MOBSF

ANDROID STATIC ANALYSIS REPORT

mSpy Installer (1.2.0)

File Name:	bt_installer.apk
Package Name:	update.service.android.installer
Scan Date:	Aug. 10, 2024, 7:04 p.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	15	3	1	1

FILE INFORMATION

File Name: bt_installer.apk
Size: 12.78MB
MD5: 9d21e42afdb8db38a700255fa1831e0f
SHA1: 66fd0a6ddb84654f2939b84afbd9acc61d46ae9c
SHA256: 2d17b536e34d393d3454a9c170717ca0070784cded06eaa748df70bbf35e68fd

APP INFORMATION

App Name: mSpy Installer
Package Name: update.service.android.installer
Main Activity: update.service.core.ui.main.MainActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 1.2.0

Android Version Code: 104

APP COMPONENTS

Activities: 8
Services: 12
Receivers: 13
Providers: 3
Exported Activities: 1
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=inst, OU=inst, O=inst, L=inst, ST=inst, C=inst
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-10-26 17:12:12+00:00
Valid To: 2048-10-19 17:12:12+00:00
Issuer: CN=inst, OU=inst, O=inst, L=inst, ST=inst, C=inst
Serial Number: 0x1
Hash Algorithm: sha256
md5: 3de4f32396f1e11918f063f9daf70a08
sha1: fe821a533bdc31822d9eb5f98243eb16917c8ee7
sha256: e75f60c12f180cd11855f5a3b0d3cfa5432b03986a55c4bfcd608212a642cacb
sha512: d56e1916c0e3d20e660afc18ae99ba6f183719d7853dbdb0f0b4b26de00f6bc97194303c2d6d9aeb9a8c1e8db82e92c33e0f58218ab97b3bf782d0ea6f29be99
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: ba36a000f697cceec56b2d318b18a4ba1661d27a608a2fcf31a183dd873858b2
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
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.READ_PRIVILEGED_PHONE_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
update.service.android.installer.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
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.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.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
SIM operator check
network operator name check
device ID check
ro.kernel.qemu check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes3.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.PRODUCT check Build.HARDWARE check Build.TAGS check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

FILE	DETAILS
classes4.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.PRODUCT check Build.HARDWARE check Build.BOARD check Build.TAGS check network operator name check possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

FILE	DETAILS
classes5.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check Build.BOARD check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.crowdin.platform.auth.AuthActivity	Schemes: crowdintest://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | 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.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **6** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched 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] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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 (com.crowdin.platform.auth.AuthActivity) 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
4	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.
5	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.
6	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.
7	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.

CODE ANALYSIS

HIGH: 0 | WARNING: 7 | INFO: 3 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				by/kirich1409/viewbindingdelegate/LifecycleViewBindingProperty.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/amplitude/api/AmplitudeClient.java com/amplitude/api/AmplitudeLog.java com/amplitude/api/DatabaseHelper.java com/appsflyer/AFLogger.java com/appsflyer/internal/AFa1cSDK.java com/appsflyer/internal/AFb1kSDK.java com/appsflyer/internal/AFc1iSDK.java com/appsflyer/internal/AFd1aSDK.java com/appsflyer/internal/AFd1bSDK.java com/appsflyer/internal/AFd1dSDK.java com/appsflyer/internal/AFd1fSDK.java com/appsflyer/internal/AFd1kSDK.java com/appsflyer/internal/AFe1dSDK.java com/appsflyer/internal/AFe1pSDK.java com/appsflyer/internal/AFe1qSDK.java com/appsflyer/internal/AFe1rSDK.java com/appsflyer/internal/AFe1tSDK.java com/appsflyer/internal/AFe1ySDK.java com/appsflyer/internal/AFe1zSDK.java com/appsflyer/internal/AFf1ySDK.java com/appsflyer/internal/AFg1jSDK.java com/crowdin/platform/Crowdin.java com/crowdin/platform/CrowdinConfig.java com/crowdin/platform/ShakeDetectorManager.java com/crowdin/platform/auth/AuthActivity.java com/crowdin/platform/data/DataManager.java com/crowdin/platform/data/remote/CrowdingRe

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/crowdin/platform/data/remote/CrowdingRepository$getManifest$1.java com/crowdin/platform/data/remote/CrowdingRepository.java com/crowdin/platform/data/remote/DistributionInfoManager.java com/crowdin/platform/data/remote/MappingRepository.java com/crowdin/platform/data/remote/StringDataRemoteRepository.java com/crowdin/platform/data/remote/TranslationDataRepository$getFiles$1.java com/crowdin/platform/data/remote/TranslationDataRepository.java com/crowdin/platform/realtimeupdate/EchoWebSocketListener.java com/crowdin/platform/realtimeupdate/RealTimeUpdateManager.java com/crowdin/platform/screenshot/ScreenshotService.java com/crowdin/platform/util/ExtensionsKt.java com/journeyapps/barcodescanner/CameraPreview.java com/journeyapps/barcodescanner/CaptureManager.java com/journeyapps/barcodescanner/DecoderThread.java com/journeyapps/barcodescanner/camera/AutoFocusManager.java com/journeyapps/barcodescanner/camera/CameraConfigurationUtils.java com/journeyapps/barcodescanner/camera/CameraInstance.java com/journeyapps/barcodescanner/camera/CameraManager.java com/journeyapps/barcodescanner/camera/CenterCropStrategy.java com/journeyapps/barcodescanner/camera/FitCenterStrategy.java com/journeyapps/barcodescanner/camera/LegacyPreviewScalingStrategy.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/journeyapps/barcodescanner/camera/PreviewScalingStrategy.java com/qonversion/android/sdk/Qonversion.java com/qonversion/android/sdk/QonversionConfig.java com/qonversion/android/sdk/internal/logger/ExceptionHandler.java com/qonversion/android/sdk/internal/logger/QExceptionManager$sendCrashReportsInBackground$1$1$1$2.java com/qonversion/android/sdk/internal/logger/QExceptionManager.java dagger/android/AndroidInjection.java timber/log/Timber.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/amplitude/api/AmplitudeClient.java com/crowdin/platform/data/model/AuthConfig.java com/crowdin/platform/data/model/RefreshToken.java com/crowdin/platform/data/model/StringData.java com/crowdin/platform/data/model/TokenRequest.java com/qonversion/android/sdk/automations/internal/macros/ScreenProcessor.java com/qonversion/android/sdk/automations/mvp/ScreenFragment.java com/qonversion/android/sdk/dto/properties/QUserProperty.java com/qonversion/android/sdk/internal/Constants.java com/qonversion/android/sdk/internal/api/ApiHeadersProvider.java com/qonversion/android/sdk/internal/dto/SendPropertiesResult.java com/qonversion/android/sdk/internal/dto/config/PrimaryConfig.java com/qonversion/android/sdk/internal/dto/request/CrashRequest.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/qonversion/android/sdk/internal/dto/request/DataUserPropertyRequestData.java com/qonversion/android/sdk/internal/extractor/SkuDetailsTokenExtractor.java com/qonversion/android/sdk/internal/storage/LaunchResultCacheWrapperKt.java com/qonversion/android/sdk/internal/storage/PurchasesCache.java com/qonversion/android/sdk/internal/storage/TokenStorage.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java update/service/core/BuildConfig.java update/service/core/initializers/AmplitudeInitializer.java update/service/core/initializers/CrowdinInitializers.java
3	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	com/appsflyer/internal/AFa1ySDK.java com/qonversion/android/sdk/internal/IncrementalDelayCalculator.java com/qonversion/android/sdk/internal/di/module/ManagersModule.java
4	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	update/service/data/remote/repository/RemoteRepositoryImpl.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amplitude/api/PinnedAmplitudeClient.java com/crowdin/platform/data/remote/CrowdinRetrofitService.java com/qonversion/android/sdk/internal/di/module/NetworkModule.java update/service/data/di/DataModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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/neovisionaries/ws/client/HandshakeReader.java
7	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/amplitude/api/DatabaseHelper.java
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/crowdin/platform/CrowdinPreferences.java com/crowdin/platform/data/local/SharedPrefLocalRepository.java
9	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/amplitude/eventexplorer/EventExplorerInfoActivity.java
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/journeyapps/barcodescanner/CaptureManager.java
11	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/NetworkCache.java update/service/data/util/CryptUtilImpl.java update/service/data/util/SecurityUtilImpl.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/24	android.permission.SYSTEM_ALERT_WINDOW, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.CAMERA
Other Common Permissions	5/45	android.permission.REQUEST_INSTALL_PACKAGES, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE

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
sattr.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
api.qonversion.io	ok	**IP:** 104.22.7.135 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api2.amplitude.com	ok	**IP:** 35.80.156.95 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
regionconfig.eu.amplitude.com	ok	**IP:** 3.165.206.121 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sapp.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
documentation.qonversion.io	ok	**IP:** 104.22.7.135 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
mobile-gw.thd.cc	ok	**IP:** 104.26.4.141 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sdk-logs.qonversion.io	ok	**IP:** 104.22.6.135 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
regionconfig.amplitude.com	ok	**IP:** 3.165.206.9 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sviap.s	ok	No Geolocation information available.
svalidate.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
journeyapps.com	ok	**IP:** 3.165.206.71 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sars.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
distributions.crowdin.net	ok	**IP:** 3.165.206.13 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.eu.amplitude.com	ok	**IP:** 52.29.129.64 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.crowdin.com	ok	**IP:** 18.204.137.91 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
accounts.crowdin.com	ok	**IP:** 54.209.15.179 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sinapps.s	ok	No Geolocation information available.

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/125
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_api_key" : "AIzaSyBCBCs0EKod5eyoJIG9jJlT3pT-uVIFYGQ"
"google_crash_reporting_api_key" : "AIzaSyBCBCs0EKod5eyoJIG9jJlT3pT-uVIFYGQ"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

POSSIBLE SECRETS
yXdkchwXd7KBwiPBiUydLTG3hsBC8U5EW7urXPkQrKc=
rY9DNDEvlJE2YV76YVSJLP4cBUy/u1xcBXUcMxb1h8o=
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
yqGfvaGOT1fOScq8M0g9vywM6jvcTWdjxf27npfqtn0=
NYpdto3gBV8HiZtFXi3NN2dSfPyfe2T+8tUnAUjRH8A=
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
Kmv9uscZLQkY9DcwgermeDphrIGnHnQJYdRAudw6Thg=
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
Md0NasjzX5Dv6RV9gbRrdbbQw799E9EBpEgmAwiNqi/RiG7V51y0yTZI5hLTRiUF
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
lJSjzU0WHYWPVV9sbEMt+ajOnNQwNtdM0PEq4BwIHEoSxWMr7EQ/IWk1GxHpKsqd
Mx1UeFqV1fjeaaqnMs31Cpnz92KBTGXH/Fg2ftteXVEThFuI1yrtq0+LdsZyqokl
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
BEk7ZnZgUEtCcnEVmnqrsudDaU91B7wv3jOIcYFOdixfCZNd4CeUtXw9CNec1bEk

POSSIBLE SECRETS
NSYe0Ak7CUXd9zFZA3bczJ8pTgBK/kfUu9ICpHR+lQrTNc8+V7Owo49e2WIp0407
Yj2yffKjPUt0Mx1uRMPIz4KPVLEfX/KYQGpvpNjX0eY=
470fa2b4ae81cd56ecbcda9735803434cec591fa
ae2044fb577e65ee8bb576ca48a2f06e
B3EEABB8EE11C2BE770B684D95219ECB
bwYfemyqKvs+5mX5RaQoUxmdyIG97sQWktW0fw649v7l/u+oM9fVxJ1I47AdFZo9
ue4Q/YADEXoviiBHZurTF9IPPlfQKRVJdzRZ56oggWM=
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943 10b30090603550406130255533113301106035504081 30a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b300906035504061302555331133011060355040813 0a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100 19d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b

POSSIBLE SECRETS
Cm/m2hUfCdldkdMMT3yEm1sAGuFpKVfLQblDoR20XcK7ttTDkHIz3fwaKTv7az9S
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
c7c0e3677d615ffd6b795c948d3bb4d9
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
BZSpo1ki7Qq4VpNbKNY5xp3ObP5b46iKtLhMqj95i84Sl1pKZG1hW1hXSXh30EEu
0H2C2EeQe84lGZgr+dAw2Fmmx+KWvzkBWNdP/wQOLp8=
ZlhR2acRJ5DFhes+PG5pnG7AissVCA1YeE0si8KUOuk=
Rh7wPiyt0Q0zAefasWAQ/36LhULiVi3U1eCO9K34euxkll+3xBb3q2iaqyDuAy33
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
k9LiT4122PpqzUH6coaRvTZE6l9CWOGxr21WpJpkxjE=
wC9I8kYd+RKAHfQkBEAJYQw7avQUH+U9s6BQ/SJiEcKjDl2sT+FDEb6J3VYVY+ui

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
LbaQh8VAFWEQeupBiMdSh8EgMse5yKT8p6jkCYTG+aQ=
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
FIES3RTkQwHbrKX6yNHRLvjdTy/vAwaHt4NSjNSY8AdC8m3WKKtOY2UmKZKAKB0T
NK1iwlHEHCICBCLEvTy0TnuhgEeSXovnPs9zKPvVW8trSfaaB+/inefY+5AxSSUI

POSSIBLE SECRETS
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
6LxD9DBfXSlooSx7/LozL06rdHrjyh7Q8PNFejLJXxiRhvgA5vOTtEhIRp3pKXIi
5181942b9ebc31ce68dacb56c16fd79f
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
F3lRDxfW1sfbPaHnIYKQdnyja8qzB0dR
DVrAFpWxz2kcLonXDVqzAxxY5qZgb6+MyY8HJZUy9HF2czdhCSx5Lbv7dDVJMgy/
NOQ7v89FdlqbWITe5fQxaJU2MeOCrxMPjMVtpwyCEdc=
5c746f59f79156c6a8020e8

POSSIBLE SECRETS
pECbn1i7ArZz8HseR71ZVkvFfTp84DNv2haWC1WmGQudMO74UcIxEa2NyELtzZhK
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
fOkIRsWNRFrLLiTxAAtymkQwvThROsAenMGWOswUGPc=
2q9SJ42xLZKaCbpMEBENFcJEqDDES1vvcaask6iD3co=
FSkZmgTbP/gL1jHU7M+TcfgVpePk57vWMdHk6knGCa4=
kgLg33QaU762V6pmSw9NTYQDT3UN+SfZqKWL+LtHgczBAmljOlYdBxhmK655CLWm
BF4UgSmqTS0MLe4qitQi/hj1jIQ+0vLIJEn32u0TtZn0VL9j15ZHt04Do4ADy833
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
4FqMwpBmkecZ5KuntXganMUU8jtWDsP5C5fiOE4sCtY=
2LDOSJy2Fx9VBMC+bm+0OJly9nmnJoeXDwyJmbeZyYc=
WLzuG2U+Kkbg0oKQlrLQGRQCiSGGQTHe1FZJKw3vRH0=
LLuZlwuRYspGUGo7OZU51ciMYYFQ89K2r1TLDzvNq9k=
E20AdmxNj0iK7Vx72nHXXjWnsmv4FUkyxC/Oztwx6eZIzlENIrQYdkN17JfC0Q1q
QXllCfiT7SVSRUb0DD1a74y++UqnSLMKlPOXAn9FNLrl7qN9uprYrk5dswjj/dLi
Yw5N4XiXXiTiwJwrJ8hW/AfPIwRQ2KMfiYKb9xu8vYQ=

POSSIBLE SECRETS
6XqKWQ93+VsENz1XMuSK8tgooVS0F/+xtezkhSGK2kwZU9gOCstoEHJ4LdRwy+D0
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

SCAN LOGS

Timestamp	Event	Error
2024-08-10 19:04:28	Generating Hashes	OK
2024-08-10 19:04:28	Extracting APK	OK
2024-08-10 19:04:28	Unzipping	OK
2024-08-10 19:04:28	Getting Hardcoded Certificates/Keystores	OK
2024-08-10 19:04:30	Parsing AndroidManifest.xml	OK
2024-08-10 19:04:30	Parsing APK with androguard	OK

2024-08-10 19:04:31	Extracting Manifest Data	OK
2024-08-10 19:04:31	Performing Static Analysis on: mSpy Installer (update.service.android.installer)	OK
2024-08-10 19:04:31	Fetching Details from Play Store: update.service.android.installer	OK
2024-08-10 19:04:31	Manifest Analysis Started	OK
2024-08-10 19:04:31	Checking for Malware Permissions	OK
2024-08-10 19:04:31	Fetching icon path	OK
2024-08-10 19:04:32	Library Binary Analysis Started	OK
2024-08-10 19:04:32	Reading Code Signing Certificate	OK
2024-08-10 19:04:32	Running APKiD 2.1.5	OK
2024-08-10 19:04:36	Detecting Trackers	OK
2024-08-10 19:04:39	Decompiling APK to Java with jadx	OK

2024-08-10 19:05:13	Converting DEX to Smali	OK
2024-08-10 19:05:13	Code Analysis Started on - java_source	OK
2024-08-10 19:05:46	Android SAST Completed	OK
2024-08-10 19:05:46	Android API Analysis Started	OK
2024-08-10 19:05:54	Android Permission Mapping Started	OK
2024-08-10 19:06:16	Android Permission Mapping Completed	OK
2024-08-10 19:06:18	Finished Code Analysis, Email and URL Extraction	OK
2024-08-10 19:06:18	Extracting String data from APK	OK
2024-08-10 19:06:18	Extracting String data from Code	OK
2024-08-10 19:06:18	Extracting String values and entropies from Code	OK
2024-08-10 19:06:21	Performing Malware check on extracted domains	OK

2024-08-10 19:06:24	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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.