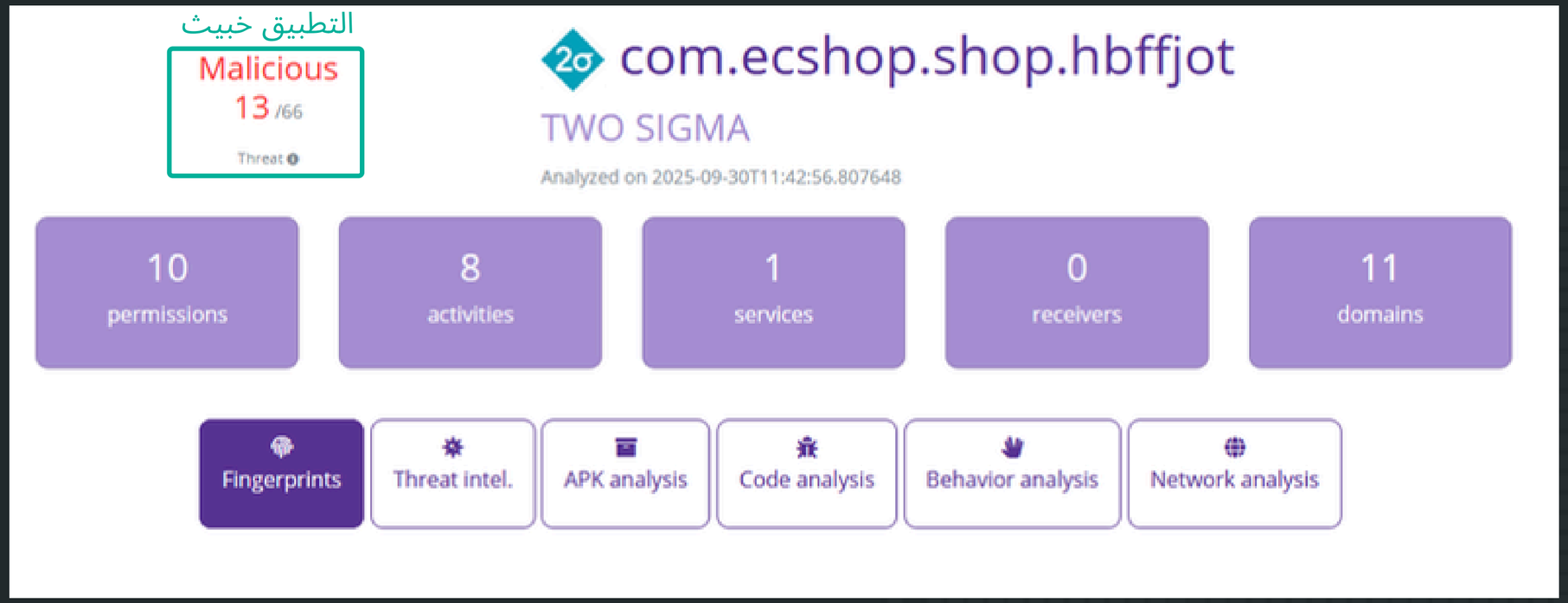
اختيار تطبيق
مشبوه

# تحليل التطبيق بأستخدام اداة Pithus

هي منصة مجانية ومفتوحة المصدر لتحليل Pithus
البرمجيات الضارة، مصممة خصيصًا لتطبيقات ألأندرويد
(APKs)

https://beta.pithus.org

# تحليل Pithus




Sample link

# تحليل Pithus

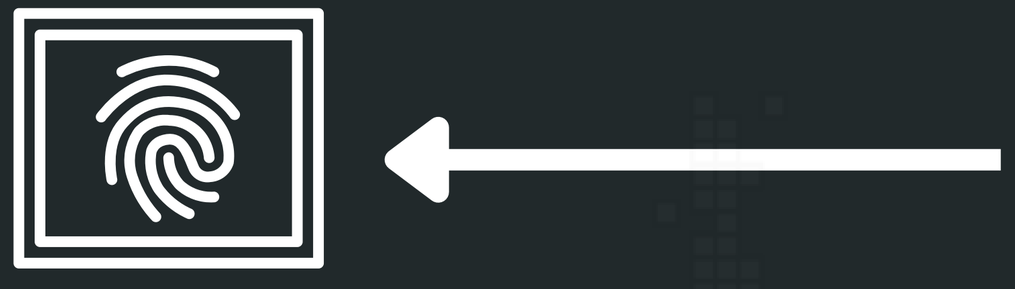
Fingerprints | Threat Intel. | APK Analysis | Code Analysis | Behavior Analysis | Network Analysis

# بصمة رقمية للتطبيق

## File sums

| | |
|---|---|
| MD5 | f47df545387d24d6308ba399feec4b8e |
| SHA1 | 79e6c89a4a12216403d0758e82731900690b4b54 |
| SHA256 | 5bbc7312cf8096e7c11912f443c74f088d41b237c0d79e3498cdca370750cba1 |
| Size | 6.31MB |

# ما هو ال Hashing؟



Chrome.apk

5a00be6e1e8304d4
124f815f0346ebd0

بصمة رقمية للملفات

## خصائص ال Hashing

1. فريد
2. حتمي

# نـتـائـج APKiD

المعلومات المستخرجة من خلال التطبيق
هذه المعلومات يمكن ان تكون معلومات حساسة

من هذه المعلومات VM check الذي يتاكد من استخدام
Virtual Machine (VM) لتشغيل التطبيق

| /tmp/tmp2onf1_ay!classes.dex | |
|---|---|
| anti_vm | Build.FINGERPRINT check<br>Build.MODEL check<br>Build.MANUFACTURER check<br>Build.BRAND check<br>Build.DEVICE check<br>Build.PRODUCT check<br>possible Build.SERIAL check<br>SIM operator check<br>network operator name check<br>possible VM check |
| compiler | r8 without marker (suspicious) |

مُجمِّع r8 هو مُجمِّع يحول مصدر الكود الى تطبيق يمكن تشغيله على
الهاتف, ولكن بشكل مشفر ويصعب استرجاعه

# نـتـائـج SSdeep و Dexofuzzy

النتائج تبين تطبيقات مشابه لهذا التطبيق

من خلال fuzzy hashes التي تظهر اي تطبيقات قريبة من التطبيق الذي يتم تحليله

## SSdeep

Information computed with ssdeep.

| | |
|---|---|
| APK file | 196608:DPKlhg8GQULRO5VfybP+E8bgbWQ/BN/410l:7KlhdR5Vab4bY5/BN/4g |
| Manifest | 192:90uZPZPAeDzOUbtyna0hVkrsGyOMO/OTO6ezBtCoVkx1vTUzrjSj+zELysP14Vm+:… |
| classes.dex | 196608:Gt9w2tL+auMrib6f+Um/RPLFbxBnfP5GPvr:kmh2ib6f+Um/RPLFbxBnfRGb |
| classes2.dex | 49152:slLH4ij8QtmVhn+oYwKffFFZ6RuZ+XEQsi8zfX:0EVgoQFZj |

## Dexofuzzy

Information computed with Dexofuzzy.

| | |
|---|---|
| APK file | 12288:9KwshqzV1v32b59j3U60Nvl84xuF0Gfmakzv:YwHt3O5NAOFfm9zv |
| classes.dex | 6144:9Kws7t57MzV1vBMujWG36/Bb59nj3IxO3JwMTEje0Q0vlrJOyk4pC44PbA4FJF0M… |
| classes2.dex | 3072:8/iR63nsZFQDR1WZuq3UKH+X4sjvakziBKKKKuto7ox:8/i03sSbGuyuosjvakziw |

# تحليل Pithus

Fingerprints | **Threat Intel.** | APK Analysis | Code Analysis | Behavior Analysis | Network Analysis

# الجدول الزمني للتطبيق

## Sample timeline

| | |
|---|---|
| Oldest file found in APK | Jan. 1, 1981, 1:01 a.m. |
| Latest file found in APK | Jan. 1, 1981, 1:01 a.m. |
| Certificate valid not before | June 18, 2021, 3:56 p.m. |
| First submission on VT | Sept. 30, 2025, 6:28 a.m. |
| Last submission on VT | Sept. 30, 2025, 7:17 a.m. |
| Upload on Pithus | Sept. 30, 2025, 11:42 a.m. |
| Certificate valid not after | June 12, 2046, 3:56 p.m. |

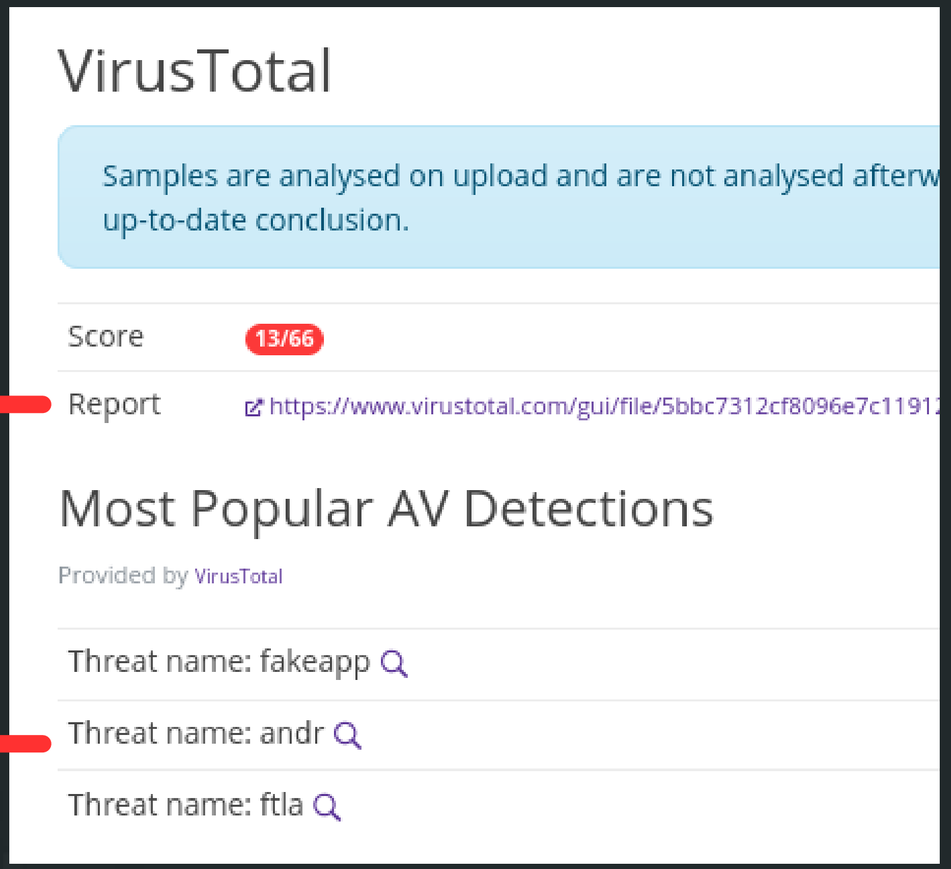
ظهور التطبيق على منصة VirusTotal

ظهور التطبيق على Pithus

# نـتـائـج خـارجـيـة

من بين 66 anti-virus الذي قاموا بفحص
الملف، صنف انه تطبيق خبيث من قبل 13

ظهر نفس التطبيق باسماء مختلفة



# تحليل Pithus

Fingerprints | Threat Intel. | **APK Analysis** | Code Analysis | Behavior Analysis | Network Analysis

# تـفـاصـيـل APK

| | |
|---|---|
| Package | com.wire |
| App name | Wire |
| Version name | 3.65.979 |
| Version code | 979 |
| SDK | 18 - 22 |
| UAID | 60c18d14be88e9af123c54989cafea86527f7b30 |
| Signature | Signature V1 |
| Frosting | Not frosted |

البيانات الوصفية توكد ان التطبيق تم نشره على Google Play Store وقام المستخدم تثبيته من خلال Google Play Store

التوقيع الرقمي يؤكد موثوقية التطبيق

# مقارنة مع التطبيق الأساسي

| | |
|---|---|
| Package | com.wire |
| App name | Wire |
| Version name | 3.65.979 |
| Version code | 979 |
| SDK | 18 - 22 |
| UAID | 60c18d14be88e9af123c54989cafea86527f7b30 |
| Signature | Signature V1 |
| Frosting | Not frosted |

| | |
|---|---|
| Package | com.wire |
| App name | Wire |
| Version name | 3.65.979 |
| Version code | 979 |
| SDK | 24 - 30 |
| UAID | 0e5427f51b20ea156a7c6bf9e40262112756a308 |
| Signature | Signature V1 Signature V2 |
| Frosting | Frosted<br>Blocks found within V2 signature:<br>0x7109871a: Unknown<br>0x42726577: Verity padding<br>0x2146444e: Google metadata |

# تفاصيل شهادة رقمية

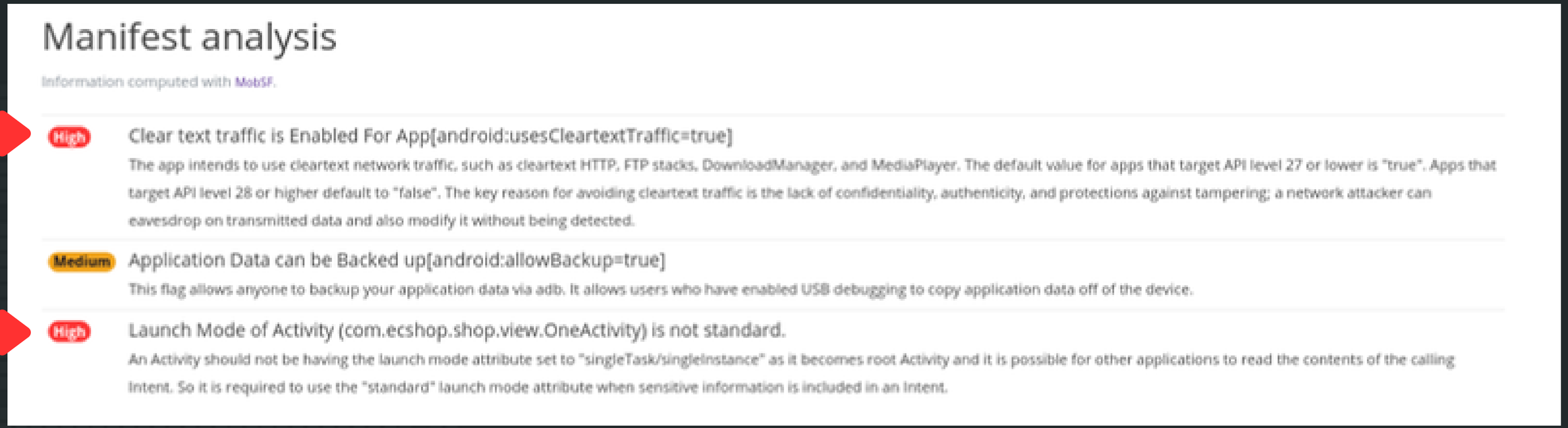
## Certificate details

Information computed with AndroGuard.

| | |
|---|---|
| MD5 | 4cab072675d38b13eb15c82fb99917ee |
| SHA1 | 0fdd367c0a1ee16ecc935407ab42b839bd3ae778 |
| SHA256 | a2146890906d91d5bae3a29500d41aa8a5feef2967206d0e7cf06d3ab967579b |
| Issuer | Common Name: vvvv, Organizational Unit: 3333, Organization: 深圳宇宙学研究所, Locality: 深圳, State/Province: 1, Country: 86 |
| Not before | 2021-06-18T15:56:01+00:00 |
| Not after | 2046-06-12T15:56:01+00:00 |

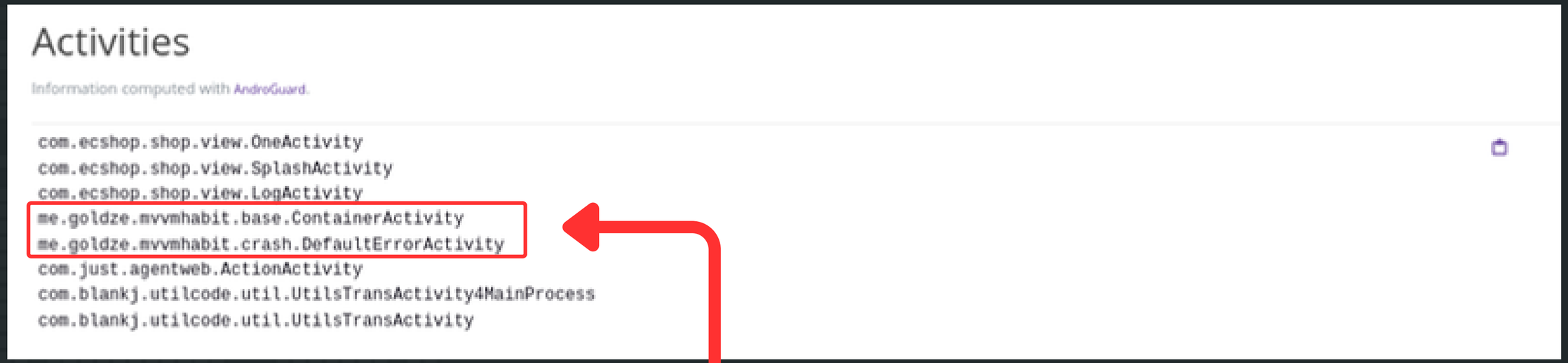
منظمة غريبة

# تحليل الmanifests




بعض الmanifests تحتوي على كود غير آمن الذي قد يسبب اختراق للجهاز

# الأنــشطـة

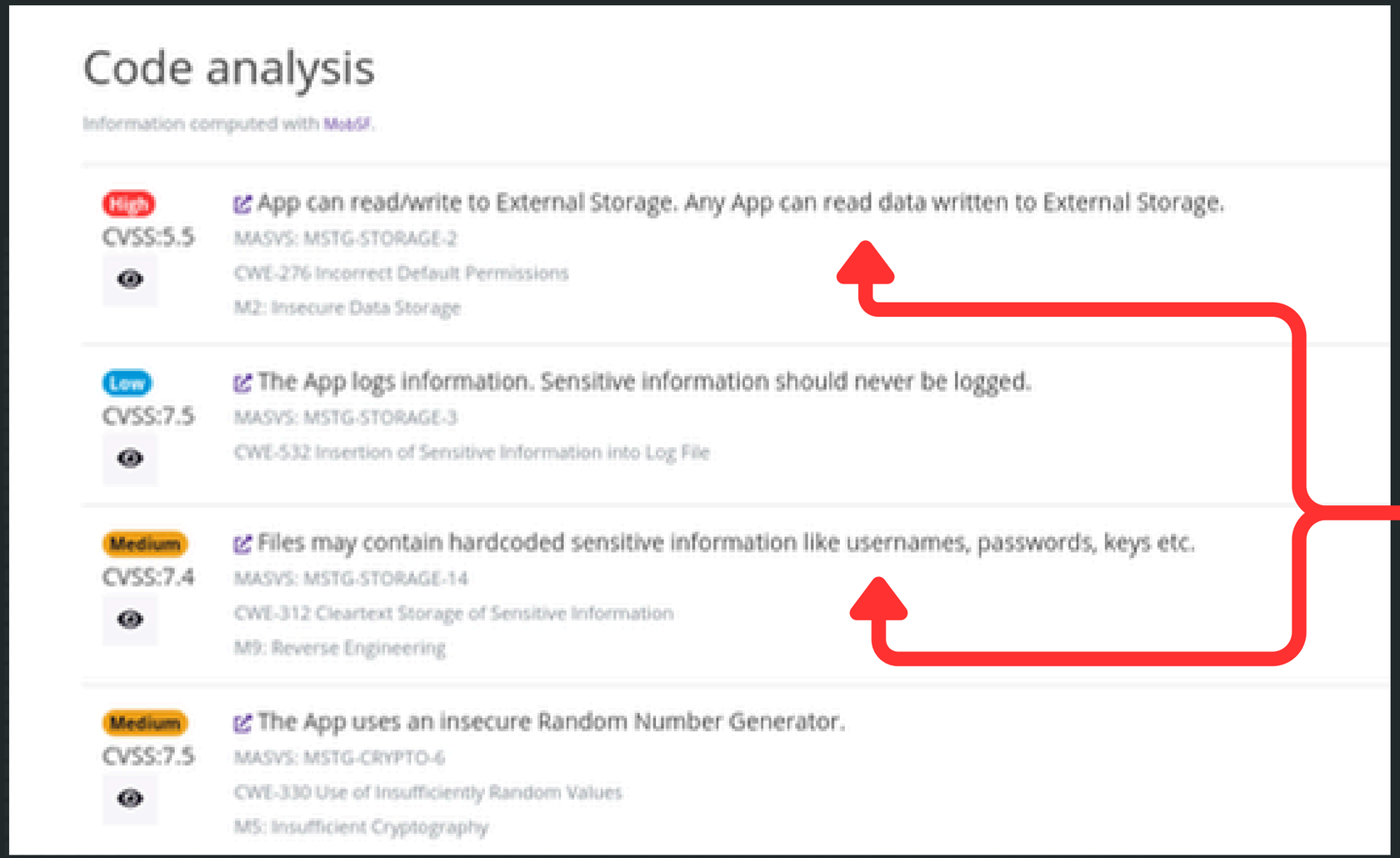



بعض الأنشطة يمكن ان تكون مثير للشك

# Pithus تحليل

Fingerprints | Threat Intel. | APK Analysis | **Code Analysis** | Behavior Analysis | Network Analysis

# تـحـلـيـل الـكـود




كود التطبيق يحتوي على ثغرات, التي تصنف حسب خطورتها:

- high
- medium
- low
- info

يمكن للمهاجم ان يخترق هذه الثغرات للوصول الى معلومات على الجهاز

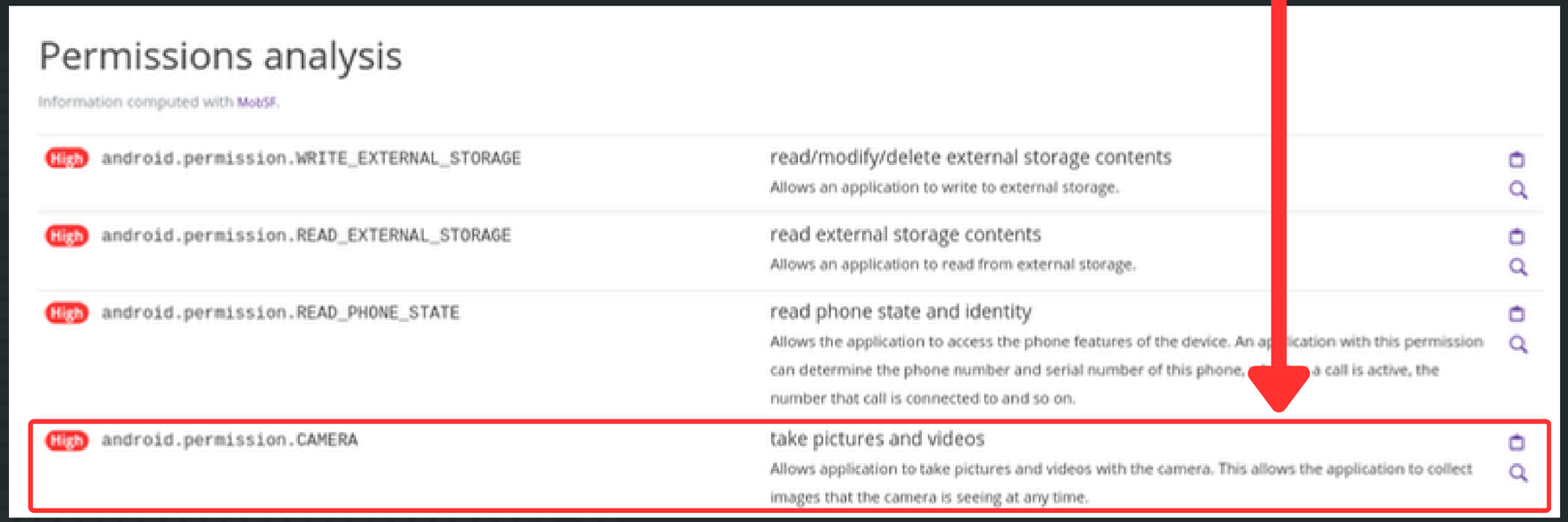
# تحليل Pithus

Fingerprints | Threat Intel. | APK Analysis | Code Analysis | **Behavior Analysis** | Network Analysis

# تـحـلـيـل الأذونـات

التطبيق ممكن ان يطلب permissions
خارج عن نطاق استخدامات التطبيق

هذه الpermissions ممكن انتسخدم
لتجسس على مالك الجهاز



# تحليل الthreats

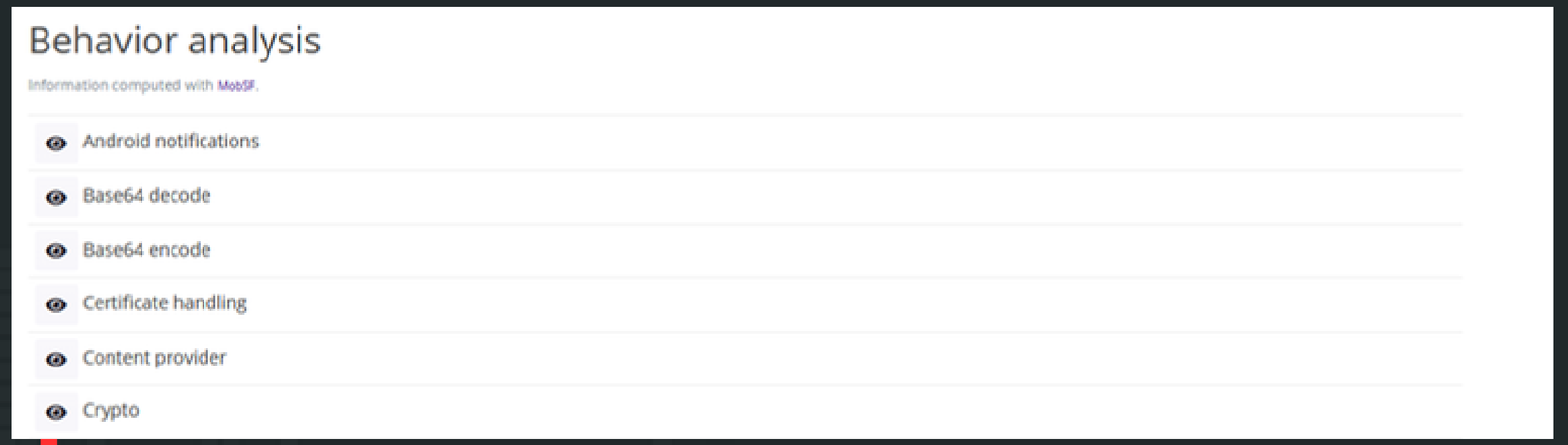
## Threat analysis

Information computed with Quark-Engine.

| | |
|---|---|
| Confidence: 100% | Load external class |
| Confidence: 100% | Query the current data network type |
| Confidence: 100% | Implicit intent(view a web page, make a phone call, etc.) |
| Confidence: 100% | Find a method from given class name, usually for reflection |
| Confidence: 100% | Read data and put it into a buffer stream |
| Confidence: 100% | Connect to a URL and receive input stream from the server |
| Confidence: 100% | Method reflection |
| Confidence: 100% | Install other APKs from file |
| Confidence: 100% | Connect to a URL and read data from it |
| Confidence: 100% | Read file and put it into a stream |
| Confidence: 100% | Load class from given class name |
| Confidence: 100% | Retrieve data from broadcast |
| Confidence: 100% | Read sensitive data(SMS, CALLLOG, etc) |
| Confidence: 100% | Open a file from given absolute path of the file |
| Confidence: 100% | Implicit intent(view a web page, make a phone call, etc.) via setData |

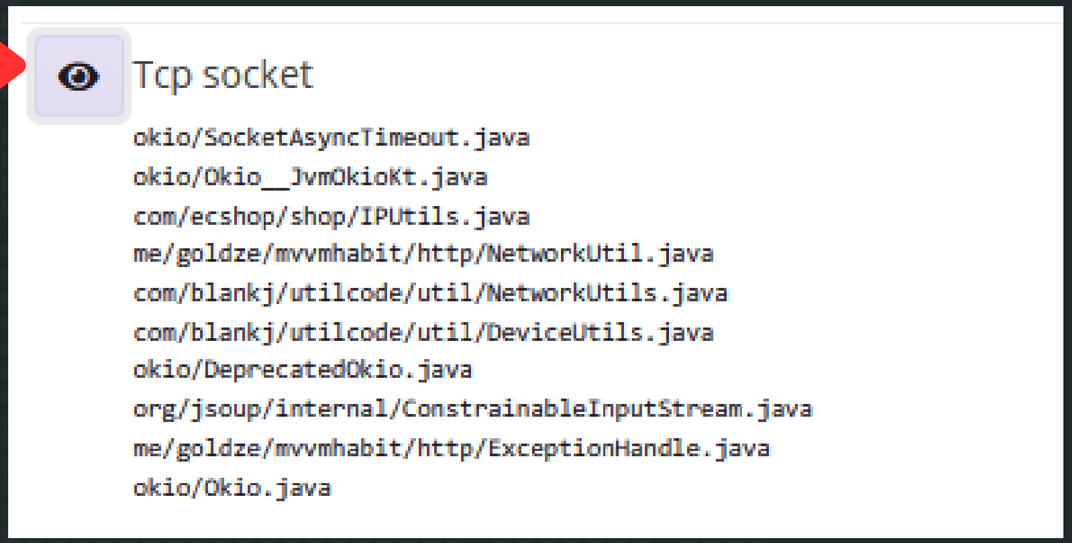
التطبيق قد يرتكب جرائم (crimes) ,هذه
الجرائم تعتبر خطرًا على مستخدم الجهاز

# تحليل السلوكيات




السلوكيات هي الأنشطة التي ينفذها التطبيق بالتفصيل

من هذه السلوكيات هي المواصلات بين التطبيق مع الانترنت

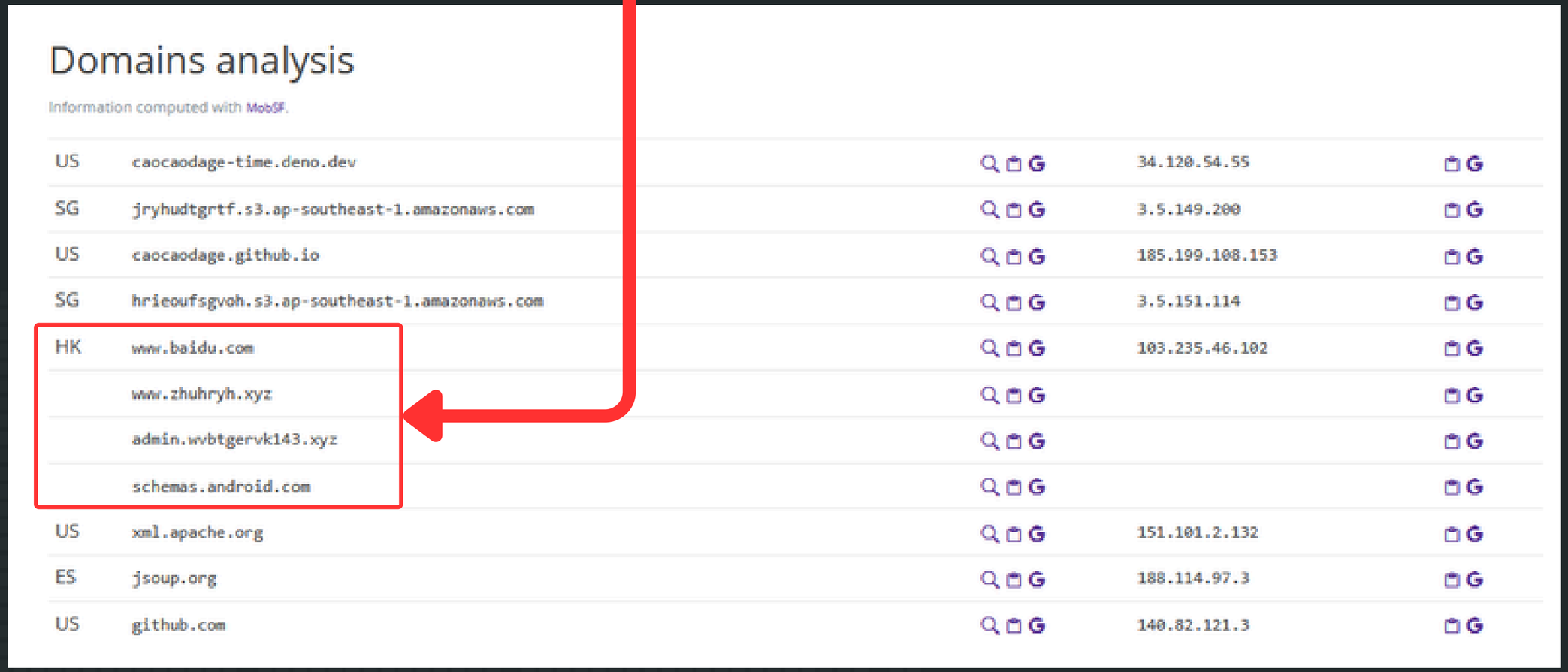


# تحليل Pithus

Fingerprints | Threat Intel. | APK Analysis | Code Analysis | Behavior Analysis | **Network Analysis**

# تحليل التواصل مع المواقع الخارجية

تواصل التطبيق مع مواقع في Hong Kong



## Domains analysis

Information computed with MobSF.

| | | | |
|---|---|---|---|
| US | caocaodage-time.deno.dev | 34.120.54.55 | |
| SG | jryhudtgrtf.s3.ap-southeast-1.amazonaws.com | 3.5.149.200 | |
| US | caocaodage.github.io | 185.199.108.153 | |
| SG | hrieoufsgvoh.s3.ap-southeast-1.amazonaws.com | 3.5.151.114 | |
| HK | www.baidu.com | 103.235.46.102 | |
| | www.zhuhryh.xyz | | |
| | admin.wvbtgervk143.xyz | | |
| | schemas.android.com | | |
| US | xml.apache.org | 151.101.2.132 | |
| ES | jsoup.org | 188.114.97.3 | |
| US | github.com | 140.82.121.3 | |

# تحليل التواصل مع المواقع الخارجية

هذه المواقع غير موثوقة

وهذا كل شيء يا أصدقاء!

# هل لديكم اي سؤال؟

# شكرًا لكم

Follow Us

خبز و نت ’٢٥
bread&net ’25

جوسا