APP SCORES

Security Score **51/100**

Trackers Detection **6/433**

FILE INFORMATION

File Name onlinepizza.apk

Size 63.39MB

MD5 bdcb0abf9a5a08406021e6f21506ff12

SHA1 580b130f8901a05829d7acf06e921638869edf9f

SHA256 2b022cfbf2f1cab5f44c66275ad7518ef91d77661f9717eb9a397f486295377c

APP INFORMATION

App Name foodora

Package Name se.onlinepizza

Main Activity

Target SDK 35 Min SDK 23 Max SDK

Android Version Name 25.7.0 Android Version Code 250700204

PLAYSTORE INFORMATION

Title foodora: Food & Groceries

Score 4.04 Installs 1,000,000+ Price 0 Android Version Support Category Food & Drink Play Store URL se.onlinepizza

Developer foodora AB, Developer ID foodora+AB

Developer Address None

Developer Website http://www.foodora.com

Developer Email support@foodora.com

Release Date Aug 23, 2012 Privacy Policy Privacy link

Description

We know where you can find the flavours that fit you. If there's one thing we know it’s food delivery. It’s our mission to bring tasty food from your favourite local restaurant right to your door so you can eat good food everyday. We'll go the extra mile to make your order the greatest food experience in the world. Hungry for wood-fired pizza, a classic burger or the freshest sushi? We know the best food for every cuisine that your city has to offer. foodora is the best food delivery and take away service in your city -- so let's take the first bite!

Check if we're in your city by downloading the app.

SO WHAT’S THE DEAL?

You’re ready and waiting to eat, we’ve all been there, dreaming of thai food, eating burgers in our dreams. Here’s what we do: first choose between delivery and Pick-Up to fit food ordering seamlessly into your schedule. Pick-Up is simple -- you make your order and then collect your food from the restaurant once it’s ready. No more queuing, ever (our app is magic). If you choose delivery, our couriers will bring the food you've been lusting after right to your door. Dreams really do come true.

HOW IT WORKS

First, enter your address (home/ office/ treehouse). Then, choose your favourite restaurant and place an order. They’ll prepare your food and once it’s ready, our courier bring it to you. If you need something to watch, you can track your rider in real-time. Then you eat. Food goals.

WHAT MAKES US SPECIAL

foodora chooses your local favourites; the best food near you. Vietnamese or Italian, healthy salads or food to nurse your hangover -- your dinner will be cooked with love and care. Our riders come to your very doorstep with a smile while you save time to do something else you love. There's a cuisine and a dish to suit every moment, and we'll help you make the first bite last.

ANYTHING ELSE?

Of course your safety is important to us. We guarantee secure, simple mobile payment, so you can eat when you're hungry and pay however you like.

TALK TO US

If you’ve ordered with us before, we’d want to know what you think. Give us your food thoughts/ teenage confessionals. Let us be your notepad.
Email us at support@foodora.se

For further info, visit
www.foodora.com

10 / 174

EXPORTED ACTIVITIES

View All

2 / 20

EXPORTED SERVICES

View All

3 / 24

EXPORTED RECEIVERS

View All

0 / 11

EXPORTED PROVIDERS

View All

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: O=Techtinium Corporation, CN=Jitendra jain
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-07-23 06:57:03+00:00
Valid To: 2112-06-29 06:57:03+00:00
Issuer: O=Techtinium Corporation, CN=Jitendra jain
Serial Number: 0x500cf5bf
Hash Algorithm: sha1
md5: 9bcef474b6c26cb2ca73aabd3516e085
sha1: ad844e68aa23bb532ec441e84098afed623354f6
sha256: dbe72829d284371075c7c278f5e39ae5555e9638f8c75fae9dc7b93c50557554
sha512: 7d6083f8a5be3d3b9400cf6d13da8c7a367d1c4286886a3726fde0d0b7c19346ce5f443902f7f2b686792eb43f3429961eb441b7865d4f7016635495ffe1be56
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: cd00ef9647b14e56d99abee13d7d26bafa5f4f9adb058eae5dea096219d61f85
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
.permission.MAPS_RECEIVE	unknown	Unknown permission	Unknown permission from android reference	
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.	
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.	
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.	
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.	
android.permission.CAMERA	dangerous	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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.DETECT_SCREEN_CAPTURE	normal	notifies when a screen capture of the app's windows is attempted.	Allows an application to get notified when a screen capture of its windows is attempted.	
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.	

Showing 1 to 10 of 36 entries

Previous 1 2 3 4 Next

ANDROID API

Search:

API	FILES
Android Notifications	
Base64 Decode	
Base64 Encode	
Certificate Handling	
Content Provider	
Crypto	
Dynamic Class and Dexloading	

API	FILES
Execute OS Command	
Get Android Advertising ID	
Get Cell Information	

Showing 1 to 10 of 41 entries

Previous 1 2 3 4 5 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
com.deliveryhero.auth.oauth.OauthActivity	**Schemes**: foodoraeu-openid://, **Hosts:** auth, **Path Patterns:** /callback, /callback/.*,
com.deliveryhero.cobrandedcard.applink.ui.CobrandedCardDeepLinkActivity	**Schemes**: foodoraeu-cobrandedcard://,
com.deliveryhero.inapprating.InAppRatingActivity	**Schemes**: foodoraeu-iar://,
com.deliveryhero.payment.cashier.PaymentActivity	**Schemes**: foodoraeu-cashier://, **Hosts:** *, **Path Patterns:** /cashier-payment,
com.facebook.CustomTabActivity	**Schemes**: fbconnect://, **Hosts:** cct.se.onlinepizza,

ACTIVITY	INTENT
com.klarna.mobile.sdk.activity.KlarnaRedirectReceiverActivity	**Schemes**: foodoraeu-klarna://, **Hosts:** @string/klarna_return_host,
de.foodora.android.ui.launcher.LauncherActivity	**Schemes**: onlinepizza://, foodoraeu://, https://, **Hosts:** foodoraeu.com, www.foodora.se, www.hungry.dk, www.foodora.dk, www.damejidlo.cz, www.foodora.cz, www.foodora.no, www.mjam.at, www.mjam.net, www.foodora.at, www.netpincer.hu, www.foodpanda.de, www.foodora.hu, www.foodpanda.sk, www.foodora.sk, www.foodora.eu, www.foodora.fi, **Paths:** /, /corporate, **Path Prefixes:** /chain, /city, /cuisine, /darkstore, /groceries, /login, /item, /restaurant, /restaurants, /shop, /special-menus, /payments, /pandapay, /cuzdan, /foodorawallet, /yuu, **Path Patterns:** /..*/,

Showing 1 to 7 of 7 entries

Previous 1 Next

NETWORK SECURITY

HIGH	WARNING	INFO	SECURE
0	0	0	0

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
No data available in table			

Showing 0 to 0 of 0 entries

Previous Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
0	2	1

Search:

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 3 of 3 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
1	16	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.	
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.	
3	**Activity-Alias** (de.foodora.android.ui.launcher.LauncherActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
4	**Activity** (com.deliveryhero.auth.oauth.OauthActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
5	**Activity** (com.klarna.mobile.sdk.activity.KlarnaRedirectReceiverActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
6	**Activity** (com.deliveryhero.auth.ui.klarna.KlarnaLoginActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
7	**Activity** (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
8	**Activity** (com.deliveryhero.payment.wallet.wechat.WeChatEntryActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
9	**Activity** (com.deliveryhero.payment.cashier.PaymentActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
10	**Activity** (com.deliveryhero.cobrandedcard.applink.ui.CobrandedCardDeepLinkActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	

Showing 1 to 10 of 18 entries

Previous 1 2 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
1	10	3	2	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
1	The App logs information. Sensitive information should never be logged.	info	**CWE:** CWE-532: Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
2	App can write to App Directory. Sensitive Information should be encrypted.	info	**CWE:** CWE-276: Incorrect Default Permissions **OWASP MASVS:** MSTG-STORAGE-14		
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	**CWE:** CWE-312: Cleartext Storage of Sensitive Information **OWASP Top 10:** M9: Reverse Engineering **OWASP MASVS:** MSTG-STORAGE-14		
4	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	**CWE:** CWE-749: Exposed Dangerous Method or Function **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-PLATFORM-7		
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	**CWE:** CWE-276: Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2		
6	App creates temp file. Sensitive information should never be written into a temp file.	warning	**CWE:** CWE-276: Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2		
7	SHA-1 is a weak hash known to have hash collisions.	warning	**CWE:** CWE-327: Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
8	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	**OWASP MASVS:** MSTG-STORAGE-10		
9	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	**CWE:** CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-3	com/incognia/core/Wo.java defpackage/C23635kt.java defpackage/C37140yO2.java	
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	**OWASP MASVS:** MSTG-NETWORK-4		

Showing 1 to 10 of 16 entries

Previous 1 2 Next

SHARED LIBRARY BINARY ANALYSIS

No Shared Objects found.

Search:

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
No data available in table									

Showing 0 to 0 of 0 entries

Previous Next

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

FIREBASE DATABASE ANALYSIS

Search:

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://online-pizza-apps.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/15017165007/namespaces/firebase:fetch?key=AIzaSyB157ejjdsLuUcSssVVzbJzpQbs054uVxQ. This is indicated by the response: The response code is 403

Showing 1 to 2 of 2 entries

Previous 1 Next

MALWARE LOOKUP

VirusTotal Report | Triage Report | MetaDefender Report | Hybrid Analysis Report

APKiD ANALYSIS

Search:

DEX	DETECTIONS
bdcb0abf9a5a08406021e6f21506ff12.apk	Search: **FINDINGS** / **DETAILS** Anti-VM Code — possible VM check Showing 1 to 1 of 1 entries Previous 1 Next
classes.dex	Search: **FINDINGS** / **DETAILS** Anti-VM Code — Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check Compiler — r8 Showing 1 to 2 of 2 entries Previous 1 Next

DEX	DETECTIONS
classes2.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check network operator name check
Compiler	r8 without marker (suspicious)

Showing 1 to 2 of 2 entries

Previous 1 Next

classes3.dex

Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check SIM operator check
Compiler	r8 without marker (suspicious)

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes4.dex	

Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check possible VM check
Compiler	r8 without marker (suspicious)

Showing 1 to 3 of 3 entries

Previous 1 Next

DEX	DETECTIONS
classes5.dex	Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check
Compiler	r8 without marker (suspicious)

Showing 1 to 3 of 3 entries

Previous 1 Next

DEX	DETECTIONS
classes6.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.MANUFACTURER check
Compiler	r8 without marker (suspicious)

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes7.dex	Search:

FINDINGS	DETAILS
Compiler	r8 without marker (suspicious)

Showing 1 to 1 of 1 entries

Previous 1 Next

Showing 1 to 8 of 8 entries

Previous 1 Next

BEHAVIOUR ANALYSIS

Search:

RULE ID	BEHAVIOUR	LABEL	FILES
00003	Put the compressed bitmap data into JSON object	camera	defpackage/C9967Uld.java defpackage/I15.java
00004	Get filename and put it to JSON object	file collection	
00005	Get absolute path of file and put it to JSON object	file	com/braze/Braze.java com/shakebugs/shake/internal/I6.java defpackage/C26855o57.java
00009	Put data in cursor to JSON object	file	

RULE ID	BEHAVIOUR	LABEL	FILES
00010	Read sensitive data(SMS, CALLLOG) and put it into JSON object	sms calllog collection	com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/shakebugs/shake/internal/l7.java com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java defpackage/C6582Mj7.java
00012	Read data and put it into a buffer stream	file	
00013	Read file and put it into a stream	file	
00014	Read file into a stream and put it into a JSON object	file	
00015	Put buffer stream (data) to JSON object	file	defpackage/C17107eWc.java

Showing 1 to 10 of 55 entries

Previous 1 2 3 4 5 6 Next

ABUSED PERMISSIONS

Top Malware Permissions **12**/25

android.permission.INTERNET,
android.permission.ACCESS_NETWORK_STATE,
android.permission.ACCESS_WIFI_STATE,
android.permission.VIBRATE,
android.permission.ACCESS_COARSE_LOCATION,
android.permission.ACCESS_FINE_LOCATION,
android.permission.READ_CONTACTS,
android.permission.CAMERA,
android.permission.WRITE_EXTERNAL_STORAGE,
android.permission.READ_EXTERNAL_STORAGE,

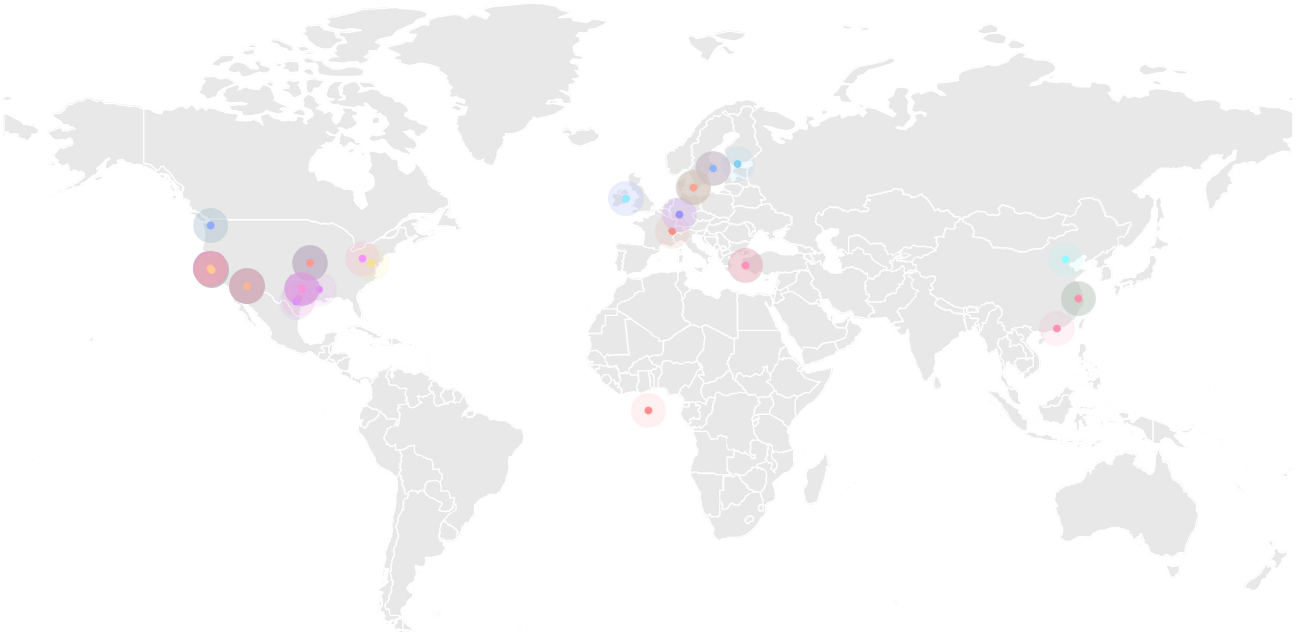
Other Common Permissions **5**/44

android.permission.READ_CALENDAR,
android.permission.FOREGROUND_SERVICE,
com.google.android.c2dm.permission.RECEIVE,
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE,
com.google.android.gms.permission.AD_ID

android.permission.WAKE_LOCK,
android.permission.RECEIVE_BOOT_COMPLETED

Malware Permissions are the top permissions that are widely abused by known malware.
Other Common Permissions are permissions that are commonly abused by known malware.

SERVER LOCATIONS



This app may communicate with the following OFAC sanctioned list of countries.

Search:

DOMAIN	COUNTRY/REGION
app.adjust.cn	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou
gdpr.adjust.cn	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou
long.open.weixin.qq.com	**IP:** 109.244.216.15 **Country:** China **Region:** Beijing **City:** Beijing
open.weixin.qq.com	**IP:** 203.205.232.110 **Country:** China **Region:** Guangdong **City:** Shenzhen
ssrv.adjust.cn	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou
subscription.adjust.cn	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou

Showing 1 to 6 of 6 entries

Previous 1 Next

DOMAIN MALWARE CHECK

Search:

DOMAIN	STATUS	GEOLOCATION
.facebook.com	ok	No Geolocation information available.
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
accounts.google.com	ok	**IP:** 64.233.161.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
aggregator.eu.usercentrics.eu	ok	**IP:** 195.181.166.158 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aggregator.service.usercentrics.eu	ok	**IP:** 34.120.28.121 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
aomedia.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
api.avo.app	ok	**IP:** 34.102.252.42 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
api.eu.usercentrics.eu	ok	**IP:** 195.181.166.158 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map
api.production.s.fintech.deliveryhero.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api.shakebugs.com	ok	**IP:** 18.158.2.172 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

Showing 1 to 10 of 143 entries

Previous 1 2 3 4 5 … 15 Next

URLS

Search:

URL	FILE
data:(	defpackage/T33.java
data:image	defpackage/U33.java
http://goo.gl/8rd3yj	defpackage/QDe.java
http://goo.gl/8rd3yj	defpackage/RunnableC38004zFe.java
http://goo.gl/nafqqk	defpackage/FDe.java
http://hostname/?	defpackage/C24133lNe.java
http://localhost	defpackage/LFc.java

URL	FILE
http://localhost/	defpackage/C34340vb7.java
http://localhost/	defpackage/EV9.java
http://localhost/	com/deliveryhero/chatsdk/provider/RetrofitBuilderKt$DefaultRetrofitBuilder$2.java

Showing 1 to 10 of 154 entries

Previous 1 2 3 4 5 … 16 Next

EMAILS

Search:

EMAIL	FILE
android@foodora.com	defpackage/C24482ljb.java
android@foodora.com	defpackage/DialogInterfaceOnClickListenerC9142Sm4.java
support@avo.app	defpackage/XVc.java
support@foodpanda.sg support@foodora.it corporate@foodpanda.sg name@email.com support@foodora.no corporate@foodpanda.com name@company.com	Android String Resource
u0013android@android.com u0013android@android.com0	defpackage/BinderC14707cOe.java

Showing 1 to 5 of 5 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

Showing 1 to 6 of 6 entries

Previous 1 Next

POSSIBLE HARDCODED SECRETS

▶ Show all **127** secrets

STRINGS

From APK Resource

▶ Show all **11523** strings

From Code

▶ Show all **96996** strings

From Shared Objects

ACTIVITIES

▶ Show all **174** activities

SERVICES

▼ Showing all **20** services

com.deliveryhero.push.service.sp.PushMessagingService
com.shakebugs.shake.internal.shake.recording.ScreenRecordingService
com.google.android.gms.auth.api.signin.RevocationBoundService
com.google.android.gms.tagmanager.TagManagerService
com.google.firebase.components.ComponentDiscoveryService
com.google.firebase.messaging.FirebaseMessagingService
com.google.android.gms.measurement.AppMeasurementService
com.google.android.gms.measurement.AppMeasurementJobService
com.google.firebase.sessions.SessionLifecycleService
androidx.work.impl.background.systemalarm.SystemAlarmService
androidx.work.impl.background.systemjob.SystemJobService
androidx.work.impl.foreground.SystemForegroundService
androidx.room.MultiInstanceInvalidationService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService
com.incognia.core.JobTriggeredService
com.incognia.core.CommonReceiverJobService

com.incognia.core.LocationService
com.incognia.core.LocationJobService
com.incognia.core.LocationReceiverJobService

RECEIVERS

▼ Showing all **24** receivers

com.deliveryhero.referral.share.receiver.ReferralShareReceiver
com.deliveryhero.marketing.braze.BrazeBroadcastReceiver
com.google.firebase.iid.FirebaseInstanceIdReceiver
com.deliveryhero.push.service.sp.PushBroadcastReceiver
com.braze.push.BrazePushReceiver
com.shakebugs.shake.internal.NotificationReceiver
com.google.android.gms.measurement.AppMeasurementReceiver
androidx.work.impl.utils.ForceStopRunnable$BroadcastReceiver
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryChargingProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryNotLowProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$StorageNotLowProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$NetworkStateProxy
androidx.work.impl.background.systemalarm.RescheduleReceiver
androidx.work.impl.background.systemalarm.ConstraintProxyUpdateReceiver
androidx.work.impl.diagnostics.DiagnosticsReceiver
com.braze.BrazeFlushPushDeliveryReceiver
com.facebook.CurrentAccessTokenExpirationBroadcastReceiver
com.facebook.AuthenticationTokenManager$CurrentAuthenticationTokenChangedBroadcastReceiver
androidx.profileinstaller.ProfileInstallReceiver
com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver
com.instacart.library.truetime.BootCompletedBroadcastReceiver
com.incognia.core.AlarmHelperReceiver
com.incognia.core.IncogniaCommonReceiver
com.incognia.core.LocationReceiver

PROVIDERS

▼ Showing all **11** providers
com.deliveryhero.helpcenter.HcChatCacheFileProvider
com.deliveryhero.orderhistory.ReceiptDownloadFileProvider
androidx.startup.InitializationProvider
com.deliveryhero.customerchat.provider.CustomerChatFileProvider
com.shakebugs.shake.internal.utils.FileProvider
com.google.firebase.provider.FirebaseInitProvider
com.klarna.mobile.KlarnaInitProvider
com.klarna.mobile.KlarnaShareFileProvider
io.sentry.android.core.SentryInitProvider
io.sentry.android.core.SentryPerformanceProvider
com.squareup.picasso.PicassoProvider

LIBRARIES

▼ Showing all **5** libraries
com.sec.android.app.multiwindow
org.apache.http.legacy
android.ext.adservices
androidx.window.extensions
androidx.window.sidecar

SBOM

▶ Show all **125** Versioned Packages
▶ Show all **582** Packages

FILES

▶ Show all **3567** files

 Version v4.3.1