ANDROID STATIC ANALYSIS REPORT

app_icon

SingleCare (5.9.0)

File Name:	com.singlecare.scma_13518.apk
Package Name:	com.singlecare.scma
Scan Date:	Sept. 1, 2025, 9:01 a.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	8/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	21	4	2	1

FILE INFORMATION

File Name: com.singlecare.scma_13518.apk
Size: 8.34MB
MD5: c45542139b2d81ad8c46a859e9f126f1
SHA1: 3fb3fa3d0cb21944807e83ff0486b875d8f60fda
SHA256: 37273b708962fd2ca2dca33b7f51701c61d1ad8077e61f5079fe5a8aefb9a958

APP INFORMATION

App Name: SingleCare
Package Name: com.singlecare.scma
Main Activity: com.singlecare.scma.view.activity.SplashScreenActivity
Target SDK: 34
Min SDK: 27
Max SDK:
Android Version Name: 5.9.0

Android Version Code: 13518

APP COMPONENTS

Activities: 28
Services: 14
Receivers: 17
Providers: 6
Exported Activities: 5
Exported Services: 1
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: OU=Singlecare, CN=SingleCare Developer
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-04-13 16:11:00+00:00
Valid To: 2041-04-07 16:11:00+00:00
Issuer: OU=Singlecare, CN=SingleCare Developer
Serial Number: 0x261b3c10
Hash Algorithm: sha256
md5: 111868e9bc30ba0e74778dd2d66fcd1d
sha1: dd7bd76b333b225159f6d6c8b01025dba83950ad
sha256: 1a3d8e67adb28337d55e4ad95527c85fa325cc603741a399da40b07069222686
sha512: 654c32c56951a5bcfc4c981b55acf23ecfdd823aa5aec7d7fd231b6c8f2d11a7139f69a4ffa9ed6816e5350e10037e23d435be28df2004f83b93dae03b8771e2
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: cb6af68cee8069e3c006d7ee7918223620d0e22980bf7de077b1f1db1bca4cb8
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_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_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.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.INTERNET	normal	full Internet access	Allows an application to create network sockets.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
com.singlecare.scma.permission.MAPS_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.singlecare.scma.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check ro.hardware check ro.kernel.qemu 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
classes2.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 network operator name check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.singlecare.scma.view.activity.login.SetPasswordActivity	Schemes: https://, singlecaremobile://, Hosts: links.singlecare.com, path, qa.singlecare.com, www.singlecare.com, Path Prefixes: /a, Path Patterns: /forgot-password, /change-password,
com.singlecare.scma.view.activity.MainActivity	Schemes: https://, singlecareapp://, Hosts: singlecare.onelink.me,
com.singlecare.scma.view.activity.AccountActivity	Schemes: https://, Hosts: qa.singlecare.com, www.singlecare.com, Path Patterns: /signin, /signup,

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.singlecare.scma,

NETWORK SECURITY

HIGH: 0 | WARNING: 0 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 11 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.1, minSdk=27]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	App has a Network Security Configuration [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 (com.singlecare.scma.view.activity.login.SetPasswordActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.singlecare.scma.view.activity.MainActivity) 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.
5	Activity (com.singlecare.scma.view.activity.AccountNavMenuActivity) 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	Activity (com.singlecare.scma.view.activity.AccountActivity) 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.
7	Broadcast Receiver (com.appsflyer.SingleInstallBroadcastReceiver) 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.
8	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
9	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.
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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 8 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/c.java a3/i.java a3/j.java a4/l.java a6/v.java aa/c.java b1/n.java b3/e.java b3/i.java b4/e.java b4/f.java b6/e0.java b6/i0.java b6/s.java b6/v.java b6/w.java c3/a.java cf/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/appsflyer/AFLogger.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFd1eSDK.java com/appsflyer/internal/AFd1fSDK.java com/appsflyer/internal/AFd1kSDK.java com/appsflyer/internal/AFd1nSDK.java com/appsflyer/internal/AFd1oSDK.java com/appsflyer/internal/AFd1pSDK.java com/appsflyer/internal/AFd1sSDK.java com/appsflyer/internal/AFd1tSDK.java com/appsflyer/internal/AFd1uSDK.java com/appsflyer/internal/AFe1kSDK.java com/appsflyer/internal/AFe1rSDK.java com/appsflyer/internal/AFe1uSDK.java com/appsflyer/internal/AFf1bSDK.java com/braze/support/BrazeLogger.java com/singlecare/scma/MainApp.java com/singlecare/scma/view/activity/PharmacyListActivity.java com/singlecare/scma/view/activity/ProfileAndSettingsActivity.java com/singlecare/scma/view/activity/b.java com/singlecare/scma/view/activity/login/SetPasswordActivity.java com/singlecare/scma/view/fragment/PharmacyFragment.java d0/c.java d1/q.java d1/w.java d2/t.java d4/a.java d8/f.java e3/c.java e3/d.java e3/f.java e3/s.java e3/t.java e6/b.java f1/a.java f4/f.java f4/i.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	f4/l.java f6/f.java f6/p.java f6/q.java h1/h.java h3/c.java h3/i.java h3/k.java h3/l.java h3/p.java h3/u.java h3/w.java h5/k.java i1/d.java i4/a.java j1/a.java j6/b.java j9/a.java jc/c.java k5/a.java k8/f.java k8/n.java l3/a.java l3/d.java l3/j.java la/d0.java la/g.java la/g0.java la/j0.java la/k.java la/y.java lf/e.java lg/c.java m1/b.java ma/a.java mc/y0.java n1/m0.java n3/e.java n3/f.java n3/k.java n3/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n3/n.java n3/o.java n4/d0.java n4/k0.java n4/l0.java n4/v.java n8/g.java na/c.java na/f.java o3/d.java oc/b.java oc/d.java oc/g.java oc/s.java p7/d.java q0/c.java q3/h.java q7/b.java q8/r.java r3/i.java r4/c.java s0/a.java s7/g.java sc/q0.java t1/m.java t2/c.java t3/a.java t6/j.java tc/h0.java tc/u1.java u/f.java u2/a.java u5/a.java u5/d.java v2/d.java v2/e.java v3/a.java v5/r.java v5/w.java w0/a.java w3/e0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				w3/g.java w3/j0.java w3/n0.java w3/x0.java w4/c.java w6/a.java wb/a.java x0/a.java x2/b.java x2/j.java x2/l.java x3/c.java x3/f.java x3/g0.java x3/m.java x4/w.java x4/z.java x6/a.java y2/c.java y2/e.java y7/g.java z2/h.java z2/i.java z2/k.java z2/q.java z2/z.java z5/d.java z6/h.java z8/g.java z9/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	bo/app/x4.java com/braze/configuration/BrazeConfig.java com/singlecare/scma/MainApp.java com/singlecare/scma/model/PricingModalForSavedCoupons.java com/singlecare/scma/model/cardwalletcoupon/CardWalletCouponDataClass.java com/singlecare/scma/model/request/SignInRequest.java kb/c.java oc/g.java r8/b.java s8/e.java s8/w.java w2/g.java y1/d.java z2/d.java z2/p.java z2/x.java z3/g.java
3	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	q8/i.java y7/b.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	d1/w.java z9/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	bo/app/b0.java bo/app/e.java bo/app/g1.java bo/app/h6.java bo/app/i4.java bo/app/k6.java bo/app/l0.java bo/app/m.java bo/app/m0.java bo/app/m1.java bo/app/n0.java bo/app/q6.java bo/app/s3.java bo/app/u0.java bo/app/z0.java bo/app/z4.java bo/app/z5.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/managers/BrazeGeofenceManager.java com/singlecare/scma/view/activity/b.java d4/j.java j4/b.java w3/b.java w3/l0.java w3/o0.java w3/x0.java x4/y.java xc/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	bo/app/f1.java c9/a.java com/appsflyer/internal/AFa1wSDK.java com/appsflyer/internal/AFb1pSDK.java com/braze/support/IntentUtils.java g9/j.java l9/i.java me/a.java n4/k0.java qb/h.java v5/g.java w3/n.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	kf/c.java kf/d.java kf/i.java kf/j.java
8	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/appsflyer/internal/AFb1zSDK.java g9/m.java w4/a.java z9/b.java
9	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	ac/a.java i1/c.java o5/m0.java o5/t0.java vb/a.java z8/h.java
10	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/appsflyer/internal/AFb1zSDK.java com/braze/support/StringUtils.java f4/l.java x3/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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	com/singlecare/scma/view/fragment/PharmacyFragment.java n4/k0.java
12	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/singlecare/scma/view/activity/PharmacyListActivity.java
13	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	l9/c.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	g4/f.java p4/c.java t4/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFe1uSDK.java g4/j.java j4/a.java p4/k.java r8/f.java x8/a.java z9/c.java
00022	Open a file from given absolute path of the file	file	ac/b.java com/appsflyer/internal/AFe1uSDK.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java d1/w.java d9/g.java e2/c.java h0/m.java i1/d.java pb/a.java r8/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	ac/b.java bo/app/o0.java com/appsflyer/internal/AFa1jSDK.java com/appsflyer/internal/AFe1uSDK.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java d1/w.java e2/c.java e3/f.java f1/b.java f4/l.java fe/i.java g4/j.java h0/m.java j4/a.java p4/k.java q8/a0.java r8/f.java u2/a.java v8/e.java x3/f.java x8/a.java z9/c.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFe1uSDK.java r8/f.java
00031	Check the list of currently running applications	reflection collection	oc/b0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1oSDK.java com/braze/Braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java com/singlecare/scma/view/activity/AccountActivity.java com/singlecare/scma/view/activity/PharmacyListActivity.java com/singlecare/scma/view/activity/ProfileAndSettingsActivity.java com/singlecare/scma/view/activity/SavingCardActivity.java com/singlecare/scma/view/activity/SplashScreenActivity.java com/singlecare/scma/view/fragment/PharmacyFragment.java n4/a.java n4/d0.java n4/k0.java n4/l0.java n4/p0.java oc/v.java tc/g.java x4/c.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/singlecare/scma/view/activity/AccountActivity.java com/singlecare/scma/view/activity/PharmacyListActivity.java com/singlecare/scma/view/activity/ProfileAndSettingsActivity.java com/singlecare/scma/view/activity/SavingCardActivity.java com/singlecare/scma/view/fragment/PharmacyFragment.java n4/k0.java n4/l0.java oc/v.java tc/g.java
00078	Get the network operator name	collection telephony	bo/app/m0.java com/appsflyer/internal/AFa1iSDK.java n4/k0.java wb/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1iSDK.java n4/a.java n4/d0.java n4/k0.java
00036	Get resource file from res/raw directory	reflection	com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFf1gSDK.java com/appsflyer/internal/AFf1iSDK.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java mc/y0.java n4/a.java n4/k0.java n4/l0.java n4/p0.java oc/v.java
00094	Connect to a URL and read data from it	command network	u8/a.java
00096	Connect to a URL and set request method	command network	aa/c.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1rSDK.java e2/f.java w3/e0.java z3/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	aa/c.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1rSDK.java e2/f.java w4/c.java x2/j.java z3/g.java
00109	Connect to a URL and get the response code	network command	aa/c.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1rSDK.java com/appsflyer/internal/AFd1lSDK.java e2/f.java u5/d.java x2/j.java z3/g.java
00153	Send binary data over HTTP	http	e2/f.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFb1uSDK.java com/braze/push/BrazeNotificationUtils.java com/singlecare/scma/view/activity/MainActivity.java com/singlecare/scma/view/activity/PharmacyListActivity.java com/singlecare/scma/view/activity/PrescriptionBuildActivity.java com/singlecare/scma/view/activity/SetPriceActivity.java com/singlecare/scma/view/activity/SetPriceSignUpActivity.java com/singlecare/scma/view/activity/SplashScreenActivity.java n4/d0.java x4/c0.java
00012	Read data and put it into a buffer stream	file	e2/c.java f4/l.java x3/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	oc/d0.java
00162	Create InetSocketAddress object and connecting to it	socket	kf/b.java kf/j.java
00163	Create new Socket and connecting to it	socket	kf/b.java kf/j.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFa1eSDK.java com/appsflyer/internal/AFf1gSDK.java com/appsflyer/internal/AFf1hSDK.java n4/d0.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFa1eSDK.java com/appsflyer/internal/AFf1gSDK.java com/appsflyer/internal/AFf1hSDK.java n4/d0.java y2/c.java
00114	Create a secure socket connection to the proxy address	network command	gf/f.java
00121	Create a directory	file command	com/singlecare/scma/view/activity/PharmacyListActivity.java com/singlecare/scma/view/fragment/PharmacyFragment.java
00125	Check if the given file path exist	file	com/singlecare/scma/view/activity/PharmacyListActivity.java com/singlecare/scma/view/fragment/PharmacyFragment.java g4/f.java
00003	Put the compressed bitmap data into JSON object	camera	a4/l.java w3/e0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00202	Make a phone call	control	com/singlecare/scma/view/activity/PharmacyListActivity.java
00203	Put a phone number into an intent	control	com/singlecare/scma/view/activity/PharmacyListActivity.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFa1eSDK.java
00030	Connect to the remote server through the given URL	network	com/appsflyer/internal/AFa1uSDK.java x2/j.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFf1hSDK.java n4/d0.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFf1hSDK.java n4/d0.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFf1hSDK.java n4/d0.java
00187	Query a URI and check the result	collection sms calllog calendar	n4/d0.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFf1hSDK.java n4/d0.java
00123	Save the response to JSON after connecting to the remote server	network command	bo/app/t1.java
00132	Query The ISO country code	telephony collection	wb/c.java
00033	Query the IMEI number	collection	bo/app/m0.java
00083	Query the IMEI number	collection telephony	bo/app/m0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00015	Put buffer stream (data) to JSON object	file	n4/k0.java
00009	Put data in cursor to JSON object	file	n4/k0.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://singlecare-232802-bf5e0.firebaseio.com/
App talks to a Firebase database	info	The app talks to Firebase database at https://singlecare-232802.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/383742106474/namespaces/firebase:fetch?key=AIzaSyAO5x6IoR2RPJ5AHQ-mW38ZuIUVdCQ7s6Q is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'android_feature_flag_enable_security_flag': 'false', 'android_feature_flag_load_contentful_ad': 'true', 'android_feature_flag_loyalty_signup_bonus': '$3', 'android_sign_up_drug_price_display_variant': 'price_button_with_substracted_savings', 'app_launch_variant': 'loyalty_welcome_screen', 'iOS_coupon_drug_price_signup_variant': 'show_signup_no_green_sticker', 'iOS_coupon_drug_price_variant': 'show_price_label', 'iOS_feature_flag_enableSSLPinning': 'true', 'iOS_feature_flag_loyalty_signup_bonus': '$3', 'iOS_feature_flag_showAddToWalletButton': 'false', 'iOS_feature_flag_show_prospect_id': 'true', 'iOS_hooking_enable_in_ios_14_and_lower': 'false', 'ios_feature_flag_show_patientcompassAd': 'true'}, 'state': 'UPDATE', 'templateVersion': '111'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_PHONE_STATE, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	5/44	android.permission.CALL_PHONE, 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
webapi.singlecare.com	ok	**IP:** 3.220.208.77 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.singlecare.com	ok	**IP:** 18.155.173.62 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
graph-video.s	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
mobile.events.data.microsoft.com	ok	**IP:** 13.89.179.13 **Country:** United States of America **Region:** Iowa **City:** Des Moines **Latitude:** 41.600540 **Longitude:** -93.609108 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sdk.iad-01.braze.com	ok	**IP:** 172.64.148.188 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.linkedin.com	ok	**IP:** 104.18.41.41 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
graph.s	ok	No Geolocation information available.
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.74.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
smonitorsdk.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
prodapi.singlecare.com	ok	**IP:** 34.228.126.156 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.braze.com	ok	**IP:** 104.17.228.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
sars.s	ok	No Geolocation information available.
sondheim.braze.com	ok	**IP:** 172.64.144.252 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.74.162 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sregister.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
singlecare-232802.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
scdn-ssettings.s	ok	No Geolocation information available.
www.instagram.com	ok	**IP:** 31.13.70.174 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
console.firebase.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.ipify.org	ok	**IP:** 104.26.13.205 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
scdn-stestsettings.s	ok	No Geolocation information available.
sstats.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
www.twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
in.appcenter.ms	ok	**IP:** 4.153.25.42 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
sapp.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
firebase-settings.crashlytics.com	ok	**IP:** 216.58.207.195 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api2.singlecare.com	ok	**IP:** 18.155.173.75 **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.
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
svalidate.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
singlecare-232802-bf5e0.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

EMAILS

EMAIL	FILE
appsupport@singlecare.com appsupport@rxsense.com email@domain.com support@singlecare.com youremail@gmail.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67

TRACKER	CATEGORIES	URL
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
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"appcenter_key" : "57a87596-f0f2-4286-9f64-eaa0e55950f3"
"appsflyer_key" : "bBg46Naz95pzs7kNsZNBmA"
"com_braze_api_key" : "ef42d4be-d548-4d29-9b76-af4bb3229158"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"

POSSIBLE SECRETS
"cvs_partner_password" : "DCw%ZgaBa3BffW_P"
"facebook_client_token" : "378cae4da8389048cf02a82bf0dc7782"
"firebase_application_details" : "application_details"
"firebase_contact_us" : "contact_us"
"firebase_database_url" : "https://singlecare-232802.firebaseio.com"
"firebase_privacy_policy" : "privacy_policy"
"firebase_realtime_database_url" : "https://singlecare-232802-bf5e0.firebaseio.com/"
"firebase_sender_id" : "383742106474"
"firebase_terms_and_conditions" : "terms_and_conditions"
"ga4_session_id" : "GA4_Session_ID"
"google_api_key" : "AIzaSyAO5x6IoR2RPJ5AHQ-mW38ZuIUVdCQ7s6Q"
"google_crash_reporting_api_key" : "AIzaSyAO5x6IoR2RPJ5AHQ-mW38ZuIUVdCQ7s6Q"
"iterable_api_key" : "7e0ed498690d4c039642da5783fdd6a3"
"map_key" : "AIzaSyBlLdVBjoSL2ZcC84Pe0r4Em0lgeAZNlHA"
"optimizly_key" : "8WtfjTMixfMX4LrCE58Up9"

POSSIBLE SECRETS
"pPass" : "pPass"
"partner_password" : "PartnerPassword"
"partner_username" : "PartnerUsername"
"password" : "Password"
"reg_partner_password" : "E3b?62XKE8"
"reset_password" : "reset_password"
"segment_key" : "46gxxyhGcXO7JHWQ9wd40ynAMzXgdRjR"
"set_password" : "set_password"
"token" : "token"
"wg_partner_password" : "4U{.A3AnW2m.S+qX"
"wm_partner_password" : "FC:v)6-SpuP%Wp7N"
"com_facebook_device_auth_instructions" : "facebook.com/device□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□facebook.com/device□□□□□□□□□□□□□□"
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212

POSSIBLE SECRETS
411ac1d458f4d31605332f08000280b5
9d0768679c3acd8ac626979b6ba7bd5e
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
c56fb7d591ba6704df047fd98f535372fea00211
cc2751449a350f668590264ed76692694a80308a
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
470fa2b4ae81cd56ecbcda9735803434cec591fa
37a6259cc0c1dae299a7866489dff0bd
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
9b8f518b086098de3d77736f9458a3d2f6f95a37
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
3071c8717539de5d5353f4c8cd59a032
7d73d21f1bd82c9e5268b6dcf9fde2cb

PLAYSTORE INFORMATION

Title: SingleCare - Rx Coupons

Score: 4.675241 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.singlecare.scma

Developer Details: RxSense, RxSense, None, https://www.singlecare.com, tech@singlecare.com,

Release Date: Apr 20, 2016 **Privacy Policy:** Privacy link

Description:

Discover the power of prescription discount coupons with SingleCare - Rx Coupons, the popular app for saving up to 80% on your prescription medications. With a user-friendly interface and an extensive network of participating pharmacies, SingleCare ensures you'll get discounted prices on more than 10,000 medications, making healthcare more accessible for everyone. Best of all, the SingleCare prescription savings card (also known as a "coupon card") is completely free to use. Just get your coupon, show it to your pharmacist, and unlock your discount. Whether you're insured, underinsured, or uninsured, you qualify for a reduced rate on pharmacy prescriptions with SingleCare. Just use our drug pricing tool to find discounts on thousands of FDA-approved medications. Key Features: Access a wide range of free Rx coupons and discounts for prescription drugs, helping you save up to 80% on medications prescribed by your healthcare provider. Say goodbye to high costs and hello to significant savings on 10,000+ medications at 35,000+ pharmacies across the country! Member perks: If you choose to create a free account, you'll receive an extra $3 in bonus savings to use on your next eligible refill, plus you'll start to earn additional bonus savings just by filling more prescriptions. Members get access to our lowest prices! Easy Refills • Set up helpful refill reminders, so you never miss a dose. • Remember, you can always reuse the card again for a discount on your next refill! Navigate through the app effortlessly with its intuitive design. SingleCare - Rx Coupons offers a seamless user experience, allowing you to quickly search for medications, locate nearby pharmacies, and compare prices for drugs and medications, all with just a few taps. Try SingleCare in 3 simple steps: 1. Search for your prescription medication on the free SingleCare app. 2. Compare discounts on medications at nearby pharmacies and get a free Rx coupon card. 3. Show your Rx coupon card at the pharmacy counter to save up to 80% on your prescription medication. SingleCare partners with a vast network of over 35,000 participating pharmacies nationwide, including major chains and regional stores. Easily find the nearest pharmacy and discover which ones offer the lowest prices for your prescribed medications. With SingleCare, you'll always have access to affordable drugs and medications. Prescription Discount Finder Enter your zip code on the app to find a participating pharmacy near you. We partner directly with thousands of major pharmacies nationwide, including: • CVS • CVS Pharmacy at Target • Walmart • Walgreens • Kroger • Albertsons • Rite Aid • Longs Drugs • Sav-On Pharmacy • Fry's • Harris Teeter • Wegmans • H-E-B • Meijer Take advantage of the app's transparent pricing information, which enables you to make informed decisions about where to fill your prescriptions. SingleCare provides up-to-date pricing details for a wide range of medications, helping you choose the most cost-effective option available. SingleCare prescription coupons include drugs used to treat: • Weight loss • Infection • High blood pressure • Birth Control • & more! Stay on top of your medication schedule with the app's convenient reminder feature. Set personalized reminders for refilling your medications, so you never miss a dose. SingleCare - Rx Coupons is the go-to app for those seeking significant savings on prescription medications. Say goodbye to inflated costs and hello to affordable medications. Download the app today and unlock the power of substantial savings! Please note: SingleCare is not insurance, but rather a free discount program. The app is not intended to replace your insurance coverage but to complement it by providing additional savings options for drugs and medications. By downloading SingleCare, you agree to be bound by our Terms and Conditions found at https://www.singlecare.com/terms-and-conditions.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 09:01:47	Generating Hashes	OK
2025-09-01 09:01:47	Extracting APK	OK
2025-09-01 09:01:47	Unzipping	OK
2025-09-01 09:01:48	Parsing APK with androguard	OK
2025-09-01 09:01:48	Extracting APK features using aapt/aapt2	OK
2025-09-01 09:01:48	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 09:01:51	Parsing AndroidManifest.xml	OK
2025-09-01 09:01:51	Extracting Manifest Data	OK
2025-09-01 09:01:51	Manifest Analysis Started	OK
2025-09-01 09:01:52	Reading Network Security config from network_security_config.xml	OK

2025-09-01 09:01:52	Parsing Network Security config	OK
2025-09-01 09:01:52	Performing Static Analysis on: SingleCare (com.singlecare.scma)	OK
2025-09-01 09:01:54	Fetching Details from Play Store: com.singlecare.scma	OK
2025-09-01 09:01:55	Checking for Malware Permissions	OK
2025-09-01 09:01:55	Fetching icon path	OK
2025-09-01 09:01:55	Library Binary Analysis Started	OK
2025-09-01 09:01:55	Reading Code Signing Certificate	OK
2025-09-01 09:01:55	Running APKiD 2.1.5	OK
2025-09-01 09:01:58	Detecting Trackers	OK
2025-09-01 09:02:00	Decompiling APK to Java with JADX	OK
2025-09-01 09:02:13	Converting DEX to Smali	OK

2025-09-01 09:02:13	Code Analysis Started on - java_source	OK
2025-09-01 09:02:15	Android SBOM Analysis Completed	OK
2025-09-01 09:02:19	Android SAST Completed	OK
2025-09-01 09:02:19	Android API Analysis Started	OK
2025-09-01 09:02:22	Android API Analysis Completed	OK
2025-09-01 09:02:23	Android Permission Mapping Started	OK
2025-09-01 09:02:25	Android Permission Mapping Completed	OK
2025-09-01 09:02:26	Android Behaviour Analysis Started	OK
2025-09-01 09:02:31	Android Behaviour Analysis Completed	OK
2025-09-01 09:02:31	Extracting Emails and URLs from Source Code	OK
2025-09-01 09:02:33	Email and URL Extraction Completed	OK

2025-09-01 09:02:33	Extracting String data from APK	OK
2025-09-01 09:02:33	Extracting String data from Code	OK
2025-09-01 09:02:33	Extracting String values and entropies from Code	OK
2025-09-01 09:02:36	Performing Malware check on extracted domains	OK
2025-09-01 09:02:38	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.