MOBSF

ANDROID STATIC ANALYSIS REPORT

Bolt (CA.188.0)

File Name:	base.apk
Package Name:	ee.mtakso.client
Scan Date:	Nov. 27, 2025, 3:57 a.m.
App Security Score:	50/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	11/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	33	4	3	2

FILE INFORMATION

File Name: base.apk
Size: 111.66MB
MD5: d5de3f36cf2b82691ab53051913f6a66
SHA1: 6826cc7dbd4e1c87ab01fcb542fb48d383e78b2b
SHA256: 76a775e35b3a112100586d05d2c23c570e1e3c2b91328af1c6b0cc87bec6e05a

APP INFORMATION

App Name: Bolt
Package Name: ee.mtakso.client
Main Activity:
Target SDK: 35
Min SDK: 21
Max SDK:
Android Version Name: CA.188.0

Android Version Code: 3620

APP COMPONENTS

Activities: 20
Services: 25
Receivers: 26
Providers: 8
Exported Activities: 6
Exported Services: 4
Exported Receivers: 7
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: O=Mtakso OÜ
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-06-25 11:30:50+00:00
Valid To: 2038-06-19 11:30:50+00:00
Issuer: O=Mtakso OÜ
Serial Number: 0x51c97f6a
Hash Algorithm: sha1
md5: babd7a6bb58e4c0634c2367513f6e029
sha1: cf5a183937792e02b58734a135733131c8561cab
sha256: a75c6372a0b67db01686b47df68c91516ee16229eec4c0c67d355e32207c6617
sha512: 745657b5a55a38c925edd0bb5a8822ed2b78ba1b09e10afaca28d2cd25b744c730a174933c2113e17ab02736b492ffe0f0fe3e13c92346fb0c883a1ea04be826
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 69683294c2e1a530f42c12d9a23327cc374e2e0c25ef9d9d9e98a544868451e5
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.
android.permission.GET_PACKAGE_SIZE	normal	measure application storage space	Allows an application to find out the space used by any package.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_ADVERTISE	dangerous	required to advertise to nearby Bluetooth devices.	Required to be able to advertise to nearby Bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
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.
com.samsung.android.mapsagent.permission.READ_APP_INFO	unknown	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.providers.gsf.permission.READ_GSERVICES	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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
ee.mtakso.client.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE_PHONE_CALL	normal	enables foreground services during phone calls.	Allows a regular application to use Service.startForeground with the type "phoneCall".
android.permission.MANAGE_OWN_CALLS	normal	enables a calling app to manage its own calls.	Allows a calling application which manages it own calls through the self-managed ConnectionService APIs.

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.HARDWARE check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes10.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes11.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check
possible Build.SERIAL check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes12.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes13.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check
ro.hardware check
ro.kernel.qemu check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes8.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
network operator name check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes9.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
ee.mtakso.client.newbase.deeplink.DeeplinkActivity	Schemes: taxify://, bolt://, https://, boltprelive://, geo://, http://, Hosts: action, scooters.taxify.eu, maps.google.com, Path Prefixes: /qr,
ee.mtakso.client.newbase.deeplink.appsflyer.AppsFlyerDeeplinkActivity	Schemes: https://, Hosts: bolt.onelink.me,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.ee.mtakso.client,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
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.

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 20 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	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	Application Data can be Backed up [android:allowBackup=true]	warning	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.
3	Activity (ee.mtakso.client.newbase.RideHailingMapActivity) 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.
4	Activity-Alias (ee.mtakso.client.activity.SplashHomeActivity) 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.
5	Activity (ee.mtakso.client.newbase.voip.VoipTrampolineActivity) 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
6	App Link assetlinks.json file not found [android:name=ee.mtakso.client.newbase.deeplink.DeeplinkActivity] [android:host=https://scooters.taxify.eu]	high	App Link asset verification URL (https://scooters.taxify.eu/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
7	Activity (ee.mtakso.client.newbase.deeplink.DeeplinkActivity) 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 (ee.mtakso.client.newbase.deeplink.appsflyer.AppsFlyerDeeplinkActivity) 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	Content Provider (com.facebook.FacebookContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider 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
10	Broadcast Receiver (com.appsflyer.MultipleInstallBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
11	Broadcast Receiver (ee.mtakso.client.notifications.SignupNotificationUpdateReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Broadcast Receiver (eu.bolt.client.otp.receiver.OtpCodeReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Service (eu.bolt.service.CrossAppLoginService) is not Protected. [android:exported=true]	warning	A Service 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
14	Broadcast Receiver (com.clevertap.android.sdk.pushnotification.fcm.CTFirebaseMessagingReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
15	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
16	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
17	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.
18	TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
19	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
20	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
21	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
22	Service (com.sinch.android.rtc.internal.client.fcm.InstanceIDTokenService) is not Protected. [android:exported=true]	warning	A Service 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: 1 | WARNING: 10 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/braze/Constants.java com/braze/configuration/BrazeConfig.java com/braze/enums/CardKey.java com/braze/images/DefaultBrazeImageLoader.java com/braze/models/inappmessage/InAppMessageHtml.java com/braze/models/outgoing/AttributionData.java com/braze/push/BrazeNotificationUtils.java com/braze/push/BrazePushReceiver.java com/braze/support/StringUtils.java com/braze/ui/contentcards/ContentCardsFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				nt.java com/braze/ui/inappmessage/listeners/DefaultInAppMessageWebViewClientListener.java com/bumptech/glide/load/engine/c.java com/bumptech/glide/load/engine/n.java com/bumptech/glide/load/engine/u.java ee/mtakso/client/core/data/storage/migration/UserMigrator.java ee/mtakso/client/ribs/root/RootRouter.java ee/mtakso/client/ribs/root/ridehailing/activerideflow/ActiveRideFlowRibInteractor.java ee/mtakso/client/ribs/root/ridehailing/preorderflow/PreOrderFlowRibInteractor.java ee/mtakso/internal/di/modules/g3.java eu/bolt/android/audio_recording_engine/db/OrderRecordingsData.java eu/bolt/android/audio_recording_engine/db/RecordingFileInfo.java eu/bolt/android/deeplink/core/key/DeeplinkConst.java eu/bolt/android/rib/BaseRibInteractor.java eu/bolt/android/rib/Router.java eu/bolt/android/rib/multistack/StackUpdateEvent.java eu/bolt/android/webview/WebPageRibInteractor.java eu/bolt/campaigns/core/domain/model/CampaignDetailsInfo.java eu/bolt/chat/data/c.java eu/bolt/chat/data/connection/ChatConnectionSettings.java eu/bolt/client/appstate/data/network/model/InitialChallengeConfigResponse.java eu/bolt/client/appstate/domain/model/AppStateOnStartupBundle.java eu/bolt/client/appstate/domain/model/InitialChallengeConfig.java eu/bolt/client/bugreport/data/network/model/FlagsReportModel.java eu/bolt/client/captcha/recaptcha/ReCaptchaRibArgs.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eu/bolt/client/carsharing/data/model/offer/MapOptionsNetworkModel.java eu/bolt/client/carsharing/data/model/order/CreateOrderConfirmationNetworkModel.java eu/bolt/client/carsharing/domain/model/CarsharingBluetoothCommandsInfo.java eu/bolt/client/carsharing/domain/model/CarsharingMapVehicle.java eu/bolt/client/carsharing/domain/model/CarsharingVehicleMapFilterConfig.java eu/bolt/client/carsharing/domain/model/map/RouteOrderMapVehicle.java eu/bolt/client/carsharing/domain/model/order/CreateOrderConfirmation.java eu/bolt/client/carsharing/network/model/offlinemode/a.java eu/bolt/client/carsharing/network/model/response/CarsharingVehiclesByCategoryResponse.java eu/bolt/client/chat/ribs/chat/ChatRibInteractor.java eu/bolt/client/core/data/network/model/rentals/CityAreaFilterNetworkModel.java eu/bolt/client/core/profile/data/credential/model/a.java eu/bolt/client/core/profile/data/network/model/CompletePasskeyCreationRequest.java eu/bolt/client/core/profile/data/network/model/ProfileCreatePasskeyResponse.java eu/bolt/client/core/profile/domain/model/ProfileCreatePasskeyConfig.java eu/bolt/client/core/profilecontent/data/network/model/ProfileContentResponse.java eu/bolt/client/core/profilecontent/domain/model/ProfileContent.java eu/bolt/client/creditcard/ribs/addcreditcardflow/AddCreditCardFlowRibInteractor.java eu/bolt/client/design/model/BitmapWithKey.java eu/bolt/client/driverdetails/DriverDetailsRouter.java eu/bolt/client/familyprofile/rib/FamilyProfileFlowRibInteractor.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eu/bolt/client/familyprofile/rib/choosevalue/ChooseValueRibInteractor.java eu/bolt/client/familyprofile/rib/customspendlimit/CustomSpendLimitRibInteractor.java eu/bolt/client/home/rib/home/HomeRibRouter.java eu/bolt/client/home/rib/homescreencontent/HomeScreenContentRibRouter.java eu/bolt/client/home/rib/savedplace/SavedPlacesRibRibRouter.java eu/bolt/client/login/domain/interactor/SaveCrossAppCredentialsUseCase.java eu/bolt/client/micromobility/blocksview/domain/interactor/SelectHorizontalSelectorValueUseCase.java eu/bolt/client/micromobility/blocksview/domain/model/BlockRowFilter.java eu/bolt/client/micromobility/blocksview/domain/model/blockrow/HorizontalSelectorRow.java eu/bolt/client/micromobility/blocksview/networkshared/data/network/model/BlockRowFilterNetworkModel.java eu/bolt/client/micromobility/blocksview/networkshared/data/network/model/BlockRowNetworkModel.java eu/bolt/client/micromobility/blocksview/ui/model/KeyValueUiModel.java eu/bolt/client/micromobility/confirmationdialog/domain/model/ConfirmationDialog.java eu/bolt/client/micromobility/confirmationflow/domain/model/ConfirmationFlowLayout.java eu/bolt/client/micromobility/confirmationflow/domain/model/RideFinishCheckPhotoScreen.java eu/bolt/client/micromobility/confirmationflow/domain/model/RideFinishedValidationStatus.java eu/bolt/client/micromobility/confirmationflow/ribs/photocapture/RideFinishedPhotoCaptureRibListener.java eu/bolt/client/micromobility/map/filters/domain/usecase/SelectFilterValueUseCase.java eu/bolt/client/micromobility/map/shared/domain

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	/model/MapVehicle.java eu/bolt/client/orderpreferences/core/data/model/OrderPreferencesSelectionOptionNetworkModel.java eu/bolt/client/orderpreferences/core/domain/model/OrderPreferenceData.java eu/bolt/client/orderpreferences/core/domain/model/OrderPreferencesSelectionOption.java eu/bolt/client/orderpreferences/core/domain/model/SelectedOrderPreference.java eu/bolt/client/orderpreferences/data/model/OrderPreferenceNetworkModel.java eu/bolt/client/orderpreferences/domain/model/OrderPreferenceOption.java eu/bolt/client/orderpreferences/ribs/preferences/OrderPreferencesBottomSheetRibPresenter.java eu/bolt/client/orderpreferences/ribs/selection/PreferenceSelectionBottomSheetRibPresenter.java eu/bolt/client/orderpreferences/ui/model/OrderPreferenceSelectionOptionUiModel.java eu/bolt/client/orderpreferences/ui/model/OrderPreferenceUiModel.java eu/bolt/client/payment/rib/overview/balance/BalanceSummaryRibInteractor.java eu/bolt/client/profile/rib/deletionflow/AccountDeletionFlowRibRouter.java eu/bolt/client/profile/rib/profileedit/ProfileEditRibInteractor.java eu/bolt/client/profilecontent/rib/profilesection/ProfileSectionRibInteractor.java eu/bolt/client/ridehistory/audioupload/entity/GetUrlForFileUploadEntity.java eu/bolt/client/ridehistory/audioupload/network/GetUrlForFileUploadResponse.java eu/bolt/client/ridehistory/details/RideDetailsRouter.java eu/bolt/client/sharedprefs/PreferenceKey.java eu/bolt/client/subscriptions/rib/SubscriptionsFlowRibInteractor.java eu/bolt/client/subscriptions/rib/cancel/reasons/input/SubscriptionCancelReasonInputRibInteractor.j

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ava eu/bolt/client/support/web/SupportWebRibInteractor.java eu/bolt/client/targeting/TargetingManagerImpl.java eu/bolt/client/trips/filters/TripsFilterRibInteractor.java eu/bolt/client/user/domain/model/User.java eu/bolt/client/user/domain/model/a.java eu/bolt/client/verifyprofile/domain/model/PasskeyAuthentication.java eu/bolt/horizontalselector/ribs/HorizontalSelectorRibInteractor.java eu/bolt/micromobility/categoriesoverview/data/model/GetVehiclesResponse.java eu/bolt/micromobility/categoriesoverview/domain/model/BadgeStyleConfig.java eu/bolt/micromobility/networkshared/data/network/model/ConfirmationViewNetworkModel.java eu/bolt/micromobility/networkshared/data/network/model/VehicleOnMapNetworkModel.java eu/bolt/micromobility/onboarding/rib/MicromobilityOnboardingFlowRibInteractor.java eu/bolt/micromobility/order/data/network/model/response/GetCancelReservationScreenResponse.java eu/bolt/micromobility/ridefinished/domain/model/RideFinishedReportIssueState.java eu/bolt/micromobility/ridefinished/networkshared/data/network/model/FinishRideConfirmationViewModel.java eu/bolt/micromobility/ridefinished/networkshared/data/network/model/FinishRideReportIssueViewNetworkModel.java eu/bolt/micromobility/ridefinished/networkshared/data/network/model/ParkingPhotoMandatoryScreenNetworkModel.java eu/bolt/micromobility/ridefinished/networkshared/data/network/model/response/ParkingPhotoValidationResponse.java eu/bolt/micromobility/ridefinished/ribs/feedback/

NO	ISSUE	SEVERITY	STANDARDS	FILES
				RideFinishedFeedbackRibInteractor.java eu/bolt/micromobility/ridefinished/ribs/feedback/RideFinishedFeedbackRouter.java eu/bolt/micromobility/ridefinished/ribs/success/RideFinishedSuccessfulRouter.java eu/bolt/micromobility/vehiclecard/networkshared/data/network/model/SubscriptionPackSourceNetworkModel.java eu/bolt/micromobility/vehiclecard/shared/domain/model/SubscriptionSource.java eu/bolt/micromobility/vehiclecard/ui/ribs/route/RouteOnMapRibInteractor.java eu/bolt/mqtt/model/MqttAuth.java eu/bolt/rentals/cityzones/data/database/model/RentalCityAreaFiltersDbModel.java eu/bolt/rentals/cityzones/domain/model/RentalCityAreaFilterParams.java eu/bolt/rentals/subscriptions/rib/subscriptionlist/SubscriptionListRibInteractor.java eu/bolt/rhsafety/core/data/network/model/UnsafeDrivingOption.java eu/bolt/rhsafety/core/domain/model/ReportUnsafeDrivingOption.java eu/bolt/rhsafety/domain/interactor/UpdateAudioRecordingStateUseCase.java eu/bolt/rhsafety/ui/model/ReportUnsafeDrivingFormUIOption.java eu/bolt/ridehailing/core/data/network/model/GetCryptoKeyResponse.java eu/bolt/ridehailing/core/domain/model/ActiveOrdersEntity.java eu/bolt/ridehailing/core/domain/model/GetCryptoKeyEntity.java eu/bolt/ridehailing/core/domain/model/vehicles/InvalidationKeyState.java eu/bolt/ridehailing/core/domain/model/vehicles/SelectedVehiclesEntity.java eu/bolt/ridehailing/core/domain/model/vehicles/VehiclesPollingResult.java eu/bolt/ridehailing/domain/liveactivity/preference/LastLiveActivityPreferenceController.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eu/bolt/ridehailing/ui/ribs/activerideflow/activerideinfo/RideInfoRibInteractor.java eu/bolt/ridehailing/ui/ribs/activerideflow/finishedrideflow/RideFinishedFlowRouter.java eu/bolt/ridehailing/ui/ribs/activerideflow/finishedrideflow/finishedride/RideFinishedRouter.java eu/bolt/ridehailing/ui/ribs/pickupdirections/PickupDirectionsRibRouter.java eu/bolt/ridehailing/ui/ribs/preorder/addresssearch/AddressSearchRibInteractor.java eu/bolt/searchaddress/ui/ribs/chooselocationmap/ChooseLocationMapRibInteractor.java eu/bolt/searchaddress/ui/ribs/favourite/prediction/PredictionBasedFavLocationFlowRibRouter.java eu/bolt/servicedesk/report/model/ServiceDeskReportData.java eu/bolt/servicedesk/report/usecase/SendServiceDeskReportUseCase.java eu/bolt/verification/core/network/model/VerificationCameraContentNetworkModel.java eu/bolt/verification/core/rib/VerificationFlowRouterImpl.java io/ktor/client/request/forms/FormPart.java io/ktor/http/auth/HttpAuthHeader.java io/ktor/http/x.java io/netty/handler/codec/http/HttpHeaders.java io/netty/handler/ssl/PemPrivateKey.java io/netty/handler/ssl/SslMasterKeyHandler.java org/jctools/maps/NonBlockingHashMap.java org/jctools/maps/NonBlockingIdentityHashMap.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	bo/app/r20.java com/braze/support/IntentUtils.java com/clevertap/android/sdk/pushnotification/e.java com/clevertap/android/sdk/pushnotification/g.java com/vulog/carshare/ble/utils/CommonUtil.java io/netty/handler/ssl/util/ThreadLocalInsecureRandom.java io/netty/util/internal/PlatformDependent.java io/netty/util/internal/ThreadLocalRandom.java j$/util/concurrent/ThreadLocalRandom.java java9/util/concurrent/ThreadLocalRandom.java
3	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/clevertap/android/sdk/inapp/f.java com/clevertap/android/sdk/inapp/i.java ee/mtakso/client/activity/ThreeDSActivity.java
				co/touchlab/kermit/e.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/c.java com/bumptech/glide/disklrucache/b.java com/bumptech/glide/gifdecoder/d.java com/bumptech/glide/gifdecoder/f.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/load/data/mediastore/c.java com/bumptech/glide/load/data/mediastore/e.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/bitmap_recycle/j.java com/bumptech/glide/load/engine/bitmap_recycle

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	/l.java com/bumptech/glide/load/engine/cache/e.java com/bumptech/glide/load/engine/cache/l.java com/bumptech/glide/load/engine/executor/a.java com/bumptech/glide/load/engine/executor/b.java com/bumptech/glide/load/engine/g.java com/bumptech/glide/load/engine/i.java com/bumptech/glide/load/engine/prefill/a.java com/bumptech/glide/load/engine/w.java com/bumptech/glide/load/model/c.java com/bumptech/glide/load/model/d.java com/bumptech/glide/load/model/g.java com/bumptech/glide/load/model/t.java com/bumptech/glide/load/model/u.java com/bumptech/glide/load/model/v.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/bitmap/b0.java com/bumptech/glide/load/resource/bitmap/e.java com/bumptech/glide/load/resource/bitmap/g.java com/bumptech/glide/load/resource/bitmap/k0.java com/bumptech/glide/load/resource/bitmap/v.java com/bumptech/glide/load/resource/bitmap/w.java com/bumptech/glide/load/resource/gif/a.java com/bumptech/glide/load/resource/gif/d.java com/bumptech/glide/load/resource/gif/j.java com/bumptech/glide/load/resource/j.java com/bumptech/glide/manager/e.java com/bumptech/glide/manager/r.java com/bumptech/glide/manager/s.java com/bumptech/glide/module/e.java com/bumptech/glide/request/SingleRequest.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/request/target/f.java com/bumptech/glide/request/target/r.java com/bumptech/glide/util/c.java com/bumptech/glide/util/pool/a.java com/veriff/sdk/camera/core/ImageProcessingUtil.java com/veriff/sdk/camera/core/Logger.java eu/bolt/chat/tools/logger/a.java eu/bolt/logger/a.java io/ktor/client/plugins/logging/g.java io/ktor/http/parsing/d.java io/ktor/util/q.java io/netty/util/Version.java io/netty/util/internal/logging/MessageFormatter.java io/sentry/android/core/z1.java io/sentry/j7.java io/sentry/transport/b0.java org/ccil/cowan/tagsoup/c.java org/ccil/cowan/tagsoup/jaxp/a.java org/jctools/maps/ConcurrentAutoTable.java org/jctools/maps/NonBlockingHashMap.java org/jctools/maps/NonBlockingHashMapLong.java org/jctools/maps/NonBlockingIdentityHashMap.java org/jctools/maps/NonBlockingSetInt.java org/slf4j/helpers/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/clevertap/android/sdk/network/e.java com/hivemq/client/util/a.java eu/bolt/client/network/di/module/a.java io/netty/handler/ssl/JdkSslClientContext.java io/netty/handler/ssl/JdkSslServerContext.java io/netty/handler/ssl/ReferenceCountedOpenSslClientContext.java io/netty/handler/ssl/ReferenceCountedOpenSslServerContext.java io/netty/handler/ssl/SslContext.java io/netty/handler/ssl/util/FingerprintTrustManagerFactory.java io/netty/handler/ssl/util/FingerprintTrustManagerFactoryBuilder.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/clevertap/android/sdk/j.java io/netty/handler/ssl/SslContext.java io/netty/handler/ssl/util/OpenJdkSelfSignedCertGenerator.java
7	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	ee/mtakso/internal/storage/StorageTotalFreeSpaceLegacyRepositoryImpl.java eu/bolt/client/datacollector/data/telephony/DataPointCollector.java eu/bolt/client/screenshot/strategy/FileCreationScreenshotDetectionStrategy.java io/sentry/android/core/v0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	bo/app/as.java bo/app/cx.java bo/app/d60.java bo/app/dq.java bo/app/i80.java bo/app/iu.java bo/app/kc0.java bo/app/lq.java bo/app/mq.java bo/app/mt.java bo/app/nf0.java bo/app/om.java bo/app/pc.java bo/app/q.java bo/app/se0.java bo/app/t50.java bo/app/tx.java bo/app/vd0.java bo/app/z30.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/managers/BrazeGeofenceManager.java
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/clevertap/android/sdk/cryption/a.java com/vulog/carshare/ble/f/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	com/veriff/sdk/camera/core/ImageSaver.java io/netty/handler/codec/http/multipart/AbstractDiskHttpData.java io/netty/handler/ssl/util/SelfSignedCertificate.java io/netty/util/internal/NativeLibraryLoader.java io/netty/util/internal/PlatformDependent.java
11	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	com/mobileapptracker/b.java eu/bolt/android/audio_recording_engine/engine/e.java io/ktor/util/CryptoKt__CryptoJvmKt.java io/ktor/util/NonceKt$nonceGeneratorJob$1.java io/netty/handler/codec/http/websocketx/WebSocketUtil.java io/sentry/util/y.java
12	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	com/clevertap/android/sdk/inbox/g.java eu/bolt/client/helper/ClipboardHelper.java
13	MD5 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	com/airbnb/lottie/network/f.java com/braze/support/StringUtils.java com/clevertap/android/sdk/cryption/a.java com/f2prateek/rx/preferences2/EncryptedSharedPreferences.java com/mobileapptracker/b.java io/ktor/client/plugins/cache/storage/FileCacheStorage.java io/netty/handler/codec/http/websocketx/WebSocketUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/mixpanel/android/mpmetrics/MPDbAdapter.java
15	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/n.java
16	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/n.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/appsflyer/internal/AFa1oSDK.java com/appsflyer/internal/AFb1rSDK.java com/appsflyer/internal/AFe1jSDK.java com/braze/Braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/inappmessage/views/InAppMessageHtmlBaseView.java com/braze/ui/support/UriUtils.java com/clevertap/android/sdk/CleverTapAPI.java com/clevertap/android/sdk/InAppNotificationActivity.java com/clevertap/android/sdk/inapp/d.java com/clevertap/android/sdk/inbox/m.java com/clevertap/android/sdk/pushnotification/CTNotificationIntentService.java com/clevertap/android/sdk/pushnotification/CTPushNotificationReceiver.java com/clevertap/android/sdk/pushnotification/e.java com/clevertap/android/sdk/pushnotification/g.java com/mobileapptracker/g0.java ee/mtakso/client/fcm/delegate/ShowNotificationPushDelegate.java ee/mtakso/client/fcm/handlers/z.java ee/mtakso/client/newbase/RideHailingMapActivityExtrasHandler.java ee/mtakso/client/newbase/deeplink/dispatcher/ScheduledRidesOnboardingDispatcher.java ee/mtakso/client/notifications/local/HandleLocalNotificationUseCase.java eu/bolt/android/deeplink/core/key/DeeplinkConst.java eu/bolt/android/webview/WebPageRibPresenterImpl.java eu/bolt/android/webview/util/a.java eu/bolt/client/carsharing/push/OrderLiveActivityNotificationBuilder.java eu/bolt/client/core/market/domain/OpenAppMarketDelegate.java eu/bolt/client/extensions/p.java eu/bolt/client/extensions/v.java eu/bolt/client/geofencing/GeofencingBroadcastReceiver.java eu/bolt/client/homewidget/HomeWidgetUpdater.java eu/bolt/client/micromobility/liveactivity/notification/OrderLiveActivityNotificationBuilder.java eu/bolt/client/ribsshared/intent/d.java eu/bolt/ridehailing/domain/liveactivity/delegate/LiveActivityPushDelegate.java

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	bo/app/lq.java com/appsflyer/internal/AFi1pSDK.java com/clevertap/android/sdk/n0.java com/mixpanel/android/mpmetrics/q.java com/mobileapptracker/g.java eu/bolt/client/datacollector/data/telephony/DataPointCollector.java
00065	Get the country code of the SIM card provider	collection	com/clevertap/android/sdk/n0.java eu/bolt/client/datacollector/data/telephony/DataPointCollector.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFj1rSDK.java com/appsflyer/internal/AFj1tSDK.java com/appsflyer/internal/AFj1uSDK.java com/appsflyer/internal/AFj1zSDK.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFd1jSDK.java com/appsflyer/internal/AFd1zSDK.java com/bumptech/glide/load/data/j.java com/clevertap/android/sdk/bitmap/e.java com/mixpanel/android/util/b.java com/mobileapptracker/l0.java io/sentry/SpotlightIntegration.java io/sentry/transport/o.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/b.java com/bumptech/glide/load/data/j.java com/clevertap/android/sdk/bitmap/e.java com/mobileapptracker/l0.java io/sentry/SpotlightIntegration.java io/sentry/transport/o.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFd1jSDK.java com/appsflyer/internal/AFd1zSDK.java com/appsflyer/internal/AFe1aSDK.java com/bumptech/glide/load/data/j.java com/clevertap/android/sdk/bitmap/e.java com/mixpanel/android/util/b.java com/mobileapptracker/l0.java io/sentry/SpotlightIntegration.java io/sentry/transport/o.java
00036	Get resource file from res/raw directory	reflection	com/appsflyer/internal/AFf1zSDK.java com/appsflyer/internal/AFj1rSDK.java com/appsflyer/internal/AFj1uSDK.java com/appsflyer/internal/AFj1vSDK.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java com/clevertap/android/sdk/CleverTapAPI.java com/clevertap/android/sdk/pushnotification/CTNotificationIntentService.java com/clevertap/android/sdk/pushnotification/CTPushNotificationReceiver.java com/clevertap/android/sdk/pushnotification/d.java com/clevertap/android/sdk/pushnotification/e.java com/clevertap/android/sdk/pushnotification/g.java ee/mtakso/client/fcm/handlers/z.java eu/bolt/client/carsharing/push/OrderLiveActivityNotificationBuilder.java eu/bolt/client/core/market/domain/OpenAppMarketDelegate.java eu/bolt/client/extensions/p.java eu/bolt/client/homewidget/HomeWidgetUpdater.java eu/bolt/client/micromobility/liveactivity/notification/OrderLiveActivityNotification Builder.java eu/bolt/client/ribsshared/intent/d.java eu/bolt/ridehailing/domain/liveactivity/delegate/LiveActivityPushDelegate.java
			bo/app/ea.java bo/app/fa.java bo/app/ko.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	bo/app/rb0.java bo/app/ug0.java bo/app/xc.java com/airbnb/lottie/d0.java com/airbnb/lottie/network/f.java com/airbnb/lottie/network/g.java com/appsflyer/internal/AFg1oSDK.java com/braze/d0.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/clevertap/android/sdk/utils/c.java com/hivemq/client/util/a.java com/veriff/sdk/camera/core/VideoCapture.java ee/mtakso/client/monitors/AppStorageMonitor.java eu/bolt/android/audio_recording_engine/engine/AudioRecorderImpl.java eu/bolt/android/audio_recording_engine/engine/FileDeletionUtil.java eu/bolt/client/camera/camerax/CameraDelegate.java eu/bolt/client/carsharing/ribs/worker/CarsharingCleanUpWorker.java eu/bolt/client/screenshot/FileCreationEventsRepository$fileCreationDetectorFlow$1.java eu/bolt/micromobility/report/worker/ReportCleanUpWorker.java eu/bolt/verification/core/domain/interactor/PreparePreviewPhotoUseCase.java io/netty/handler/codec/http/multipart/DiskFileUpload.java io/netty/util/internal/NativeLibraryLoader.java io/sentry/SentryOptions.java io/sentry/android/core/cache/b.java io/sentry/android/core/v0.java io/sentry/android/core/z.java io/sentry/android/replay/ReplayCache.java io/sentry/android/replay/capture/BufferCaptureStrategy.java io/sentry/c3.java io/sentry/cache/c.java io/sentry/cache/d.java io/sentry/cache/f.java io/sentry/e3.java io/sentry/instrumentation/file/a.java io/sentry/q.java io/sentry/y.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	bo/app/pa0.java bo/app/sq.java com/airbnb/lottie/network/f.java com/airbnb/lottie/network/g.java com/appsflyer/internal/AFc1tSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFg1oSDK.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/bumptech/glide/disklrucache/b.java com/bumptech/glide/load/b.java com/bumptech/glide/load/model/g.java com/bumptech/glide/load/resource/bitmap/c0.java com/clevertap/android/sdk/utils/b.java com/hivemq/client/util/a.java com/veriff/sdk/camera/core/ImageSaver.java eu/bolt/servicedesk/report/repository/ServiceDeskReportRepository$getServiceDeskReport$2.java eu/bolt/servicedesk/report/storage/ServiceDeskLogsStorage.java eu/bolt/servicedesk/report/usecase/CollectServiceDeskReportLogsUseCase.java io/ktor/client/plugins/cache/storage/FileCacheStorage.java io/netty/handler/ssl/PemReader.java io/netty/handler/ssl/util/SelfSignedCertificate.java io/netty/resolver/HostsFileEntriesProvider.java io/netty/util/NetUtil.java io/netty/util/internal/PlatformDependent.java io/sentry/android/core/b2.java io/sentry/android/replay/ReplayCache.java io/sentry/c3.java io/sentry/cache/c.java io/sentry/cache/d.java io/sentry/cache/f.java io/sentry/config/e.java io/sentry/e3.java io/sentry/instrumentation/file/b.java io/sentry/instrumentation/file/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
			io/sentry/util/f.java io/sentry/y.java okio/q0.java
00163	Create new Socket and connecting to it	socket	com/hivemq/client/internal/mqtt/handler/proxy/a.java com/hivemq/client/internal/netty/b.java io/netty/bootstrap/Bootstrap.java io/netty/channel/AbstractChannel.java io/netty/channel/AbstractChannelHandlerContext.java io/netty/channel/ChannelDuplexHandler.java io/netty/channel/ChannelOutboundHandlerAdapter.java io/netty/channel/CombinedChannelDuplexHandler.java io/netty/channel/DefaultChannelPipeline.java io/netty/channel/embedded/EmbeddedChannel.java io/netty/channel/socket/nio/NioDatagramChannel.java io/netty/channel/socket/nio/NioDomainSocketChannel.java io/netty/channel/socket/nio/NioSocketChannel.java io/netty/channel/socket/oio/OioDatagramChannel.java io/netty/channel/socket/oio/OioSocketChannel.java io/netty/handler/address/DynamicAddressConnectHandler.java io/netty/handler/address/ResolveAddressHandler.java io/netty/handler/codec/DatagramPacketEncoder.java io/netty/handler/codec/http/HttpClientUpgradeHandler.java io/netty/handler/codec/http/websocketx/WebSocketClientProtocolHandler.java io/netty/handler/codec/http/websocketx/WebSocketProtocolHandler.java io/netty/handler/codec/http/websocketx/WebSocketServerProtocolHandler.java io/netty/handler/codec/spdy/SpdyFrameCodec.java io/netty/handler/logging/LoggingHandler.java io/netty/handler/ssl/SslClientHelloHandler.java io/netty/handler/ssl/SslHandler.java io/netty/util/internal/SocketUtils.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/mobileapptracker/g0.java ee/mtakso/client/newbase/deeplink/dispatcher/ScheduledRidesOnboardingDispatcher.java eu/bolt/android/webview/WebPageRibPresenterImpl.java eu/bolt/client/homewidget/HomeWidgetUpdater.java

RULE ID	BEHAVIOUR	LABEL	FILES
00112	Get the date of the calendar event	collection calendar	eu/bolt/client/scheduledrides/timepicker/delegate/ScheduledRidesDateTimeDelegate.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1kSDK.java eu/bolt/client/download/e.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFa1oSDK.java com/appsflyer/internal/AFa1tSDK.java com/braze/push/BrazeNotificationUtils.java com/clevertap/android/sdk/CleverTapAPI.java com/clevertap/android/sdk/pushnotification/CTNotificationIntentService.java com/clevertap/android/sdk/pushnotification/fcm/CTFirebaseMessagingReceiver.java eu/bolt/client/sms/VerificationSmsProviderImpl.java
00034	Query the current data network type	collection network	com/clevertap/android/sdk/o1.java
00094	Connect to a URL and read data from it	command network	com/clevertap/android/sdk/o1.java com/mixpanel/android/util/b.java
00195	Set the output path of the recorded file	record file	eu/bolt/android/audio_recording_engine/engine/AudioRecorderImpl.java
00199	Stop recording and release recording resources	record	eu/bolt/android/audio_recording_engine/engine/AudioRecorderImpl.java
00198	Initialize the recorder and start recording	record	eu/bolt/android/audio_recording_engine/engine/AudioRecorderImpl.java
00194	Set the audio source (MIC) and recorded file format	record	eu/bolt/android/audio_recording_engine/engine/AudioRecorderImpl.java

RULE ID	BEHAVIOUR	LABEL	FILES
00197	Set the audio encoder and initialize the recorder	record	eu/bolt/android/audio_recording_engine/engine/AudioRecorderImpl.java
00007	Use absolute path of directory for the output media file path	file	eu/bolt/android/audio_recording_engine/engine/AudioRecorderImpl.java
00196	Set the recorded file format and output path	record file	eu/bolt/android/audio_recording_engine/engine/AudioRecorderImpl.java
00041	Save recorded audio/video to file	record	eu/bolt/android/audio_recording_engine/engine/AudioRecorderImpl.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/b.java com/appsflyer/internal/AFd1jSDK.java com/appsflyer/internal/AFd1zSDK.java com/mixpanel/android/util/b.java com/mobileapptracker/l0.java io/sentry/SpotlightIntegration.java io/sentry/transport/o.java
00108	Read the input stream from given URL	network command	com/mixpanel/android/util/b.java
00208	Capture the contents of the device screen	collection screen	eu/bolt/screenshotty/internal/projection/c.java
00209	Get pixels from the latest rendered image	collection	com/veriff/sdk/camera/core/ImageCapture.java eu/bolt/screenshotty/internal/projection/c.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	eu/bolt/screenshotty/internal/projection/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFj1tSDK.java eu/bolt/client/core/contactpicker/domain/a.java eu/bolt/verification/core/domain/interactor/FileDetailsCollectorUseCase.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFj1tSDK.java eu/bolt/client/core/contactpicker/domain/a.java eu/bolt/verification/core/domain/interactor/FileDetailsCollectorUseCase.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1kSDK.java com/appsflyer/internal/AFj1tSDK.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFj1tSDK.java eu/bolt/client/core/contactpicker/domain/a.java eu/bolt/verification/core/domain/interactor/FileDetailsCollectorUseCase.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFj1tSDK.java eu/bolt/client/core/contactpicker/domain/a.java eu/bolt/verification/core/domain/interactor/FileDetailsCollectorUseCase.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1kSDK.java com/appsflyer/internal/AFj1tSDK.java com/bumptech/glide/load/data/mediastore/c.java
00012	Read data and put it into a buffer stream	file	io/ktor/client/plugins/cache/storage/FileCacheStorage.java io/sentry/c3.java io/sentry/cache/c.java io/sentry/cache/f.java io/sentry/config/e.java io/sentry/util/f.java io/sentry/y.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFg1oSDK.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/d0.java com/appsflyer/internal/AFg1oSDK.java
00162	Create InetSocketAddress object and connecting to it	socket	com/hivemq/client/internal/mqtt/handler/proxy/a.java io/netty/bootstrap/Bootstrap.java io/netty/channel/AbstractChannel.java io/netty/channel/socket/nio/NioDatagramChannel.java io/netty/channel/socket/nio/NioSocketChannel.java io/netty/channel/socket/oio/OioDatagramChannel.java io/netty/channel/socket/oio/OioSocketChannel.java io/netty/handler/codec/DatagramPacketEncoder.java io/netty/util/internal/SocketUtils.java
00009	Put data in cursor to JSON object	file	com/clevertap/android/sdk/db/DBAdapter.java com/mixpanel/android/mpmetrics/MPDbAdapter.java
00004	Get filename and put it to JSON object	file collection	com/airbnb/lottie/d0.java com/clevertap/android/sdk/db/DBAdapter.java com/mixpanel/android/mpmetrics/MPDbAdapter.java
00016	Get location info of the device and put it to JSON object	location collection	com/braze/models/outgoing/BrazeLocation.java com/clevertap/android/sdk/utils/a.java
00115	Get last known location of the device	collection location	com/clevertap/android/sdk/b1.java
00123	Save the response to JSON after connecting to the remote server	network command	com/mobileapptracker/l0.java
00024	Write file after Base64 decoding	reflection file	com/airbnb/lottie/d0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00132	Query The ISO country code	telephony collection	com/mobileapptracker/g.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	eu/bolt/chat/media/a.java eu/bolt/chat/media/b.java eu/bolt/client/design/image/BitmapSerializableWrapper.java
00187	Query a URI and check the result	collection sms calllog calendar	eu/bolt/client/calendar/c.java
00028	Read file from assets directory	file	eu/bolt/client/micromobility/confirmationflow/ui/opengl/Shader.java
00038	Query the phone number	collection	eu/bolt/client/datacollector/data/telephony/DataPointCollector.java
00130	Get the current WIFI information	wifi collection	eu/bolt/client/datacollector/data/telephony/DataPointCollector.java
00033	Query the IMEI number	collection	eu/bolt/client/datacollector/data/telephony/DataPointCollector.java
00066	Query the ICCID number	collection	eu/bolt/client/datacollector/data/telephony/DataPointCollector.java
00083	Query the IMEI number	collection telephony	eu/bolt/client/datacollector/data/telephony/DataPointCollector.java
00128	Query user account information	collection account	com/mobileapptracker/z.java
00075	Get location of the device	collection location	eu/bolt/client/locationcore/data/location/ReserveLocationProvider.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://taxify-client.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/718916732167/namespaces/firebase:fetch?key=AIzaSyA1oNkgJ-bbPAuP4jM5Zb8HA8yROWwLJtw. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK
Other Common Permissions	9/44	android.permission.FOREGROUND_SERVICE, android.permission.ACCESS_BACKGROUND_LOCATION, com.google.android.gms.permission.AD_ID, android.permission.READ_CALENDAR, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
dust.k8s.test-001.d-usw-2.braze.com	ok	No Geolocation information available.
svalidate-and-log.s	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
sdk.iad-01.braze.com	ok	**IP:** 104.18.39.68 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cs.android.com	ok	**IP:** 142.250.139.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
business.bolt.eu	ok	**IP:** 18.67.39.99 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
privacy-sandbox.appsflyersdk.com	ok	**IP:** 3.164.92.60 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
i1.wp.com	ok	**IP:** 192.0.77.2 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.748425 **Longitude:** -122.413673 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.taxify.eu	ok	**IP:** 18.67.39.16 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
player.vimeo.com	ok	**IP:** 162.159.128.61 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
upload.wikimedia.org	ok	**IP:** 208.80.154.240 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.791256 **Longitude:** -122.400810 **View:** Google Map
img.utdstc.com	ok	**IP:** 151.101.139.52 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
iamcache.braze	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.eclipse.org	ok	**IP:** 198.41.30.198 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.345139 **Longitude:** -75.765076 **View:** Google Map
assets3.lottiefiles.com	ok	**IP:** 104.18.38.252 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
sars.s	ok	No Geolocation information available.
previews.123rf.com	ok	**IP:** 18.67.17.59 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
placekitten.com	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
static.onecms.io	ok	**IP:** 162.159.141.224 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.ccil.org	ok	**IP:** 192.178.192.121 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ktor.io	ok	**IP:** 3.164.92.43 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
gethopp.com	ok	**IP:** 18.67.17.112 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
netty.io	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
youtrack.jetbrains.com	ok	**IP:** 63.35.30.167 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
sondheim.braze.com	ok	**IP:** 172.64.144.252 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.bolt.eu	ok	**IP:** 18.67.17.4 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.braze.com	ok	**IP:** 104.17.228.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.mixpanel.com	ok	**IP:** 107.178.240.159 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sviap.s	ok	No Geolocation information available.
vereshchaka-private.s3.eu-central-1.amazonaws.com	ok	**IP:** 3.5.138.82 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
svalidate.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.openssl.org	ok	**IP:** 34.49.79.89 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
admin-panel.prelive.bolt.eu	ok	**IP:** 172.65.228.109 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
assets4.lottiefiles.com	ok	**IP:** 172.64.149.4 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
sadrevenue.s	ok	No Geolocation information available.
blog.passmefast.co.uk	ok	**IP:** 104.26.5.89 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
s.prelive.bolt.eu	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
bolt.eu	ok	**IP:** 104.18.36.249 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
static.wizrocket.com	ok	**IP:** 3.164.92.92 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
taxify.atlassian.net	ok	**IP:** 13.227.180.4 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
images.bolt.eu	ok	**IP:** 3.164.92.51 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.forest.me	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
admin-panel.bolt.eu	ok	**IP:** 172.65.240.204 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sattr.s	ok	No Geolocation information available.
pngimg.com	ok	**IP:** 104.26.4.108 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.politsei.ee	ok	**IP:** 141.101.90.17 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
cdn-icons-png.flaticon.com	ok	**IP:** 67.69.196.145 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.402420 **Longitude:** -75.653954 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
taxify-client.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
admin.bolt.eu	ok	**IP:** 172.65.240.204 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
i.ibb.co	ok	**IP:** 207.174.26.219 **Country:** United States of America **Region:** Colorado **City:** Longmont **Latitude:** 40.165714 **Longitude:** -105.136505 **View:** Google Map
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
s.bolt.eu	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
alchemy.veriff.com	ok	**IP:** 18.245.104.58 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
i.insider.com	ok	**IP:** 151.101.138.217 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
prelive.bolt.eu	ok	**IP:** 104.18.36.249 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
s-admin.prelive.taxify.eu	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
starwarsblog.starwars.com	ok	**IP:** 184.150.70.56 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.402420 **Longitude:** -75.653954 **View:** Google Map
play.google.com	ok	**IP:** 192.178.192.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
static.wikia.nocookie.net	ok	**IP:** 74.120.184.204 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.788464 **Longitude:** -122.394608 **View:** Google Map
admin.prelive.bolt.eu	ok	**IP:** 172.65.228.109 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
partners.bolt.eu	ok	**IP:** 18.245.104.76 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
s-admin.taxify.eu	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
static.vecteezy.com	ok	**IP:** 172.64.152.224 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
memegenerator.net	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
lumiere-a.akamaihd.net	ok	**IP:** 184.150.163.88 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.402420 **Longitude:** -75.653954 **View:** Google Map
www.inclusion-europe.eu	ok	**IP:** 84.16.76.207 **Country:** Switzerland **Region:** Geneve **City:** Carouge **Latitude:** 46.180962 **Longitude:** 6.139210 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
habrastorage.org	ok	**IP:** 95.47.173.34 **Country:** Estonia **Region:** Harjumaa **City:** Tallinn **Latitude:** 59.436958 **Longitude:** 24.753531 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
spia.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
wiki.eclipse.org	ok	**IP:** 198.41.30.195 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.345139 **Longitude:** -75.765076 **View:** Google Map
node.bolt.eu	ok	**IP:** 104.18.36.249 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
i.imgflip.com	ok	**IP:** 104.16.40.101 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.facebook.com	ok	**IP:** 31.13.71.36 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map
google.com	ok	**IP:** 142.250.137.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
user.live.boltsvc.net	ok	**IP:** 172.64.154.110 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

EMAILS

EMAIL	FILE
this@copy.slice	io/ktor/util/j0.java

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
CleverTap	Location, Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/174
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Flipper	Analytics	https://reports.exodus-privacy.eu.org/trackers/392
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447
Tune	Analytics	https://reports.exodus-privacy.eu.org/trackers/38

HARDCODED SECRETS

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"ar_core_key" : "AIzaSyBCrsKCcwYojdbT_ALZ9qI8hl2Z_pnZQw8"
"braze_api_key" : "bb337267-38b5-4b4d-9e4c-f6238d69bf06"
"carsharing_car_key_mode_banner_connecting_v2" : "Connecting..."
"clevertap_account_token" : "3aa-600"
"com.google.firebase.crashlytics.mapping_file_id" : "6b94469adf3846aba2b658ee3c6546c8"
"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"
"facebook_client_token" : "dc2d1966f5960e30234a7832bf765fd8"
"firebase_database_url" : "https://taxify-client.firebaseio.com"
"google_api_key" : "AIzaSyA1oNkgJ-bbPAuP4jM5Zb8HA8yROWwLJtw"
"google_auth_web_client_id" : "718916732167-fg6lta9iiuo6o1pcrnhat8fsot6hd6nd.apps.googleusercontent.com"
"google_crash_reporting_api_key" : "AIzaSyA1oNkgJ-bbPAuP4jM5Zb8HA8yROWwLJtw"

POSSIBLE SECRETS
"google_maps_key" : "AIzaSyCEcs8rW-83laJLGF-oSUTPFvnv1dJi47E"
50d4ace1-3ad6-455e-992e-1489c63a3d90
6e400002-b5a3-f393-e0a9-e50e24dcca9e
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
18cfd564147c65144daaeeed505bbb60
1cbd3130fa23b59692c061c594c16cc0
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
db43f61d7a0610f4a57c29be27a38897
567484d7dd0895ff5d8b4849
c6f78175ab66f9474487f8e777fc0d7b
fb28fa831029f96af7dc3b43c602f144
df9f369bd1c71b8b5700beae0f6ec485f22b4c3daec37c4f6d52b6df682d7063
c56fb7d591ba6704df047fd98f535372fea00211
cc2751449a350f668590264ed76692694a80308a
Mtz4Rj18FV0a401PxJWjOmNoEa6ox5YNVYI

POSSIBLE SECRETS
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
a84ec91056c45148ff2877ec0259ee3b
23456789abcdefghjkmnpqrstvwxyz
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
308203c7308202afa003020102021500dc286b43b4ea12039958a00a6655eb84720e46c9300d06092a864886f70d01010b05003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577311430120603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577311430120603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f6964310300e06035504031307416e64726f6964301e170d313730383034313635333375a170d343730383034313635333375a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577311430120603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f6964310300e06035504031307416e64726f69643082012230
0d06092a864886f70d01010105000382010f003082010a0282010100898646f47fc333db09644c303104ed183e904e351152aa66a603b77f63389d45d6fcffae3c94fadf1f28038e265d697fea347327f9081a7f0b9074d5b148db5bf357c611a77f87f844a15068818bdcd5b21d187e93fa2551676170eedce04a150c35ec0a791eef507fa9b406573c36f6f207764842e5677e35a281a422659e91e26eb4fecfb053b5c936d0976c37f8757adb57a37953da5844ea350695854d343a61ad341b63a1c425d22855af7ebfee018e1736cee98536be5b9947f288e2a26f99eb9f91b5de93fecc513019d2e90f12b38610d1f02eaa81deca4ce91c19cbce36d6c3025ce2432b3d178616beafaf437c08451bc469c6bc6f4517a714a5b0203010001a350304e300c0603551d13040530030101ff301d0603551d0e0416041419a864c0f2618c67c803a23da909bc70521f269b301f0603551d2304183016801419a864c0f2618c67c803a23da909bc70521f269b300d06092a864886f70d01010b05000382010100540
3fc56fdefc440376a0337815002b96a15bffc2fe42de6c58f52fae4d80652e3704455b885409eef81ffbb4c44dba104b6b8e24c9e2e0e7a04338ee73baa5b71bfb4488f8e04bef3d0eaf7d43aa42b03b278c33cc1f0dd3802571624baa161d851fab37db4bc92b9094b6885dff62b400ecd81f069d56a1be1db46d8198c50c9628cdb6e38686ef640fd386775f50376f957e24ea45ed1942968f20c82f189607fdb22f11cfdfd0760a77a60ceb3416cfb3f48f13f9f83f3834a01001750a7c78bc1fd81f0b53a7c41dcba9f5a0118259d083c32bb9ebb84d645d6f6b9c31923d8ab70e7f0a25940ecc9f4945144419f86e8c421d3b99774f4b8f3d09262e7
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
ea02c28d07c2f1e3eeeeb3aa803f9ae6
df6b721c8b4d3b6eb44c861d4415007e5a35fc95

POSSIBLE SECRETS
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
eyJzZXNzaW9uX2lkIjoiMWRhNTAxNWEtOWM0YS00MGQzLTk0N2QtYmI3NTVlZGZkYjYxIiwiaWF0IjoxNjMwNDg1MTY4fQ
6e400003-b5a3-f393-e0a9-e50e24dcca9e
a-95ed6082-b8e9-46e8-a73f-ff56f00f5d9d
86254750241babac4b8d52996a675549
46fafdf2bb7d7862205427ef8c650ea6
58be38eadffae3ef523007f956473e51
55d25469d633fd7665e838aff88eacf6
72ff7e5e-ef19-4915-ae1f-4ca7908cc55a
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
37a6259cc0c1dae299a7866489dff0bd
9b8f518b086098de3d77736f9458a3d2f6f95a37
470fa2b4ae81cd56ecbcda9735803434cec591fa
8a3c4b262d721acd49a4bf97d5213199c86fa2b9

PLAYSTORE INFORMATION

Title: Bolt: Request a Ride

Score: 4.802407 **Installs:** 100,000,000+ **Price:** 0 **Android Version Support:** **Category:** Maps & Navigation **Play Store URL:** ee.mtakso.client

Developer Details: Bolt Technology, 8420210619522248974, None, https://bolt.eu/, info@bolt.eu,

Release Date: Jul 19, 2013 **Privacy Policy:** Privacy link

Description:

Make getting around easier with Bolt! Whether you need a ride across town, an airport transfer, or a scooter to zip through traffic, our app makes it easy to move around confidently and conveniently. WHY CHOOSE BOLT? - Request a ride in seconds: enjoy safe, affordable rides with top-rated drivers. - Transparent pricing: see your fare upfront so there are no surprises. - Multiple payment options: pay securely using a credit/debit card, Apple Pay, Google Pay, or cash. EASY ORDERING: - Open the app and set your destination. - Choose from various ride types to suit your needs (Comfort, Premium, Electric, XL, and more). - Track your driver in real time. - Arrive in comfort and rate your experience. SAFETY FIRST: Some of Bolt's safety features require the app to run in the background. - Emergency assist button: discreetly alert our Safety Team in case of emergencies. - Audio trip recording: record audio during rides for added peace of mind. - Private phone details: your contact information stays confidential when you call a driver. PLAN AHEAD: Need an airport transfer or an early morning ride? You can schedule your trip in advance from 30 minutes to 90 days before your expected pickup time. *JOIN BOLT PLUS TO UNLOCK PREMIUM FEATURES! Get the best of Bolt with Bolt Plus. Enjoy exclusive perks that save you time and money, making every ride smoother and more convenient. *BOLT DRIVE: We're committed to our carbon net zero goal by 2040. That's why we're increasing the lineup of electric and hybrid cars in Bolt Drive, our car-sharing service. You can also rent Bolt scooters and e-bikes via the app. *DELIVER PACKAGES Use the 'Send' ride type to arrange fast and convenient parcel delivery in your city. Bolt is available in 50 countries and 600+ cities worldwide (see the full list at https://bolt.eu/en/cities/). We rebranded from Taxify to Bolt in 2019. Bolt is the perfect taxi alternative for fast, reliable, and affordable rides. The app provides a seamless ride-ordering experience whether you're commuting, travelling, or running errands. So, the next time you need a ride, choose Bolt! *Bolt options differ by location. Check the app for availability in your city. Earn money driving with the Bolt Driver app. Sign up: https://bolt.eu/driver/ Questions? Get in touch via info@bolt.eu or at https://bolt.eu Follow us on social media for updates, discounts, and offers! Facebook — https://www.facebook.com/Bolt/ Instagram — https://www.instagram.com/bolt X — https://x.com/Boltapp

SCAN LOGS

Timestamp	Event	Error
2025-11-27 03:57:54	Generating Hashes	OK
2025-11-27 03:57:54	Extracting APK	OK

2025-11-27 03:57:54	Unzipping	OK
2025-11-27 03:57:55	Parsing APK with androguard	OK
2025-11-27 03:57:56	Extracting APK features using aapt/aapt2	OK
2025-11-27 03:57:56	Getting Hardcoded Certificates/Keystores	OK
2025-11-27 03:58:06	Parsing AndroidManifest.xml	OK
2025-11-27 03:58:06	Extracting Manifest Data	OK
2025-11-27 03:58:06	Manifest Analysis Started	OK
2025-11-27 03:58:06	Performing Static Analysis on: Bolt (ee.mtakso.client)	OK
2025-11-27 03:58:07	Fetching Details from Play Store: ee.mtakso.client	OK
2025-11-27 03:58:07	Checking for Malware Permissions	OK

2025-11-27 03:58:07	Fetching icon path	OK
2025-11-27 03:58:07	Library Binary Analysis Started	OK
2025-11-27 03:58:07	Reading Code Signing Certificate	OK
2025-11-27 03:58:10	Running APKiD 3.0.0	OK
2025-11-27 03:58:36	Detecting Trackers	OK
2025-11-27 03:58:58	Decompiling APK to Java with JADX	OK
2025-11-27 04:08:42	Converting DEX to Smali	OK
2025-11-27 04:08:42	Code Analysis Started on - java_source	OK
2025-11-27 04:10:45	Android SBOM Analysis Completed	OK
2025-11-27 04:11:35	Android SAST Completed	OK
2025-11-27 04:11:35	Android API Analysis Started	OK

2025-11-27 04:12:25	Android API Analysis Completed	OK
2025-11-27 04:12:25	Android Permission Mapping Started	OK
2025-11-27 04:21:58	Android Permission Mapping Completed	OK
2025-11-27 04:22:01	Android Behaviour Analysis Started	OK
2025-11-27 04:23:11	Android Behaviour Analysis Completed	OK
2025-11-27 04:23:11	Extracting Emails and URLs from Source Code	OK
2025-11-27 04:24:06	Email and URL Extraction Completed	OK
2025-11-27 04:24:06	Extracting String data from APK	OK
2025-11-27 04:24:06	Extracting String data from Code	OK
2025-11-27 04:24:06	Extracting String values and entropies from Code	OK
2025-11-27 04:24:33	Performing Malware check on extracted domains	OK

2025-11-27 04:24:42	Saving to Database	OK

Report Generated by - MobSF v4.4.3

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.