



ANDROID STATIC ANALYSIS REPORT



 BestHelp (8.6.7.532)

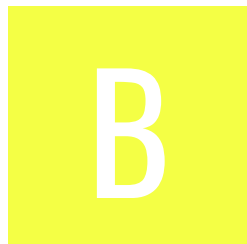
File Name: BestHelp - Psychological Help_8.6.7.532_Apkpure.xapk

Package Name: com.involtapp.psyans

Scan Date: Dec. 3, 2023, 10:02 p.m.






App Security Score: 40/100 (MEDIUM RISK)

Grade:



Trackers Detection: 2/428

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
8	17	2	2	2

FILE INFORMATION

File Name: BestHelp - Psychological Help_8.6.7.532_Apkpure.xapk

Size: 10.31MB

MD5: 3570b60deff72fe355b04398517ed248

SHA1: 6ee53f4b3457e053494af568045bedc216d3dc22

SHA256: a8b1facc7af50874822efd65c3b2c1916bfbee53176e7184d11f22fdf2b665f1

APP INFORMATION

App Name: BestHelp

Package Name: com.involtapp.psyans

Main Activity: com.involtapp.psyans.ui.activities.SplashActivity

Target SDK: 33

Min SDK: 21

Max SDK:

Android Version Name: 8.6.7.532

Android Version Code: 532

APP COMPONENTS

Activities: 44

Services: 15

Receivers: 14

Providers: 4

Exported Activities: 3

Exported Services: 3

Exported Receivers: 4

Exported Providers: 1

CERTIFICATE INFORMATION

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: 2017-10-13 13:20:48+00:00

Valid To: 2047-10-13 13:20:48+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0x3fa3d5c1fa7e7b04d7523e8481c12302dd70fd8c

Hash Algorithm: sha256

md5: 9284f8a793bc775e33ed334a310f40a1

sha1: aea6e79359cf436f427a8e29b5a1019d9738a7e0

sha256: 0b5b1d77845317a9b0423f4af8fb6545a67c1aec8e7bc474353919f8750f86cf

sha512: 04c4167baf368d5eed83092acc4dbdab45c77cb789e58d6784b42ad0055d6f04b2a545bde3275b245459a4d356387078bdb004c8e9a01aa8c64aa291ca3a839a

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 356b17c07ee20e30cae7225ebe90b235ae7e7d4639198e80c8a322fe65d9e67a

Found 1 unique certificates

≡ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.

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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.POST_NOTIFICATIONS	dangerous		Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
com.involtapp.psyans.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	Show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.android.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference



FILE	DETAILS
------	---------

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check Build.TAGS check
	Compiler	r8
classes2.dex	FINDINGS	DETAILS
	Anti Debug Code	Debug.isDebuggerConnected() check
	Anti-VM Code	Build.MANUFACTURER check
	Compiler	r8 without marker (suspicious)
classes3.dex	FINDINGS	DETAILS
	Compiler	r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.involtapp.psyans.ui.activities.SplashActivity	Schemes: https://, http://, psyans://, Hosts: psyans.page.link, splash,
com.involtapp.psyans.ui.activities.buyPremium.PremiumActiveSubscribe	Schemes: psyans://, Hosts: premium,
com.involtapp.psyans.ui.activities.ListHistoryActivity	Schemes: psyans://, Hosts: history,

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

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.

Q MANIFEST ANALYSIS

HIGH: 7 | WARNING: 6 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=21]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Broadcast Receiver (com.involtapp.psyans.util.InstallReceiver) is not Protected. [android:exported=true]	high	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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Activity (com.involtapp.psyans.ui.activities.buyPremium.PremiumActiveSubscribe) is not Protected. [android:exported=true]	high	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.involtapp.psyans.ui.activities.ListHistoryActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.involtapp.psyans.ui.activities.MainActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	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.
9	Content Provider (com.yandex.metrca.PreloadInfoContentProvider) is not Protected. [android:exported=true]	high	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.
10	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.

NO	ISSUE	SEVERITY	DESCRIPTION
11	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.
12	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.
13	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [android:exported=true]	high	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: 8 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a1/m0.java a3/a.java a3/d.java a3/j.java a8/h.java b7/b.java c0/c.java c3/e.java c3/f.java c3/k.java c3/l.java c3/n.java c3/o.java c7/f.java c7/p.java c7/q.java cb/d.java com/airbnb/lottie/LottieAnimationView.java com/bumptech/glide/b.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/h.java com/bumptech/glide/load/engine/i.java com/bumptech/glide/load/engine/j.java com/bumptech/glide/load/engine/v.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/c.java com/bumptech/glide/load/resource/bitmap/e.java com/bumptech/glide/load/resource/bitmap/e0.java com/bumptech/glide/load/resource/bitmap/p.java

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/bumptech/glide/load/resource/bitMap/t.java com/bumptech/glide/request/h.java com/involtapp/imageviewer/flingswipe/b.java com/involtapp/imageviewer/materialrangebar/RangeBar.java com/involtapp/psyans/a.java com/involtapp/psyans/ucrop/view/f.java com/involtapp/psyans/ui/activities/buyPremium/PremiumHelloOnboard.java com/involtapp/psyans/util/audioMessages/VisualAmplitudeSoundView.java com/yandex/metrica/gpllibrary/a.java com/yandex/metrica/impl/ob/C0688h2.java com/yandex/metrica/impl/ob/Nf.java com/yandex/metrica/impl/ob/R1.java com/yandex/metrica/impl/ob/T2.java com/yandex/metrica/impl/ob/Tf.java com/yandex/metrica/impl/ob/Uf.java d1/i.java d3/d.java g5/f.java g5/l.java g7/d.java h2/e.java i0/b.java ia/l2.java j3/a.java j7/l.java k0/a.java k2/a.java k4/f.java m2/d.java m2/e.java n0/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n6/e.java n6/g.java n9/o.java o0/a.java o2/b.java o2/j.java o2/l.java o8/e.java og/e.java p/d.java p0/a.java p0/c.java p2/c.java p2/e.java p6/a.java p6/b.java p6/e.java p6/h.java p6/j.java p8/b.java q1/a.java q1/c.java qa/b.java qb/e.java qc/b.java r0/b0.java r0/q.java r0/t.java r0/w.java r2/i.java r2/k.java r8/g.java r9/e.java ra/c.java s2/e.java s2/i.java s4/d.java s6/b0.java t0/a.java t1/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t2/a.java u1/a.java u2/c.java u2/d.java u2/f.java u2/s.java u2/t.java u6/b.java u6/i0.java u6/n0.java u6/t.java u6/w.java u7/a.java v0/k.java v5/k.java w0/d.java w2/m.java x0/a.java x6/a.java x7/a.java xc/a.java xc/p.java xg/a.java y5/a.java yc/l.java z/g.java
				z0/b.java z8/a.java c6/t0.java com/yandex/metrica/impl/ob/A8.java com/yandex/metrica/impl/ob/B8.java com/yandex/metrica/impl/ob/C0535b.java com/yandex/metrica/impl/ob/C0793l8.java com/yandex/metrica/impl/ob/C0818m8.java com/yandex/metrica/impl/ob/C0843n8.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/yandex/metrica/impl/ob/C0868o8.j FILES com/yandex/metrica/impl/ob/C0893p8.j ava com/yandex/metrica/impl/ob/C0917q8.j ava com/yandex/metrica/impl/ob/C0940r8.j ava com/yandex/metrica/impl/ob/C0964s8.j ava com/yandex/metrica/impl/ob/C0988t8.j ava com/yandex/metrica/impl/ob/C1012u8.j ava com/yandex/metrica/impl/ob/C1036v8.j ava com/yandex/metrica/impl/ob/C1060w8. java com/yandex/metrica/impl/ob/C1084x8.j ava com/yandex/metrica/impl/ob/C1108y8.j ava com/yandex/metrica/impl/ob/C1132z8.j ava com/yandex/metrica/impl/ob/C8.java com/yandex/metrica/impl/ob/D8.java com/yandex/metrica/impl/ob/E8.java com/yandex/metrica/impl/ob/F8.java com/yandex/metrica/impl/ob/G8.java com/yandex/metrica/impl/ob/H8.java com/yandex/metrica/impl/ob/I8.java com/yandex/metrica/impl/ob/J7.java com/yandex/metrica/impl/ob/J8.java com/yandex/metrica/impl/ob/K7.java com/yandex/metrica/impl/ob/K8.java com/yandex/metrica/impl/ob/L7.java com/yandex/metrica/impl/ob/L8.java com/yandex/metrica/impl/ob/M8.java com/yandex/metrica/impl/ob/N8.java com/yandex/metrica/impl/ob/O8.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/yandex/metrica/impl/ob/Q8.java com/yandex/metrica/impl/ob/R8.java com/yandex/metrica/impl/ob/S8.java
				com/yandex/metrica/impl/ob/T8.java com/yandex/metrica/impl/ob/U8.java com/yandex/metrica/impl/ob/V7.java com/yandex/metrica/impl/ob/V8.java com/yandex/metrica/impl/ob/W8.java com/yandex/metrica/impl/ob/X8.java
3	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	w0/c.java com/yandex/metrica/impl/ob/X1.java z8/q.java
4	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	fc/c.java n3/a.java p0/c.java qa/c.java r0/b0.java xc/g.java
5	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	a4/b.java com/yandex/metrica/impl/ob/H.java ka/z.java qa/b.java
6	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/yandex/metrica/impl/ob/Pl.java com/yandex/metrica/impl/ob/Tl.java e2/g.java s1/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	eg/z.java io/grpc/internal/c0.java io/grpc/internal/e0.java io/grpc/internal/y1.java j\$/util/concurrent/ThreadLocalRandom.j ava k3/c.java pd/i.java rf/a.java rf/b.java rg/d.java rg/h.java sf/a.java ud/e.java ud/h.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ng/f.java ng/g.java ng/l.java ng/m.java
9	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	fc/c.java n3/a.java x3/a.java xc/v.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/involtapp/psyans/ui/activities/AboutActivity.java com/involtapp/psyans/ui/activities/BanActivity.java com/involtapp/psyans/ui/activities/Disconnect.java com/involtapp/psyans/ui/activities/TechnicalSupport.java com/involtapp/psyans/ui/activities/VerificationPsychologist.java oc/r.java
11	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/bumptech/glide/load/engine/d.java com/bumptech/glide/load/engine/o.java com/bumptech/glide/load/engine/t.java com/yandex/metrica/impl/ob/C0715i4.java com/yandex/metrica/impl/ob/D4.java com/yandex/metrica/impl/ob/Lg.java com/yandex/metrica/impl/ob/Ln.java i1/d.java io/grpc/internal/l2.java ma/b.java n2/f.java w4/g.java
12	The file or SharedPreferences is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/involtapp/psyans/ui/activities/ListHistoryActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	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/involtapp/psyans/ui/activities/ChatActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
--------	----------------

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
--------	--------	-------------

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	IP: 142.251.33.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
gateway.appo.click	ok	No Geolocation information available.
gateway.appstat.io	ok	No Geolocation information available.
yandex.com	ok	IP: 77.88.55.80 Country: Russian Federation Region: Moskva City: Moscow Latitude: 55.752220 Longitude: 37.615559 View: Google Map
issuetracker.google.com	ok	IP: 172.217.13.206 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
psyans.ru	ok	IP: 185.194.107.168 Country: Russian Federation Region: Sankt-Peterburg City: Saint Petersburg Latitude: 59.894440 Longitude: 30.264170 View: Google Map
translate.yandex.ru	ok	IP: 213.180.204.193 Country: Russian Federation Region: Moskva City: Moscow Latitude: 55.752220 Longitude: 37.615559 View: Google Map
psyans.page.link	ok	IP: 172.217.13.161 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
developer.android.com	ok	IP: 172.217.13.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
startup.mobile.yandex.net	ok	IP: 213.180.204.244 Country: Russian Federation Region: Moskva City: Moscow Latitude: 55.752220 Longitude: 37.615559 View: Google Map
redirect.appmetrica.yandex.com	ok	IP: 93.158.134.207 Country: Russian Federation Region: Moskva City: Moscow Latitude: 55.752220 Longitude: 37.615559 View: Google Map
accounts.google.com	ok	IP: 142.251.41.77 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
psyans-42b52.firebaseio.com	ok	IP: 35.190.39.113 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
<code>https://psyans-42b52.firebaseio.com</code>	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
<code>this@pushmessaging.applicatio</code>	<code>com/involtapp/psyans/util/notifications/PushMessaging.java</code>
<code>psyanschat@gmail.com</code>	<code>com/involtapp/psyans/ui/activities/BanActivity.java</code>
<code>psyanschat@gmail.com</code>	<code>com/involtapp/psyans/ui/activities/TechnicalSupport.java</code>
<code>psyanschat@gmail.com</code>	<code>com/involtapp/psyans/ui/activities/VerificationPsychologist.java</code>
<code>psyanschat@gmail.com</code>	<code>com/involtapp/psyans/ui/activities/Disconnect.java</code>
<code>psyanschat@gmail.com</code>	<code>oc/r.java</code>

TRACKERS

TRACKER	CATEGORIES	URL
AppMetrica		https://reports.exodus-privacy.eu.org/trackers/140
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://psyans-42b52.firebaseio.com"
"google_api_key" : "AlzaSyBLm9AmlEN7cmFAGI_BDSxr0XTdBJrfIW4"
"google_crash_reporting_api_key" : "AlzaSyBLm9AmlEN7cmFAGI_BDSxr0XTdBJrfIW4"
"nameUser" : "Name"
"yandex_metrika_api_key" : "6316704e-a435-40f6-8ebf-1ff41c3074f7"
"nameUser" : "Name"
"block_user" : "□□□□"
"nameUser" : "□□"
"question_for_user" : "□□□□□"
"unlock_user" : "□□□□"

POSSIBLE SECRETS
"you_can_answer_questions_private_chat_or_ask_yours" : "□□□□□□□□□□□□□□□□□□□□□□"
"nameUser" : "■■■■"
"nameUser" : "Ім'я"
"nameUser" : "Navn"
"nameUser" : "Nom"
"nameUser" : "Nombre"
"nameUser" : "Nome"
"nameUser" : "Nome"
"nameUser" : "Имя"
"nameUser" : "Namn"
5181942b9ebc31ce68dacb56c16fd79f
01528cc0-dd34-494d-9218-24af1317e1ee
20799a27-fa80-4b36-b2db-0f8141f24180
4e610cd2-753f-4bfc-9b05-772ce8905c5e
e81b774368efd4ae9093e9e6b4376cf3

POSSIBLE SECRETS
6316704e-a435-40f6-8ebf-1ff41c3074f7
6444043acda4e584a59ecb74964a68c4
67bb016b-be40-4c08-a190-96a3f3b503d3
6c5f504e-8928-47b5-bfb5-73af8d8bf4b4
7d962ba4-a392-449a-a02d-6c5be5613928
258EAFa5-E914-47DA-95CA-C5AB0DC85B11
0e5e9c33-f8c3-4568-86c5-2e4f57523f72
e4250327-8d3c-4d35-b9e8-3c1720a64b91
ae2044fb577e65ee8bb576ca48a2f06e
a72bf6f57701ed3c2b8ed570054febbff4e58c12

Report Generated by - MobSF v3.7.9 Beta

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.

© 2023 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).