

ANDROID STATIC ANALYSIS REPORT



₩ WiFi Service (1.0)

File Name: eva.apk

Package Name: com.ujiqeaqk.ottmrjzn

Scan Date: Aug. 10, 2024, 6:45 p.m.

App Security Score:

48/100 (MEDIUM RISK)

Grade:

В

♣ FINDINGS SEVERITY

∄ HIGH	▲ MEDIUM	i INFO	✓ SECURE	® HOTSPOT
2	19	1	1	1



File Name: eva.apk

Size: 3.42MB

MD5: fb07b7b61c9c01249c4b71d834e27451

SHA1: f3d1b632419416c1f6e108f9b483cb7d114de168

SHA256: d4e366b980f8c1eb18e0c5618031b9fb64228b9b3d3d5251d2cbeb58d07f3cf3

i APP INFORMATION

App Name: WiFi Service

Package Name: com.ujiqeaqk.ottmrjzn

Main Activity: com.wvwnlhuj.mitcbrrn.tokftwpyTL

Target SDK: 28 Min SDK: 19 Max SDK:

Android Version Name: 1.0
Android Version Code: 1

EXE APP COMPONENTS

Activities: 20 Services: 12 Receivers: 12 Providers: 1

Exported Activities: 3
Exported Services: 4
Exported Receivers: 5
Exported Providers: 0

***** CERTIFICATE INFORMATION

Binary is signed v1 signature: True v2 signature: True v3 signature: True v4 signature: False

X.509 Subject: C=HR, ST=SJDUZRBPes, L=HOKUInMAQU, O=vBxpqCJQiN, OU=KjvuwkCRNY, CN=paszqnvrdv.yyi

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2024-06-17 19:19:40+00:00 Valid To: 2051-11-03 19:19:40+00:00

Issuer: C=HR, ST=SJDUZRBPes, L=HOKUInMAQU, O=vBxpqCJQiN, OU=KjvuwkCRNY, CN=paszqnvrdv.yyi

Serial Number: 0x51a2aa2f Hash Algorithm: sha256

md5: 5db88f50e7a77e645465aa3a480794b0

sha1: 20c2e214704bf68dd2642ee94e60ede4b6fe661d

sha256: 122233077c7cc1605aef4231f5594a03d31edd3b0b3783abd374b9ba199d0a61

sha512: ad62ff66922042522b82fecd1b5fcee2bc4c44db3ddc70df9d4647762248adcb25b3112abad0f60cc6ea91de8c177e9e70ab5db0707275efcf076cb37b6f6faa

PublicKey Algorithm: rsa

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.wvwnlhuj.mitcbrrn.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.ANSWER_PHONE_CALLS	dangerous	permits an app to answer incoming phone calls.	Allows the app to answer an incoming phone call.
android.permission.PROCESS_OUTGOING_CALLS	dangerous	intercept outgoing calls	Allows application to process outgoing calls and change the number to be dialled. Malicious applications may monitor, redirect or prevent outgoing calls.
android.permission.READ_LOGS	dangerous	read sensitive log data	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.SDCARD_WRITE	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.

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.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.BIND_DEVICE_ADMIN	signature	interact with device admin	Allows the holder to send intents to a device administrator. Should never be needed for common applications.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.ACCESS_SUPERUSER	unknown	Unknown permission	Unknown permission from android reference
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.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.USES_POLICY_WIPE_DATA	unknown	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.WRITE_SECURE_SETTINGS	SignatureOrSystem	modify secure system settings	Allows an application to modify the system's secure settings data. Not for use by common applications.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.GET_PACKAGE_SIZE	normal	measure application storage space	Allows an application to find out the space used by any package.
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.
android.permission.BATTERY_STATS	signature	modify battery statistics	Allows the modification of collected battery statistics. Not for use by common applications.
android.permission.CHANGE_CONFIGURATION	SignatureOrSystem	change your UI settings	Allows an application to change the current configuration, such as the locale or overall font size.
android.permission.EXPAND_STATUS_BAR	normal	expand/collapse status bar	Allows application to expand or collapse the status bar.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.ujiqeaqk.ottmrjzn.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference

ক্ল APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
Classes.uex	Compiler	dexlib 2.x	

△ NETWORK SECURITY

NO SCOPE SEVERITY DESCRIPTION

CERTIFICATE ANALYSIS

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.

Q MANIFEST ANALYSIS

HIGH: 2 | WARNING: 17 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.4-4.4.4, [minSdk=19]	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	Service (com.google.firebase.messaging.FirebaseMessagingService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Activity (com.wvwnlhuj.mitcbrrn.lPSLqDkPHO) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
4	Activity (com.wwwnlhuj.mitcbrrn.core.XPifUgSiuy) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level.
5	Activity (com.wvwnlhuj.mitcbrrn.core.XPifUgSiuy) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Launch Mode of activity (com.wvwnlhuj.mitcbrrn.xQjpSVvnRC) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
7	Launch Mode of activity (com.wvwnlhuj.mitcbrrn.eqLpAUUXSk) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
8	Activity-Alias (com.wvwnlhuj.mitcbrrn.LmJzkUumyb) is not Protected. An intent-filter exists.	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
9	Broadcast Receiver (com.wvwnlhuj.mitcbrrn.core.lJnMTzPclV) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
10	Broadcast Receiver (com.wvwnlhuj.mitcbrrn.core.rLFxxBUhVQ) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
11	Broadcast Receiver (com.wvwnlhuj.mitcbrrn.core.ldUkWUGFRV) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
12	Service (com.google.firebase.iid.FirebaseInstanceIdService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	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.
14	Broadcast Receiver (com.wwwnlhuj.mitcbrrn.core.SABYleMMaJ) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_DEVICE_ADMIN [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
15	Service (com.wwwnlhuj.mitcbrrn.core.listener.NxkTmkkZqJ) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_ACCESSIBILITY_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
16	Service (com.wwnlhuj.mitcbrrn.core.listener.mJGYMxjlyS) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_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.
17	High Intent Priority (1000) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
18	High Intent Priority (1000) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
19	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

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

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/ujiqeaqk/ottmrjzn/a.java com/ujiqeaqk/ottmrjzn/a/a.java com/ujiqeaqk/ottmrjzn/a/b.java com/ujiqeaqk/ottmrjzn/c.java com/ujiqeaqk/ottmrjzn/d.java myobfuscated/a4/a.java myobfuscated/a4/b.java myobfuscated/hv0/l.java

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

***: ::** ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	17/24	android.permission.READ_CONTACTS, android.permission.READ_SMS, android.permission.READ_PHONE_STATE, android.permission.READ_CALL_LOG, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.RECORD_AUDIO, android.permission.CAMERA, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.GET_TASKS, android.permission.SYSTEM_ALERT_WINDOW, android.permission.WRITE_SETTINGS
Other Common Permissions	15/45	android.permission.CALL_PHONE, android.permission.PROCESS_OUTGOING_CALLS, android.permission.READ_CALENDAR, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE, android.permission.CHANGE_WIFI_STATE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.BIND_DEVICE_ADMIN, android.permission.CHANGE_NETWORK_STATE, android.permission.ACCESS_SUPERUSER, android.permission.PACKAGE_USAGE_STATS, android.permission.BLUETOOTH_ADMIN, android.permission.BROADCAST_STICKY, android.permission.BATTERY_STATS, 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
www.zetetic.net	ok	IP: 13.32.110.128 Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 View: Google Map
play.google.com	ok	IP: 142.251.208.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	IP: 140.82.121.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

HARDCODED SECRETS

POSSIBLE SECRETS

"library_android_database_sqlcipher_authorWebsite": "https://www.zetetic.net/sqlcipher/"

308202223082018b02044bd207bd300d06092a864886f70d01010405003058310b3009060355040613025553310b3009060355040813024341311630140603550407130d53616e204672616e636973636f3110300e060355040a1 30744726f70626f783112301006035504031309546f6d204d65796572301e170d3130303432333230343930315a170d3430303431353230343930315a3058310b3009060355040613025553310b300906035504081302434131163 0140603550407130d53616e204672616e636973636f3110300e060355040a130744726f70626f783112301006035504031309546f6d204d6579657230819f300d06092a864886f70d010101050003818d0030818902818100ac1595d 0ab278a9577f0ca5a14144f96eccde75f5616f36172c562fab0e98c48ad7d64f1091c6cc11ce084a4313d522f899378d312e112a748827545146a779defa7c31d8c00c2ed73135802f6952f59798579859e0214d4e9c0554b53b26032a4 d2dfc2f62540d776df2ea70e2a6152945fb53fef5bac5344251595b729d4810203010001300d06092a864886f70d01010405000381810055c425d94d036153203dc0bbeb3516f94563b102fff39c3d4ed91278db24fc4424a244c2e59f 03bbfea59404512b8bf74662f2a32e37eafa2ac904c31f99cfc21c9ff375c977c432d3b6ec22776f28767d0f292144884538c3d5669b568e4254e4ed75d9054f75229ac9d4ccd0b7c3c74a34f07b7657083b2aa76225c0c56ffc

308201e53082014ea00302010202044e17e115300d06092a864886f70d01010505003037310b30090603550406130255533110300e060355040a1307416e64726f6964311630140603550403130d416e64726f6964204465627567
301e170d3131303730393035303331375a170d3431303730313035303331375a3037310b30090603550406130255533110300e060355040a1307416e64726f6964311630140603550403130d416e64726f69642044656275673081
9f300d06092a864886f70d010101050003818d003081890281810096759fe5abea6a0757039b92adc68d672efa84732c3f959408e12efa264545c61f23141026a6d01eceeeaa13ec7087087e5894a3363da8bf5c69ed93657a6890738
a80998e4ca22dc94848f30e2d0e1890000ae2cddf543b20c0c3828deca6c7944b5ecd21a9d18c988b2b3e54517dafbc34b48e801bb1321e0fa49e4d575d7f0203010001300d06092a864886f70d0101050500038181002b6d4b65bcfa
6ec7bac97ae6d878064d47b3f9f8da654995b8ef4c385bc4fbfbb7a987f60783ef0348760c0708acd4b7e63f0235c35a4fbcd5ec41b3b4cb295feaa7d5c27fa562a02562b7e1f4776b85147be3e295714986c4a9a07183f48ea09ae4d3ea
31b88d0016c65b93526b9c45f2967c3d28dee1aff5a5b29b9c2c8639

∷ SCAN LOGS

Timestamp	Event	Error
2024-08-10 18:45:16	Generating Hashes	ОК
2024-08-10 18:45:16	Extracting APK	ОК

2024-08-10 18:45:16	Unzipping	ОК
2024-08-10 18:45:16	Getting Hardcoded Certificates/Keystores	ОК
2024-08-10 18:45:17	Parsing AndroidManifest.xml	ОК
2024-08-10 18:45:17	Parsing APK with androguard	ОК
2024-08-10 18:45:17	Extracting Manifest Data	ОК
2024-08-10 18:45:17	Performing Static Analysis on: WiFi Service (com.ujiqeaqk.ottmrjzn)	OK
2024-08-10 18:45:17	Fetching Details from Play Store: com.ujiqeaqk.ottmrjzn	OK
2024-08-10 18:45:17	Manifest Analysis Started	OK
2024-08-10 18:45:17	Checking for Malware Permissions	OK
2024-08-10 18:45:17	Fetching icon path	ОК
2024-08-10 18:45:17	Library Binary Analysis Started	ОК
2024-08-10 18:45:18	Analyzing lib/arm64-v8a/libehsvbyfx.so	ОК
2024-08-10 18:45:18	Analyzing lib/armeabi/libtkabhgdd.so	ОК
2024-08-10 18:45:18	Analyzing lib/armeabi/libgifimage.so	ОК

2024-08-10 18:45:18	Analyzing apktool_out/lib/arm64-v8a/libehsvbyfx.so	ОК
2024-08-10 18:45:18	Analyzing apktool_out/lib/armeabi/libtkabhgdd.so	ОК
2024-08-10 18:45:18	Analyzing apktool_out/lib/armeabi/libgifimage.so	ОК
2024-08-10 18:45:18	Reading Code Signing Certificate	ОК
2024-08-10 18:45:18	Running APKiD 2.1.5	ОК
2024-08-10 18:45:19	Detecting Trackers	ОК
2024-08-10 18:45:19	Decompiling APK to Java with jadx	ОК
2024-08-10 18:45:23	Converting DEX to Smali	ОК
2024-08-10 18:45:23	Code Analysis Started on - java_source	ОК
2024-08-10 18:45:24	Android SAST Completed	ОК
2024-08-10 18:45:24	Android API Analysis Started	ОК
2024-08-10 18:45:25	Android Permission Mapping Started	ОК
2024-08-10 18:45:36	Android Permission Mapping Completed	ОК
2024-08-10 18:45:37	Finished Code Analysis, Email and URL Extraction	ОК

2024-08-10 18:45:37	Extracting String data from APK	ОК
2024-08-10 18:45:37	Extracting String data from SO	ОК
2024-08-10 18:45:37	Extracting String data from Code	ОК
2024-08-10 18:45:37	Extracting String values and entropies from Code	ОК
2024-08-10 18:45:37	Performing Malware check on extracted domains	ОК
2024-08-10 18:45:39	Saving to Database	ОК

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.

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.