

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

كشف برامج التجسس في
التطبيقات اليومية

ورشة عملية للصحفيين والناشطين

المدة 75 دقيقة

المكان بيروت، لبنان

30 OCT 2025

خبز و نت '25
bread&net

جوسا 

المحاور الرئيسية

- 1 ما هي برامج التجسس؟
- 2 لماذا يُعدُّ هذا الأمر مهمًا؟
- 3 بعض الأمثلة من الواقع
- 4 تدريب عملي على كيفية تحليل تطبيقات الأندرويد



ماذا ستعلم

1 فهم ما هي برامج التجسس ومخاطرها

2 فحص التطبيقات باستخدام أداة 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

3 يتم تثبيتها على جهازك من دون علمك

2 يمكن لهذه البرامج تتبع الرسائل والمكالمات والموقع والنشاط عبر الإنترنت



لماذا يُعدّ هذا الأمر مهمًا؟

يمكن لبرامج التجسس أن تكشف عن مصادر معلوماتك وجهات اتصالاتك السرية



قد تؤدي أيضا 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

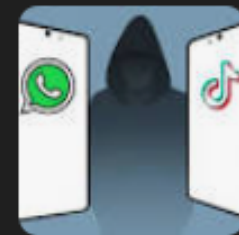



 The Hacker News

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

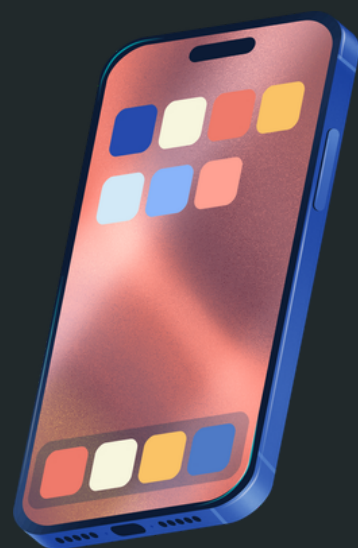


المحاور الرئيسية

- 1 ما هي برامج التجسس؟ ✓
- 2 لماذا يُعدُّ هذا الأمر مهمًا؟ ✓
- 3 بعض الأمثلة من الواقع ✓
- 4 تدريب عملي على كيفية تحليل تطبيقات الأندرويد



خطوات تحليل التطبيق؟



اختيار تطبيق
مشبوه



استخراج التطبيق
من الهاتف

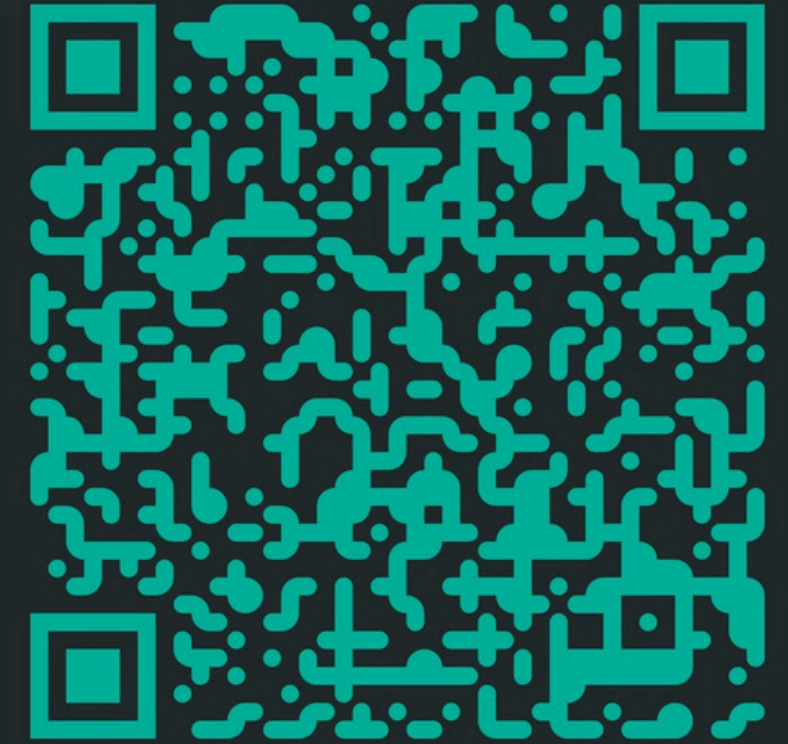


استعمال أداة
لتحليل المخاطر



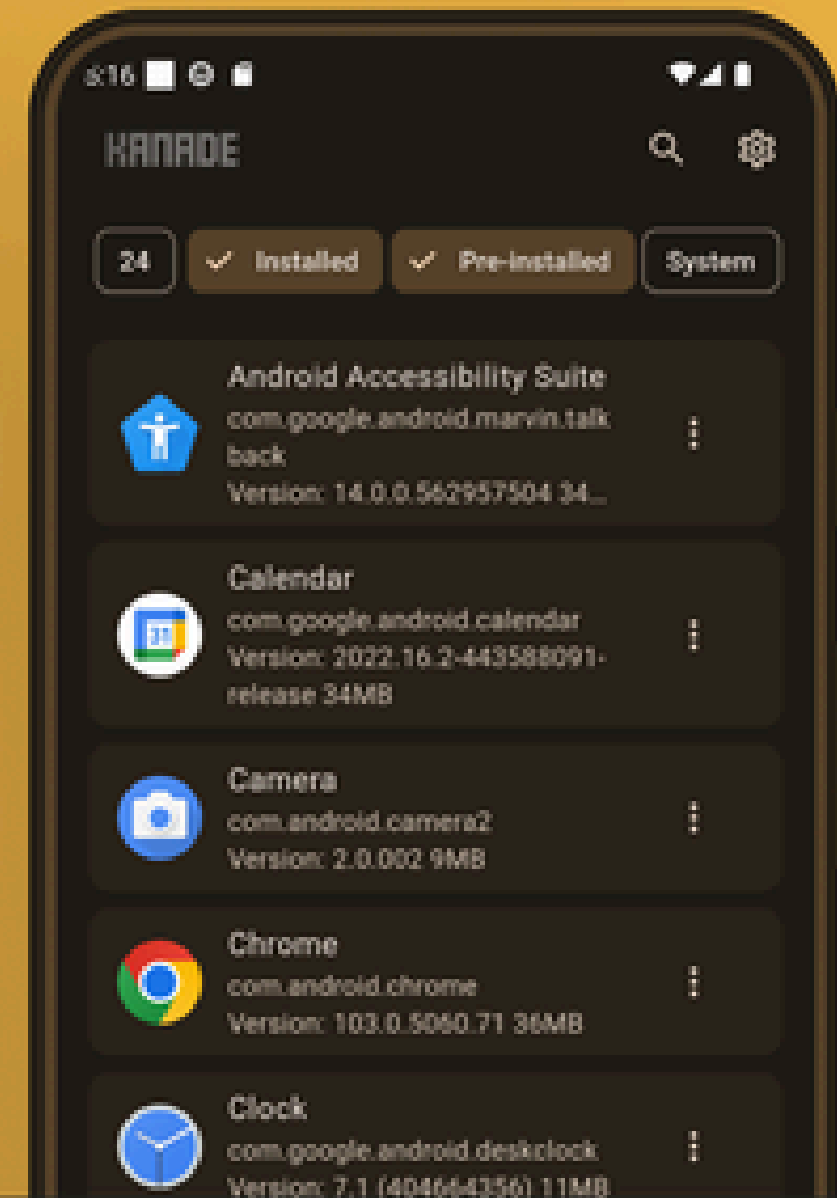
استخراج التطبيق من هاتفك

Download The App
via Play Store

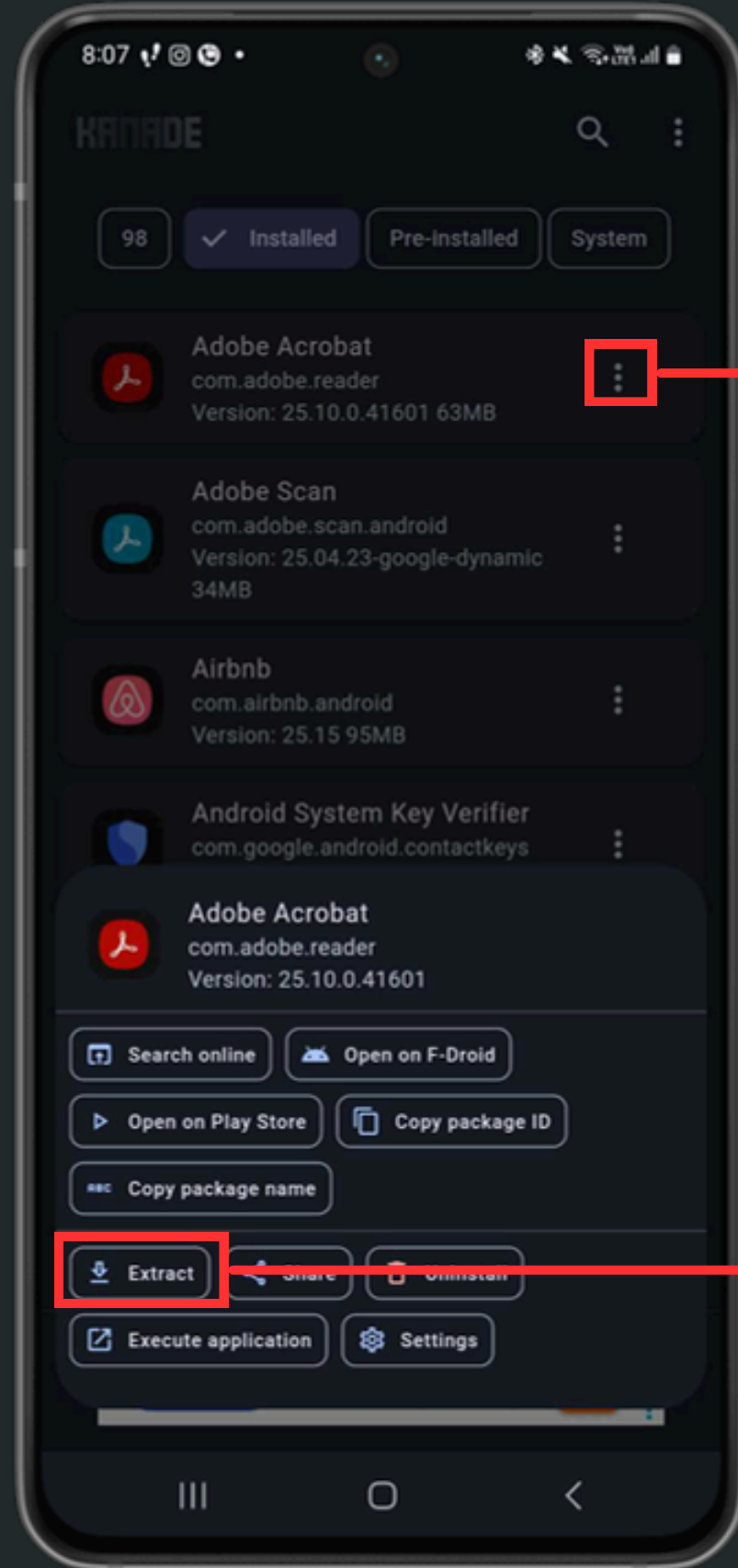


KANADE

Open source apk extractor app.



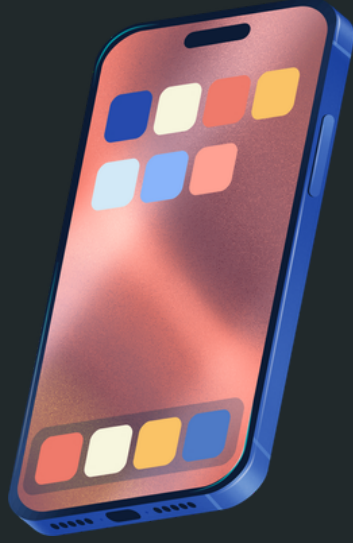
استخراج التطبيق من هاتفك



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؟



اختيار تطبيق
مشبوه



استخراج التطبيق
من الهاتف



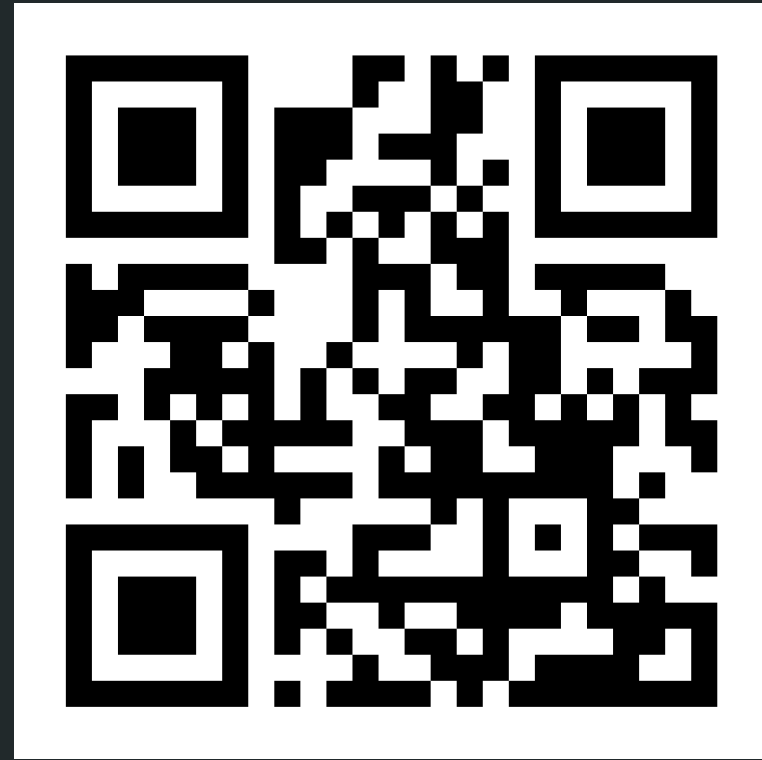
استعمال أداة
لتحليل المخاطر



تحليل التطبيق بأستخدام اداة Pithus



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

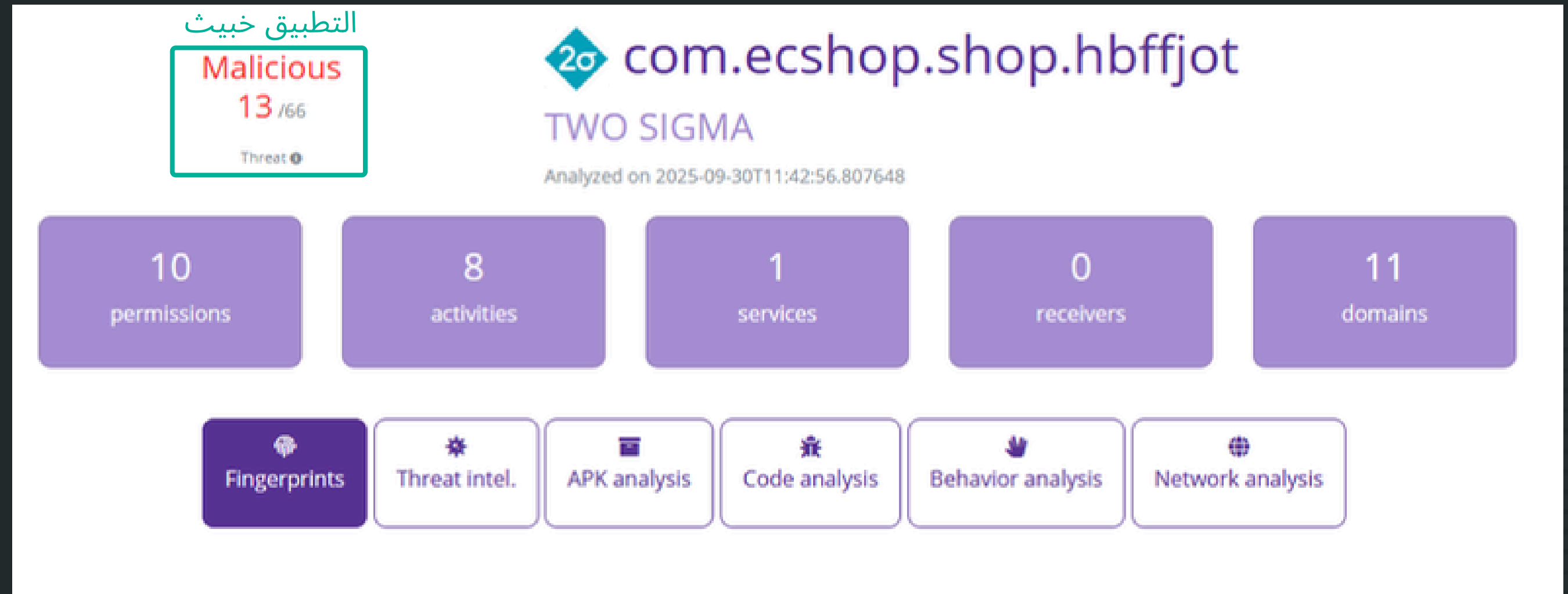


<https://beta.pithus.org>

تحليل Pithus



Sample link



تحليل Pithus

Fingerprints

Threat Intel.

APK Analysis

Code Analysis

Behavior Analysis

Network Analysis



بصمة رقمية للتطبيق

File sums

MDS	f47df545387d24d6308ba399feec4b8e
SHA1	79e6c89a4a12216403d0758e82731900690b4b54
SHA256	5bbc7312cf8096e7c11912f443c74f088d41b237c0d79e3498cdca370750cba1
Size	6.31MB



ما هو ال Hashing؟

خصائص ال Hashing

1 فريد

2 حتمي



5a00be6e1e8304d4
124f815f0346ebd0



Chrome.apk

بصمة رقمية للملفات



نتائج APKiD

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

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

```
/tmp/tmp2onf1_ay/classes.dex
anti_vm
Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.PRODUCT check
possible Build.SERIAL check
SIM operator check
network operator name check
possible VM check

compiler
r8 without marker (suspicious)
```

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



نتائج 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 <code>ssdeep</code> .		
APK file	196608:DPK1hg8GQULR05VfybP+E8bgbwQ/BN/4101:7K1hdR5Vab4bY5/BN/4g	🔍
Manifest	192:90uZPZPAeDz0Ubtyna0hVkrsgy0M0/OT06ezBtCoVkk1vTUzrjSj+zELysP14Vm+...	🔍
classes.dex	196608:Gt9w2tL+auMr1b6f+Um/RPLFbxBnfP5GPvr:kah21b6f+Um/RPLFbxBnfR6b	🔍
classes2.dex	49152:s1LH4ij8QtmVhn+oYwKfFFZ6RuZ+XEQsi8zfX:0EVgoQFZj	🔍
Dexofuzzy		
Information computed with <code>Dexofuzzy</code> .		
APK file	12288:9KwshqzV1v32b59j3U60Nvl84xuF0Gfmakzv:YwHt305MA0Ffm9zv	🔍
classes.dex	6144:9Kws7t57MzV1vBMujwG36/Bb59nj3Ix03JwMTEje0Q0v1rJ0yk4pC44PbA4FJF0M..	🔍
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.

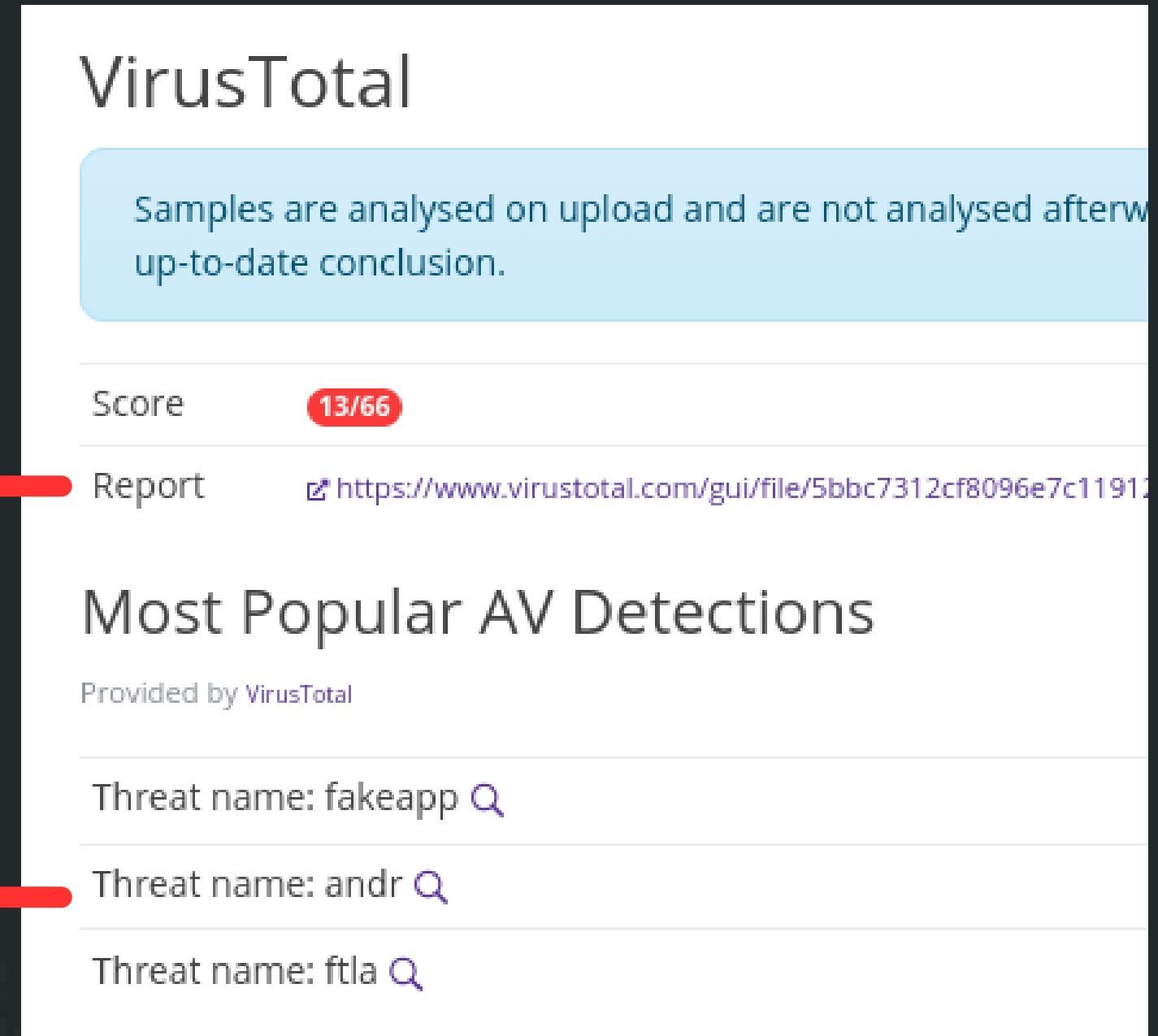
ظهور التطبيق على منصة VirusTotal

ظهور التطبيق على Pithus

نتائج خارجية

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

ظهر نفس التطبيق باسماء مختلفة



VirusTotal

Samples are analysed on upload and are not analysed afterwards. This is an up-to-date conclusion.

Score **13/66**

Report <https://www.virustotal.com/gui/file/5bbc7312cf8096e7c11912>

Most Popular AV Detections

Provided by VirusTotal

Threat name: fakeapp 🔍

Threat name: andr 🔍

Threat name: ftla 🔍



تحليل Pithus

Fingerprints

Threat Intel.

APK Analysis

Code Analysis

Behavior Analysis

Network Analysis



تفاصيل 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 تؤكد 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 Blocks found within V2 signature: 0x7109871a: Unknown 0x42726577: Verity padding 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

Manifest analysis

Information computed with MobSF.

- High** Clear text traffic is Enabled For App[android:usesCleartextTraffic=true]
The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
- Medium** Application Data can be Backed up[android:allowBackup=true]
This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
- High** Launch Mode of Activity (com.ecshop.shop.view.OneActivity) is not standard.
An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

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

الأنشطة

Activities

Information computed with [AndroGuard](#).

```
com.ecshop.shop.view.OneActivity
com.ecshop.shop.view.SplashActivity
com.ecshop.shop.view.LogActivity
me.goldze.mvvmhabit.base.ContainerActivity
me.goldze.mvvmhabit.crash.DefaultErrorActivity
com.just.agentweb.ActionActivity
com.blankj.utilcode.util.UtilsTransActivity4MainProcess
com.blankj.utilcode.util.UtilsTransActivity
```



بعض الأنشطة يمكن ان تكون مثير للشك



تحليل Pithus

Fingerprints

Threat Intel.

APK Analysis

Code Analysis

Behavior Analysis

Network Analysis



تحليل الكود

Code analysis

Information computed with MobSF.

High
CVSS:5.5
App can read/write to External Storage. Any App can read data written to External Storage.
MASVS: MSTG-STORAGE-2
CWE-276 Incorrect Default Permissions
M2: Insecure Data Storage

Low
CVSS:7.5
The App logs information. Sensitive information should never be logged.
MASVS: MSTG-STORAGE-3
CWE-532 Insertion of Sensitive Information into Log File

Medium
CVSS:7.4
Files may contain hardcoded sensitive information like usernames, passwords, keys etc.
MASVS: MSTG-STORAGE-14
CWE-312 Cleartext Storage of Sensitive Information
M9: Reverse Engineering

Medium
CVSS:7.5
The App uses an insecure Random Number Generator.
MASVS: MSTG-CRYPTO-6
CWE-330 Use of Insufficiently Random Values
M5: Insufficient Cryptography

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



تحليل الأذونات

التطبيق ممكن ان يطلب **permissions** خارج عن نطاق استخدامات التطبيق

هذه ال**permissions** ممكن انتسخدم لتجسس على مالك الجهاز

Permissions analysis

Information computed with MobSF.

High android.permission.WRITE_EXTERNAL_STORAGE	read/modify/delete external storage contents Allows an application to write to external storage.	🔍
High android.permission.READ_EXTERNAL_STORAGE	read external storage contents Allows an application to read from external storage.	🔍
High android.permission.READ_PHONE_STATE	read phone state and identity Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, when a call is active, the number that call is connected to and so on.	🔍
High android.permission.CAMERA	take pictures and videos Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.	🔍



تحليل ال threats

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

Behavior analysis

Information computed with MobSF.

- Android notifications
- Base64 decode
- Base64 encode
- Certificate handling
- Content provider
- Crypto

السلوكيات هي الأنشطة التي ينفذها التطبيق بالتفصيل من هذه السلوكيات هي المواصلات بين التطبيق مع الانترنت

Tcp socket

```
okio/SocketAsyncTimeout.java
okio/Okio__JvmOkioKt.java
com/ecshop/shop/IPUtils.java
me/goldze/mvvmhabit/http/NetworkUtil.java
com/blankj/utilcode/util/NetworkUtils.java
com/blankj/utilcode/util/DeviceUtils.java
okio/DeprecatedOkio.java
org/jsoup/internal/ConstrainableInputStream.java
me/goldze/mvvmhabit/http/ExceptionHandler.java
okio/Okio.java
```



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	🔍 📄 🌐	34.128.54.55	📄 🌐
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

URL analysis

Information computed with MobSF.

<https://github.com/ReactiveX/RxJava/wiki/Error-Handling>

Defined in io/reactivex/exceptions/OnErrorNotImplementedException.java

<http://www.zuhryh.xyz/saveLog>

Defined in com/ecshop/shop/view/LogActivity.java

<https://caocaodage.github.io/services/js/jquery-1.6.3.min.js?v=>

Defined in com/ecshop/shop/view/SplashActivity.java

<http://admin.wvbtgervk143.xyz>

Defined in com/ecshop/shop/utils/Constant.java

<http://schemas.android.com/apk/res/android>

Defined in com/afollestad/materialdialogs/prefs/PrefUtil.java

<http://www.baidu.com>

Defined in me/goldze/mvhabit/http/NetworkUtil.java

https://hrieoufsgvoh.s3.ap-southeast-1.amazonaws.com/js/icon_xp5n91.js

https://jryhudtgrtf.s3.ap-southeast-1.amazonaws.com/js/icon_xp5n91.js

Defined in Android String Resource



وهذا كل شيء يا أصدقاء!

هل لديكم اي سؤال؟



شكراً لكم

Follow Us



خبز و نت ٢٥
bread & net '25

جوسا 

