## APP SCORES

Security Score 44/100

Trackers Detection 8/432

## FILE INFORMATION

File Name Betala_P_4.5_APKPure.apk

Size 29.6MB

MD5 d6af1200a5e5ec5d4f24b1989b07bc0e

SHA1 f853be67f1c77f7e2bfe5a1e438692f1ed93049c

SHA256 d9f45ed82d36a08ad64d6fa625773ec795af77a6505a23dbd9d4133a9246eb30

## APP INFORMATION

App Name Betala P

Package Name se.stockholm.betalap

Main Activity group.flowbird.mpp.activities.SplashActivity

Target SDK 34 Min SDK 22 Max SDK

Android Version Name 4.5 Android Version Code 28

7 / 53

EXPORTED ACTIVITIES

View All

2 / 23

EXPORTED SERVICES

View All

4 / 18

EXPORTED RECEIVERS

View All

0 / 4

EXPORTED PROVIDERS

View All

## SCAN OPTIONS

## DECOMPILED CODE

## SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-09-22 14:31:34+00:00
Valid To: 2050-09-22 14:31:34+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x8fa9d00d9f9f115fba245cd7ac9aa3644bc37b03
Hash Algorithm: sha256
md5: 0a571f1d1d0fb49591c4ed2df93ad768
sha1: 61d46e2245d8bce84e21477fd515a2f13612d69c
sha256: 886214bc82f3f60e8da54f8293058b6cb2bd5cefc1bc6b36d182b2b6d3ff6691
sha512: 3911366b26d9a6abe78ccb483f25016159aa936b78875fbd8291118c044f39863ddc56efa6c4b7426f65315a2757bdda2404fa16abb7a877020b7260a384e756
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 25acbc73ca4a6fdf1755ac3680eec28238a44496351d8a4b9f44b6f3e6f510e1
Found 1 unique certificates
```

## APPLICATION PERMISSIONS

Search:

| PERMISSION | STATUS | INFO | DESCRIPTION | CODE MAPPINGS |
|---|---|---|---|---|
| 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 | CODE MAPPINGS |
|---|---|---|---|---|
| android.permission.ACCESS_FINE_LOCATION | dangerous | fine (GPS) location | Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power. | |
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. | |
| android.permission.ACCESS_WIFI_STATE | normal | view Wi-Fi status | Allows an application to view the information about the status of Wi-Fi. | |
| android.permission.CAMERA | dangerous | take pictures and videos | Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time. | |
| android.permission.FOREGROUND_SERVICE | normal | enables regular apps to use Service.startForeground. | Allows a regular application to use Service.startForeground. | |
| android.permission.FOREGROUND_SERVICE_DATA_SYNC | normal | permits foreground services for data synchronization. | Allows a regular application to use Service.startForeground with the type "dataSync". | |
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. | |
| android.permission.POST_NOTIFICATIONS | dangerous | allows an app to post notifications. | Allows an app to post notifications | |
| android.permission.READ_EXTERNAL_STORAGE | dangerous | read external storage contents | Allows an application to read from external storage. | |

Showing 1 to 10 of 24 entries

Previous 1 2 3 Next

### ANDROID API

Search:

| API | FILES |
|---|---|
| Android Notifications | |
| Base64 Decode | |
| Base64 Encode | |
| Certificate Handling | |
| Content Provider | |
| Crypto | |
| Dynamic Class and Dexloading | |
| Execute OS Command | |
| Get Installed Applications | |
| Get Network Interface information | |

Showing 1 to 10 of 36 entries

Previous 1 2 3 4 Next

## BROWSABLE ACTIVITIES

Search:

| ACTIVITY | INTENT |
|---|---|
| com.facebook.CustomTabActivity | **Schemes**: fb546567282220964://, fbconnect://,<br>**Hosts:** cct.se.stockholm.betalap, |
| com.google.android.gms.tagmanager.TagManagerPreviewActivity | **Schemes**: tagmanager.c.se.stockholm.betalap://, |
| group.flowbird.mpp.activities.AddDirectDebitActivity | **Schemes**: https://,<br>**Hosts:** @string/webSiteBaseUrl,<br>**Path Prefixes:** @string/deeplink_path_prefix_direct_debit, |
| group.flowbird.mpp.activities.EPurseActivity | **Schemes**: @string/deeplink_path_scheme_swish://,<br>**Hosts:** @string/webSiteBaseUrl,<br>**Path Prefixes:** @string/deeplink_path_prefix_swish_topup, |
| group.flowbird.mpp.activities.MainActivity | **Schemes**: @string/deeplink_path_scheme_swish://,<br>**Hosts:** @string/webSiteBaseUrl,<br>**Path Prefixes:** @string/deeplink_path_prefix_swish, |
| group.flowbird.mpp.activities.SplashActivity | **Schemes**: @string/deep_link_scheme://, https://,<br>**Hosts:** @string/webSiteBaseUrl,<br>**Path Prefixes:** /newPassword, /verification, |

Showing 1 to 6 of 6 entries

Previous 1 Next

## NETWORK SECURITY

| HIGH | WARNING | INFO | SECURE |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | 1 | 0 | 0 |

Search:

| NO | SCOPE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 1 | * | high | Base config is insecurely configured to permit clear text traffic to all domains. |
| 2 | * | warning | Base config is configured to trust system certificates. |

Showing 1 to 2 of 2 entries

Previous 1 Next

## CERTIFICATE ANALYSIS

| HIGH | WARNING | INFO |
|---|---|---|
| 0 | 1 | 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. |
| Signed Application | info | Application is signed with a code signing certificate |

Showing 1 to 2 of 2 entries

Previous 1 Next

## MANIFEST ANALYSIS

| HIGH | WARNING | INFO | SUPPRESSED |
|---|---|---|---|
| 1 | 14 | 0 | 0 |

Search:

| NO | ISSUE | SEVERITY | DESCRIPTION | OPTIONS |
|---|---|---|---|---|
| 1 | App can be installed on a vulnerable upatched Android version<br>Android 5.1-5.1.1, [minSdk=22] | high | This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates. | |
| 2 | App has a Network Security Configuration<br>[android:networkSecurityConfig=@xml/network_security_config] | info | The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app. | |
| 3 | **Activity** (group.flowbird.mpp.activities.AddDirectDebitActivity) is not Protected.<br>[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** (group.flowbird.mpp.activities.MainActivity) is not Protected.<br>[android:exported=true] | warning | An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. | |
| 5 | **Activity** (com.facebook.CustomTabActivity) is not Protected.<br>[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 |
|---|---|---|---|---|
| 6 | TaskAffinity is set for activity (se.stockholm.betalap.wxapi.WXPayEntryActivity) | 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. | |
| 7 | **Activity** (se.stockholm.betalap.wxapi.WXPayEntryActivity) 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 | **Broadcast Receiver** (com.google.android.gms.analytics.CampaignTrackingReceiver) 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. | |
| 9 | **Broadcast Receiver** (com.batch.android.BatchPushMessageReceiver) 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. | |

| NO | ISSUE | SEVERITY | DESCRIPTION | OPTIONS |
|---|---|---|---|---|
| 10 | **Service** (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked.<br>**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. | |

Showing 1 to 10 of 16 entries

Previous 1 2 Next

## </> CODE ANALYSIS

| HIGH | WARNING | INFO | SECURE | SUPPRESSED |
|---|---|---|---|---|
| 5 | 9 | 3 | 2 | 0 |

Search:

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

| NO | ISSUE | SEVERITY | STANDARDS | FILES | OPTIONS |
|---|---|---|---|---|---|
| 2 | Files may contain hardcoded sensitive information like usernames, passwords, keys etc. | warning | **CWE:** CWE-312: Cleartext Storage of Sensitive Information<br>**OWASP Top 10:** M9: Reverse Engineering<br>**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<br>**OWASP Top 10:** M2: Insecure Data Storage<br>**OWASP MASVS:** MSTG-STORAGE-2 | | |
| 4 | 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')<br>**OWASP Top 10:** M7: Client Code Quality | | |
| 5 | The App uses an insecure Random Number Generator. | warning | **CWE:** CWE-330: Use of Insufficiently Random Values<br>**OWASP Top 10:** M5: Insufficient Cryptography<br>**OWASP MASVS:** MSTG-CRYPTO-6 | | |

| NO | ISSUE | SEVERITY | STANDARDS | FILES | OPTIONS |
|---|---|---|---|---|---|
| 6 | MD5 is a weak hash known to have hash collisions. | warning | **CWE:** CWE-327: Use of a Broken or Risky Cryptographic Algorithm<br>**OWASP Top 10:** M5: Insufficient Cryptography<br>**OWASP MASVS:** MSTG-CRYPTO-4 | | |
| 7 | App creates temp file. Sensitive information should never be written into a temp file. | warning | **CWE:** CWE-276: Incorrect Default Permissions<br>**OWASP Top 10:** M2: Insecure Data Storage<br>**OWASP MASVS:** MSTG-STORAGE-2 | net/glxn/qrgen/core/AbstractQRCode.java<br>org/junit/rules/TemporaryFolder.java | |
| 8 | Weak Encryption algorithm used | high | **CWE:** CWE-327: Use of a Broken or Risky Cryptographic Algorithm<br>**OWASP Top 10:** M5: Insufficient Cryptography<br>**OWASP MASVS:** MSTG-CRYPTO-4 | com/alipay/sdk/encrypt/b.java<br>com/alipay/sdk/encrypt/f.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<br>**OWASP Top 10:** M5: Insufficient Cryptography<br>**OWASP MASVS:** MSTG-CRYPTO-3 | | |

| NO | ISSUE | SEVERITY | STANDARDS | FILES | OPTIONS |
|---|---|---|---|---|---|
| 10 | 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/batch/android/b/a.java<br>com/batch/android/i/a.java | |

Showing 1 to 10 of 19 entries

Previous 1 2 Next

### SHARED LIBRARY BINARY ANALYSIS

No Shared Objects found.

Search:

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

Showing 0 to 0 of 0 entries

Previous Next

### NIAP ANALYSIS v1.3

Search:

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| No data available in table | | | | |

Showing 0 to 0 of 0 entries

Previous Next

## FILE ANALYSIS

Search:

| NO | ISSUE | FILES |
|---|---|---|
| 1 | Hardcoded Keystore found. | com/google/api/client/googleapis/google.jks<br>res/raw/keystore_whoosh.bks |

Showing 1 to 1 of 1 entries

Previous 1 Next

## FIREBASE DATABASE ANALYSIS

Search:

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| App talks to a Firebase database | info | The app talks to Firebase database at https://api-project-604915498613.firebaseio.com |
| Firebase Remote Config disabled | secure | Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/604915498613/namespaces/firebase:fetch?key=AIzaSyCD8V9FaNvRD0T1KSUU7QR00MJYrk7K19o. This is indicated by the response: {'state': 'NO_TEMPLATE'} |

Showing 1 to 2 of 2 entries

Previous 1 Next

## MALWARE LOOKUP

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

## APKiD ANALYSIS

Search:

| DEX | DETECTIONS |
| --- | --- |
| classes.dex | |

Search:

| FINDINGS | DETAILS |
| --- | --- |
| Anti-VM Code | Build.FINGERPRINT check<br>Build.MODEL check<br>Build.MANUFACTURER check<br>Build.PRODUCT check<br>Build.HARDWARE check<br>Build.BOARD check<br>possible Build.SERIAL check<br>Build.TAGS check<br>device ID check<br>subscriber ID check<br>ro.product.device check<br>ro.kernel.qemu check<br>emulator file check<br>possible VM check |
| Compiler | r8 |

Showing 1 to 2 of 2 entries

Previous 1 Next

| DEX | DETECTIONS |
| --- | --- |
| classes2.dex | Search: |

| FINDINGS | DETAILS |
| --- | --- |
| Compiler | r8 without marker (suspicious) |

Showing 1 to 1 of 1 entries

Previous 1 Next

| DEX | DETECTIONS |
| --- | --- |
| classes3.dex | Search: |

| FINDINGS | DETAILS |
| --- | --- |
| Compiler | r8 without marker (suspicious) |

Showing 1 to 1 of 1 entries

Previous 1 Next

| DEX | DETECTIONS |
| --- | --- |
| classes4.dex | Search: |

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

Showing 1 to 3 of 3 entries

Previous 1 Next

| DEX | DETECTIONS |
|---|---|
| classes5.dex | Search: |

| FINDINGS | DETAILS |
|---|---|
| Anti-VM Code | Build.MANUFACTURER check<br>subscriber ID check |
| Compiler | r8 without marker (suspicious) |

Showing 1 to 2 of 2 entries

Previous 1 Next

Showing 1 to 5 of 5 entries

Previous 1 Next

## BEHAVIOUR ANALYSIS

Search:

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00001 | Initialize bitmap object and compress data (e.g. JPEG) into bitmap object | camera | group/flowbird/transit/utils/CompressImage.java |
| 00004 | Get filename and put it to JSON object | file collection | com/alipay/security/mobile/module/b/b.java<br>group/flowbird/mobile/feedback/sdk/client/data/FileAttachment.java |
| 00005 | Get absolute path of file and put it to JSON object | file | com/alipay/security/mobile/module/d/b.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00011 | Query data from URI (SMS, CALLLOGS) | sms calllog collection | com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java |
| 00012 | Read data and put it into a buffer stream | file | com/batch/android/n/a.java<br>group/flowbird/mpp/translation/TranslationService.java<br>group/flowbird/mpp/utils/Base64.java |
| 00013 | Read file and put it into a stream | file | |
| 00014 | Read file into a stream and put it into a JSON object | file | com/alipay/security/mobile/module/b/b.java<br>group/flowbird/mobile/feedback/sdk/client/data/FileAttachment.java |
| 00016 | Get location info of the device and put it to JSON object | location collection | group/flowbird/mobile/feedback/sdk/client/data/report/Report.java |
| 00022 | Open a file from given absolute path of the file | file | |
| 00023 | Start another application from current application | reflection control | com/samsung/android/sdk/samsungpay/v2/SamsungPay.java<br>com/samsung/android/sdk/samsungpay/v2/SamsungPayBase.java<br>group/flowbird/mpp/utils/UiUtils.java |

Showing 1 to 10 of 53 entries

Previous 1 2 3 4 5 6 Next

## ABUSED PERMISSIONS

**Top Malware Permissions** **12**/25

android.permission.INTERNET,
android.permission.ACCESS_NETWORK_STATE,
android.permission.ACCESS_COARSE_LOCATION,
android.permission.ACCESS_FINE_LOCATION,
android.permission.VIBRATE, android.permission.WAKE_LOCK,
android.permission.RECEIVE_BOOT_COMPLETED,

**Other Common Permissions** **4**/44

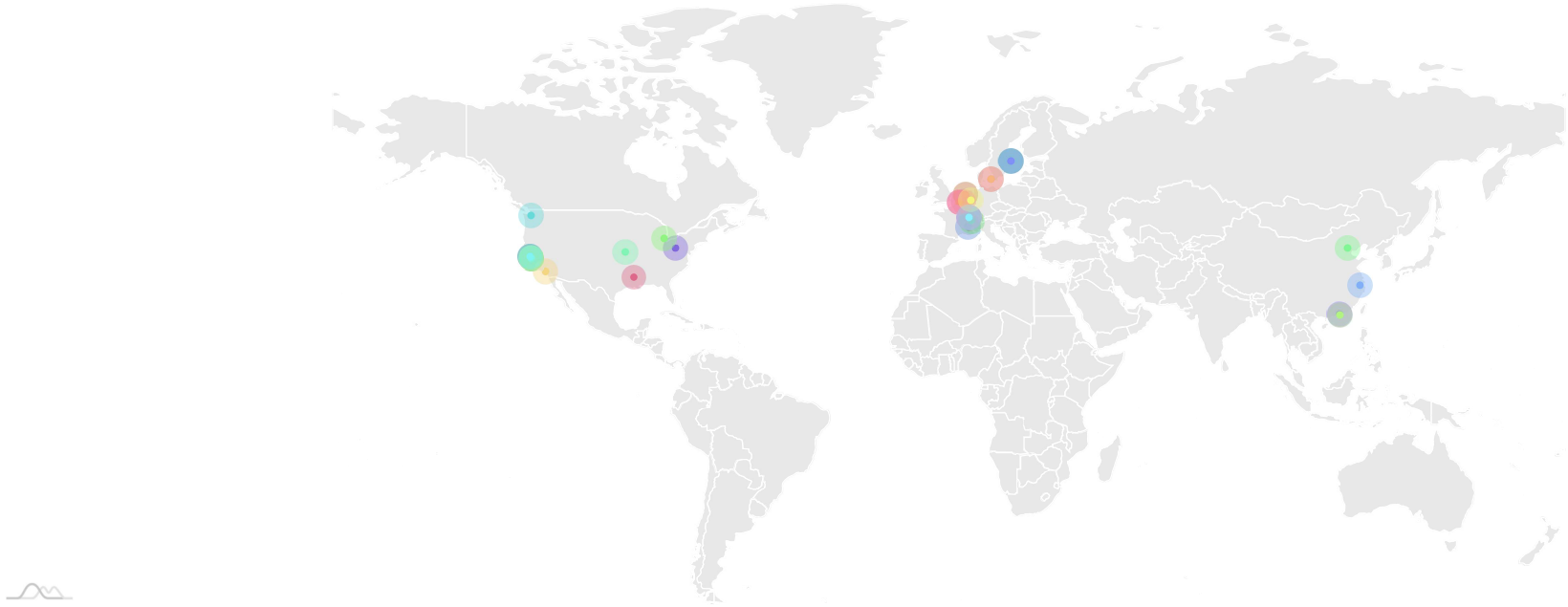
com.google.android.c2dm.permission.RECEIVE,
android.permission.FOREGROUND_SERVICE,
com.google.android.gms.permission.AD_ID,
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

android.permission.WRITE_EXTERNAL_STORAGE,
android.permission.READ_EXTERNAL_STORAGE,
android.permission.CAMERA,
android.permission.SYSTEM_ALERT_WINDOW,
android.permission.ACCESS_WIFI_STATE

---

**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 |
| --- | --- |
| long.open.weixin.qq.com | **IP:** 109.244.216.15<br>**Country:** China<br>**Region:** Beijing<br>**City:** Beijing |
| m.alipay.com | **IP:** 110.75.129.2<br>**Country:** China<br>**Region:** Zhejiang<br>**City:** Hangzhou |
| mobilegw.alipay.com | **IP:** 205.204.122.81<br>**Country:** Hong Kong<br>**Region:** Hong Kong<br>**City:** Hong Kong |
| mobilegw.alipaydev.com | **IP:** 47.235.21.32<br>**Country:** Hong Kong<br>**Region:** Hong Kong<br>**City:** Hong Kong |
| open.weixin.qq.com | **IP:** 203.205.232.110<br>**Country:** China<br>**Region:** Guangdong<br>**City:** Shenzhen |

Showing 1 to 5 of 5 entries

Previous 1 Next

## DOMAIN MALWARE CHECK

Search:

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| api-america.whooshstore.com | ok | No Geolocation information available. |
| api-europe.whooshstore.com | ok | **IP:** 104.18.8.76<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| api-project-604915498613.firebaseio.com | ok | **IP:** 35.190.39.113<br>**Country:** United States of America<br>**Region:** Missouri<br>**City:** Kansas City<br>**Latitude:** 39.099731<br>**Longitude:** -94.578568<br>**View:** Google Map |
| api.whooshstore.com | ok | **IP:** 104.18.8.76<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| batch.com | ok | **IP:** 76.76.21.21<br>**Country:** United States of America<br>**Region:** California<br>**City:** Walnut<br>**Latitude:** 34.015400<br>**Longitude:** -117.858223<br>**View:** Google Map |
| betalap.flowbirdapp.com | ok | **IP:** 185.149.62.25<br>**Country:** France<br>**Region:** Bourgogne-Franche-Comte<br>**City:** Besancon<br>**Latitude:** 47.248779<br>**Longitude:** 6.018150<br>**View:** Google Map |
| doc.batch.com | ok | No Geolocation information available. |
| docs.google.com | ok | **IP:** 142.250.74.78<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| drws.batch.com | ok | **IP:** 87.98.137.78<br>**Country:** France<br>**Region:** Hauts-de-France<br>**City:** Roubaix<br>**Latitude:** 50.694210<br>**Longitude:** 3.174560<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| duncan.imageenforcement.com | ok | **IP:** 2.23.172.155<br>**Country:** Denmark<br>**Region:** Hovedstaden<br>**City:** Ballerup<br>**Latitude:** 55.731651<br>**Longitude:** 12.363280<br>**View:** Google Map |

Showing 1 to 10 of 50 entries

Previous 1 2 3 4 5 Next

## URLS

Search:

| URL | FILE |
|---|---|
| data:image | com/bumptech/glide/load/model/DataUrlLoader.java |
| http://docs.google.com/gview?embedded=true&url= | group/flowbird/mpp/activities/SimpleWebViewActivity.java |
| http://docs.google.com/gview?embedded=true&url= | group/flowbird/mpp/activities/legal/AcceptAbstractActivity.java |
| http://localhost/ | retrofit2/Response.java |
| http://mobilegw.stable.alipay.net/mgw.htm<br>http://mobilegw.aaa.alipay.net/mgw.htm<br>http://mobilegw-1-64.test.alipay.net/mgw.htm<br>https://mobilegw.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://parkeon.com/car' | group/flowbird/mpp/model/customer/Car.java |

| URL | FILE |
|---|---|
| http://parkeon.com/order' | group/flowbird/mpp/parcers/OrderTransactionsErrorTypeParser.java |
| http://parkeon.com/order'<br>http://parkeon.com/fineresponse' | group/flowbird/mpp/parcers/FineResponseParser.java |
| http://parkeon.com/order'<br>http://parkeon.com/parkingticketorder' | group/flowbird/mpp/initializers/OrderLongTermTicketInitializer.java |
| http://parkeon.com/order'<br>http://parkeon.com/parkingticketorder' | group/flowbird/mpp/utils/StartStopOrderUtils.java |

Showing 1 to 10 of 59 entries

Previous 1 2 3 4 5 6 Next

## EMAILS

Search:

| EMAIL | FILE |
|---|---|
| betalap.stockholm@flowbird.se | Android String Resource |
| emailnotrequired@mail.com | group/flowbird/mpp/model/card/AbstractPaymentProvider.java |
| ext-cgras@parkeon.com | group/flowbird/mpp/model/card/SimplePayProvider.java |
| jdoe@parkeon.com | group/flowbird/mpp/utils/InitUtils.java |

Showing 1 to 4 of 4 entries

Previous 1 Next

## TRACKERS

Search:

| TRACKER NAME | CATEGORIES | URL |
|---|---|---|
| Batch | Profiling, Analytics | https://reports.exodus-privacy.eu.org/trackers/23 |
| Facebook Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/66 |
| Facebook Login | Identification | https://reports.exodus-privacy.eu.org/trackers/67 |
| Facebook Share | | https://reports.exodus-privacy.eu.org/trackers/70 |
| Google Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/48 |
| 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 |

Showing 1 to 8 of 8 entries

Previous 1 Next

## POSSIBLE HARDCODED SECRETS

▶ Show all **195** secrets

## STRINGS

**From APK Resource**

▶ Show all **14427** strings

**From Code**

▶ Show all **57644** strings

**From Shared Objects**

## ACTIVITIES

▶ Show all **53** activities

## SERVICES

▼ Showing all **23** services

se.stockholm.betalap.reimpl.webservices.request.RequestService
com.google.android.gms.analytics.AnalyticsService
group.flowbird.mpp.translation.TranslationService
com.google.firebase.components.ComponentDiscoveryService
group.flowbird.mobile.feedback.sdk.reporting.job.SubmitReportService
group.flowbird.mobile.feedback.sdk.reporting.legacy.SubmitReportLegacyService
com.google.android.gms.auth.api.signin.RevocationBoundService
com.google.firebase.messaging.FirebaseMessagingService
com.google.android.gms.tagmanager.TagManagerService
com.google.android.gms.measurement.AppMeasurementService
com.google.android.gms.measurement.AppMeasurementJobService
com.batch.android.BatchActionService
com.batch.android.BatchPushService
com.batch.android.BatchPushJobService
com.batch.android.BatchDisplayReceiptJobService
com.batch.android.eventdispatcher.DispatcherDiscoveryService
com.batch.android.push.PushRegistrationDiscoveryService

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

## RECEIVERS

▼ Showing all **18** receivers

group.flowbird.mpp.widget.FlowbirdWidget
com.google.android.gms.analytics.AnalyticsReceiver
com.google.android.gms.analytics.CampaignTrackingReceiver
com.batch.android.BatchPushMessageReceiver
com.google.firebase.iid.FirebaseInstanceIdReceiver
com.google.android.gms.measurement.AppMeasurementReceiver
com.facebook.CurrentAccessTokenExpirationBroadcastReceiver
com.facebook.AuthenticationTokenManager$CurrentAuthenticationTokenChangedBroadcastReceiver
com.batch.android.BatchPushMessageDismissReceiver
androidx.work.impl.utils.ForceStopRunnable$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.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver

## PROVIDERS

▼ Showing all **4** providers

androidx.core.content.FileProvider
com.google.firebase.provider.FirebaseInitProvider
com.facebook.internal.FacebookInitProvider
androidx.startup.InitializationProvider

### LIBRARIES

▼ Showing all **3** libraries
org.apache.http.legacy
androidx.window.extensions
androidx.window.sidecar

### SBOM

▼ Showing all **77** Versioned Packages
androidx.activity:activity-ktx@1.6.0
androidx.activity:activity@1.6.0
androidx.annotation:annotation-experimental@1.3.0
androidx.appcompat:appcompat-resources@1.6.1
androidx.appcompat:appcompat@1.6.1
androidx.arch.core:core-runtime@2.1.0
androidx.asynclayoutinflater:asynclayoutinflater@1.0.0
androidx.browser:browser@1.0.0
androidx.cardview:cardview@1.0.0
androidx.coordinatorlayout:coordinatorlayout@1.1.0
androidx.core:core-ktx@1.9.0
androidx.core:core@1.9.0
androidx.cursoradapter:cursoradapter@1.0.0
androidx.customview:customview@1.1.0
androidx.databinding:viewbinding@7.4.2
androidx.datastore:datastore-preferences@1.0.0-alpha06
androidx.datastore:datastore@1.0.0-alpha06
androidx.documentfile:documentfile@1.0.0
androidx.drawerlayout:drawerlayout@1.1.1

androidx.dynamicanimation:dynamicanimation@1.0.0
androidx.emoji2:emoji2-views-helper@1.2.0
androidx.emoji2:emoji2@1.2.0
androidx.exifinterface:exifinterface@1.2.0
androidx.fragment:fragment-ktx@1.5.1
androidx.fragment:fragment@1.5.1
androidx.interpolator:interpolator@1.0.0
androidx.legacy:legacy-support-core-ui@1.0.0
androidx.legacy:legacy-support-core-utils@1.0.0
androidx.legacy:legacy-support-v4@1.0.0
androidx.lifecycle:lifecycle-livedata-core-ktx@2.5.1
androidx.lifecycle:lifecycle-livedata-core@2.5.1
androidx.lifecycle:lifecycle-livedata-ktx@2.5.1
androidx.lifecycle:lifecycle-livedata@2.5.1
androidx.lifecycle:lifecycle-process@2.4.1
androidx.lifecycle:lifecycle-runtime-ktx@2.5.1
androidx.lifecycle:lifecycle-runtime@2.5.1
androidx.lifecycle:lifecycle-service@2.1.0
androidx.lifecycle:lifecycle-viewmodel-ktx@2.5.1
androidx.lifecycle:lifecycle-viewmodel-savedstate@2.5.1
androidx.lifecycle:lifecycle-viewmodel@2.5.1
androidx.loader:loader@1.0.0
androidx.localbroadcastmanager:localbroadcastmanager@1.0.0
androidx.media:media@1.0.0
androidx.paging:paging-runtime-ktx@2.1.2
androidx.paging:paging-runtime@2.1.2
androidx.preference:preference-ktx@1.2.0
androidx.preference:preference@1.2.0
androidx.print:print@1.0.0
androidx.recyclerview:recyclerview@1.1.0
androidx.room:room-ktx@2.4.3
androidx.room:room-runtime@2.4.3
androidx.room:room-rxjava2@2.4.3
androidx.savedstate:savedstate-ktx@1.2.0
androidx.savedstate:savedstate@1.2.0
androidx.slidingpanelayout:slidingpanelayout@1.2.0
androidx.sqlite:sqlite-framework@2.2.0

androidx.sqlite:sqlite@2.2.0
androidx.startup:startup-runtime@1.1.1
androidx.swiperefreshlayout:swiperefreshlayout@1.1.0
androidx.tracing:tracing@1.0.0
androidx.transition:transition@1.4.1
androidx.vectordrawable:vectordrawable-animated@1.1.0
androidx.vectordrawable:vectordrawable@1.1.0
androidx.versionedparcelable:versionedparcelable@1.1.1
androidx.viewpager2:viewpager2@1.0.0
androidx.viewpager:viewpager@1.0.0
androidx.window:window@1.0.0
androidx.work:work-runtime-ktx@2.7.1
androidx.work:work-runtime@2.7.1
com.google.android.material:material@1.6.1
com.google.dagger:dagger-android-support@2.35.1
com.google.dagger:dagger-android@2.35.1
com.google.dagger:dagger-lint-aar@2.35.1
com.google.dagger:dagger@2.35.1
org.jetbrains.kotlinx:kotlinx-coroutines-android@1.6.4
org.jetbrains.kotlinx:kotlinx-coroutines-core@1.6.4
org.jetbrains.kotlinx:kotlinx-coroutines-play-services@1.6.4

▶ Show all **136** Packages

## FILES

▶ Show all **4630** files