APP SCORES

Security Score **51/100**

Trackers Detection

7/432

FILE INFORMATION

File Name se.onlinepizza.apk

Size 62.41MB

MD5 47e629879c80bd2e051a7603443f641a

SHA1 3b92e8b88e6fa7d1822b84a69438458d8e0defcc

SHA256

3d556406f3ad46e4e07e01a703e634281d0526e6a6c38e1e5a2cbab8c9bd6b73

APP INFORMATION

App Name foodora

Package Name se.onlinepizza

Main Activity

Target SDK 35 **Min SDK** 23 **Max SDK**

Android Version Name 25.2.0 **Android Version Code**

250200094

PLAYSTORE INFORMATION

Title foodora: Food & Groceries

Score 3.94 **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
```

10 / 177
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
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPP
.permission.MAPS_RECEIVE	unknown	Unknown permission	Unknown permission from android reference	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPF
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.	
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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPF
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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPF
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	

ANDROID API

Search:

API	FILES
Base64 Decode	
Base64 Encode	
Content Provider	
Crypto	
Dynamic Class and Dexloading	
Get Android Advertising ID	
Get System Service	

API	FILES
GPS Location	1
HTTP Connection	
HTTPS Connection	

Showing 1 to 10 of 24 entries

1

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,

ACTIVITY	INTENT
com.facebook.CustomTabActivity	**Schemes**: fbconnect://, **Hosts:** cct.se.onlinepizza,
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:** /..*/,

NETWORK SECURITY

1

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	15	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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	
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.	

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
0	6	1	1	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		
2	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		
3	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	com/shakebugs/shake/internal/utils/FileProvider.java defpackage/C24061m74.java	

1

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
4	The App uses an insecure Random Number Generator.	warning	**CWE:** CWE-330: Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6		
5	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	defpackage/C19900i42.java	
6	This App may have root detection capabilities.	secure	**OWASP MASVS:** MSTG-RESILIENCE-1	defpackage/C19900i42.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
7	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	com/deliveryhero/payment/paymentselector/creditcard/webview/AddCreditCardActivity.java	

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

1

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

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

MALWARE LOOKUP

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

1

APKiD ANALYSIS

Search:

DEX	DETECTIONS

DEX	DETECTIONS
47e629879c80bd2e051a7603443f641a.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 Debug Code	Debug.isDebuggerConnected() check
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 3 of 3 entries

Previous 1 Next

DEX	DETECTIONS
classes3.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.BRAND check Build.DEVICE 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

BEHAVIOUR ANALYSIS

Search:

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	com/shakebugs/shake/internal/ya.java
00013	Read file and put it into a stream	file	com/shakebugs/shake/internal/ya.java
00022	Open a file from given absolute path of the file	file	io/sentry/android/core/C20632v.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	defpackage/C21041j10.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/shakebugs/shake/internal/oa.java defpackage/C21041j10.java defpackage/C31981uH.java
00075	Get location of the device	collection location	bo/content/o.java defpackage/ZN.java
00079	Hide the current app's icon	evasion	defpackage/C34156wW7.java defpackage/ZN.java
00108	Read the input stream from given URL	network command	defpackage/C28701qte.java
00112	Get the date of the calendar event	collection calendar	com/shakebugs/shake/internal/l1.java

1

RULE ID	BEHAVIOUR	LABEL	FILES
00115	Get last known location of the device	collection location	defpackage/ZN.java

Showing 1 to 10 of 13 entries

Previous 1 2 Next

ABUSED PERMISSIONS

Top Malware Permissions **12**/25

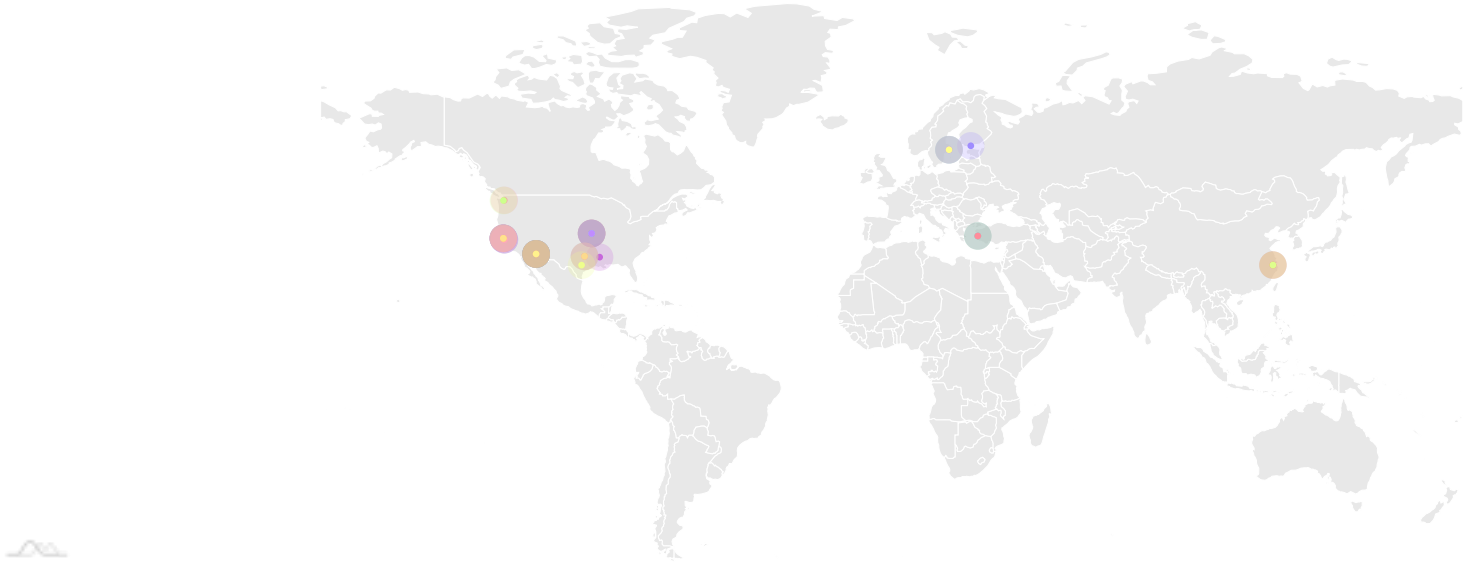
android.permission.INTERNET,
android.permission.ACCESS_NETWORK_STATE,
android.permission.ACCESS_WIFI_STATE,
android.permission.VIBRATE,
android.permission.ACCESS_COARSE_LOCATION,
android.permission.ACCESS_FINE_LOCATION,
android.permission.READ_CONTACTS,
android.permission.CAMERA,
android.permission.WRITE_EXTERNAL_STORAGE,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

Other Common Permissions

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

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

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
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

DOMAIN MALWARE CHECK

Search:

1

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
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
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
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

DOMAIN	STATUS	GEOLOCATION
api.usercentrics.eu	ok	**IP:** 35.241.3.184 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
app.adjust.cn	ok	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
app.adjust.com	ok	**IP:** 185.151.204.6 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.adjust.net.in	ok	**IP:** 185.151.204.31 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
app.adjust.world	ok	**IP:** 185.151.204.42 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
app.eu.adjust.com	ok	**IP:** 185.151.204.60

URLS

Search:

URL	FILE
http://hostname/?	defpackage/Qoe.java
http://www.google-analytics.com https://ssl.google-analytics.com	defpackage/C37307zke.java

URL	FILE
http://www.w3.org/1999/xhtml	defpackage/AbstractC29572rna.java
http://www.w3.org/xml/1998/namespace	defpackage/C22214kD3.java
https://consent-api.service.consent.usercentrics.eu https://config.eu.usercentrics.eu https://consent-api.service.consent.eu1.usercentrics.eu https://app.eu.usercentrics.eu/session/1px.png https://aggregator.eu.usercentrics.eu https://graphql.usercentrics.eu/graphql#saveconsents https://api.usercentrics.eu https://api.eu.usercentrics.eu/graphql#saveconsents https://aggregator.service.usercentrics.eu https://uct.eu.usercentrics.eu https://uct.service.usercentrics.eu https://app.usercentrics.eu/session/1px.png	defpackage/C3798Fz6.java 1
https://disco.deliveryhero.io/review-surveys/client/ https://localhost/api/v5/survey-api/v1/	defpackage/EnumC32038uKb.java
https://docs.google.com/viewer?url=	com/klarna/mobile/sdk/core/util/StringUtils.java
https://github.com/reactivex/rxjava/wiki/error-handling	io/reactivex/exceptions /OnErrorNotImplementedException.java
https://github.com/reactivex/rxjava/wiki/what's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java

URL	FILE
https://images.deliveryhero.io/image/foodpanda/gift-card/empty-payment-method.png)	defpackage/QM4.java

EMAILS

Search:

EMAIL	FILE
support@avo.app	defpackage/C30067sIc.java
support@foodora.no support@foodora.it name@email.com corporate@foodpanda.com name@company.com corporate@foodpanda.sg support@foodpanda.sg	Android String Resource

Showing 1 to 2 of 2 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Braze (formerly Appboy)	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/17
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 7 of 7 entries

Previous 1 Next

POSSIBLE HARDCODED SECRETS

▼ Showing all **34** secrets

"NEXTGEN_ACNT_PASSWORD" : "Password"
"NEXTGEN_DINEIN_PAYMENT_CANCEL_AUTH_DIALOG_CTA" : "Cancel"
"NEXTGEN_LOGIN_SHOW_PASSWORD" : "Show"
"NEXTGEN_REGISTER_STARTED_SHOW_PASSWORD" : "Show"
"NEXTGEN_SUBS_RP_SCPWD_INFO_FOOTER_BACK_CTA" : "Back"
"com.google.firebase.crashlytics.mapping_file_id" : "e639a222dc9b42b0866731e0dc07b60b"

"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"file_provider_authority" : "se.onlinepizza.fileprovider"
"firebase_database_url" : "https://online-pizza-apps.firebaseio.com"
"google_api_key" : "AIzaSyB157ejjdsLuUcSssVVzbJzpQbs054uVxQ"
"google_crash_reporting_api_key" : "AIzaSyB157ejjdsLuUcSssVVzbJzpQbs054uVxQ"
"library_fastadapter_authorWebsite" : "http://mikepenz.com/"
"library_materialize_authorWebsite" : "http://mikepenz.com/"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"shared_prefs_app_id_key_klarna_inapp_sdk" : "sdk-application-id"
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e
7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808
58037121987999716643812574028291115057151
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef
451fd46b503f00
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
11579208921035624876269744694940757353008614341529031419553363130886709785395 1
0123456789abcdefABCDEF
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633
21113864768612440380340372808892707005449
11579208921035624876269744694940757352999695522413576034242225906106851204436 9
308202eb30820254a00302010202044d36f7a4300d06092a864886f70d01010505003081b9310b3009060355040613023836311230100603550 4
0813094775616e67646f6e673111300f060355040713085368656e7a68656e31353033060355040a132c54656e63656e7420546563686e6f6c6f67
79285368656e7a68656e2920436f6d70616e79204c696d69746564313a3038060355040b133154656e63656e74204775616e677a686f752052657

3656172636820616e6420446576656c6f706d656e742043656e746572311030 0e06035504031307546 56e63656e74301e170d313130313139313
4333933325a170d343130313131313134333933325a3081b9310b300906035504061302383631123010060355040813094775616e67646f6e67311
1300f06035504071308536 8656e7a68656e31353033060355040a132c54656e63656e7420546563686e6f6c6f6779285368656e7a68656e292043
6f6d70616e79204c696d69746564313a3038060355040b133154656e63656e74204775616e677a686f752052657365617263682061 6e642044657
6656c6f706d656e742043656e746572311030 0e06035504031307546 56e63656e7430819f300d06092a864886f70d010101050003818d00308189
02818100c05f34b231b083fb1323670bfbe7bdab40c0c0a6efc87ef2072a1ff0d60cc67c8edb0d0847f210bea6cbfaa241be70c86daf56be08b723c
859e52428a064555d80db448cdcacc1aea2501eba06f8bad12a4fa49d85cacd7abeb68945a5cb5e061629b52e3254c373550ee4e40cb7c8ae6f7a
8151ccd8df582d446f39ae0c5e930203010001300d06092a864886f70d01010505000381810 09c8d9d7f2f908c42081b4c764c377109a8b2c70582
422125ce545842d5f520aea69550b6bd8bfd94e987b75a3077eb04ad341f481aac266e89d3864456e69fba13df018acdc168b9a19dfd7ad9d9cc6
f6ace57c746515f71234df3a053e33ba93ece5cd0fc15f3e389a3f365588a9fcb439e069d3629cd7732a13fff7b891499
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088
be94769fd16650
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43

A STRINGS

From APK Resource

▶ Show all **11371** strings

From Code

▶ Show all **14601** strings

From Shared Objects

ACTIVITIES

▶ Show all **177** 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.shakebugs.shake.internal.NotificationReceiver
com.braze.push.BrazePushReceiver
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$NetworkStateProxy
androidx.work.impl.background.systemalarm.RescheduleReceiver
androidx.work.impl.background.systemalarm.ConstraintProxyUpdateReceiver
androidx.work.impl.diagnostics.DiagnosticsReceiver
com.facebook.CurrentAccessTokenExpirationBroadcastReceiver
com.facebook.AuthenticationTokenManager$CurrentAuthenticationTokenChangedBroadcastReceiver
com.braze.receivers.BrazeActionReceiver
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.klarna.mobile.KlarnaInitProvider
com.klarna.mobile.KlarnaShareFileProvider
com.google.firebase.provider.FirebaseInitProvider
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 **123** Versioned Packages
▶ Show all **306** Packages

FILES

▶ Show all **3566** files

 Version v4.2.9