MOBSF

ANDROID STATIC ANALYSIS REPORT

Aptoide (9.20.6.1)

File Name:	parkify-where-is-my-car.apk
Package Name:	cm.aptoide.pt
Scan Date:	April 10, 2024, 6:51 p.m.
App Security Score:	37/100 (HIGH RISK)
Grade:	C
Trackers Detection:	6/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
15	24	2	3	2

FILE INFORMATION

File Name: parkify-where-is-my-car.apk
Size: 18.78MB
MD5: 6fcf0a130db195563c2b925d1e75a663
SHA1: b81bcd1602ee732e56086a8144a2047ce6f47af4
SHA256: bb900cd252f168f499d1dad5d94e6b4e73d52af2684f9f182172af52f5ef3f6e

APP INFORMATION

App Name: Aptoide
Package Name: cm.aptoide.pt
Main Activity: cm.aptoide.pt.view.MainActivity
Target SDK: 25
Min SDK: 16
Max SDK:
Android Version Name: 9.20.6.1
Android Version Code: 12010

APP COMPONENTS

Activities: 11
Services: 10
Receivers: 14
Providers: 6
Exported Activities: 2
Exported Services: 3
Exported Receivers: 4
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: ST=Portugal
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2009-09-22 14:53:51+00:00
Valid To: 2034-09-16 14:53:51+00:00
Issuer: ST=Portugal
Serial Number: 0x4ab8e4ff
Hash Algorithm: sha1
md5: 99bd1872bc56b4b2619e731ae9cbdc6f
sha1: d590a7d792fd0331542d99faf9997641790773a9
sha256: 73534d45c1345a4783c7eff2cf6038551ab5fdf09673f32c68c3b0864baa80e4
sha512: 8a5562a7825800df284d47dab79fcae1ccde0c3c46b1a181696809ed270576b92718130131ffef402f4d2822e235879de1e91224d91f0f4c0a0b58d2d2bc5b43
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION

android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_SYNC_STATS	normal	read sync statistics	Allows an application to read the sync stats; e.g. the history of syncs that have occurred.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
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.INSTALL_PACKAGES	SignatureOrSystem	directly install applications	Allows an application to install new or updated Android packages. Malicious applications can use this to add new applications with arbitrarily powerful permissions.
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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
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.
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.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
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.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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

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.PRODUCT check possible Build.SERIAL check network operator name check device ID check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table>
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 Build.TAGS check SIM operator check network operator name 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>

classes3.dex	

FINDINGS	DETAILS
Compiler	r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.cm.aptoide.pt,
cm.aptoide.pt.DeepLinkIntentReceiver	Schemes: file://, http://, aptoide://, aptoiderepo://, aptoideinstall://, aptoideauth://, aptoidesearch://, aptoidefeature://, market://, https://, Hosts: app.aptoide.com, market.android.com, webservices.aptoide.com, play.google.com, *.en.aptoide.com, *.pt.aptoide.com, *.br.aptoide.com, *.fr.aptoide.com, *.es.aptoide.com, *.mx.aptoide.com, *.de.aptoide.com, *.it.aptoide.com, *.ru.aptoide.com, *.sa.aptoide.com, *.id.aptoide.com, *.in.aptoide.com, *.bd.aptoide.com, *.mr.aptoide.com, *.pa.aptoide.com, *.my.aptoide.com, *.th.aptoide.com, *.vn.aptoide.com, *.tr.aptoide.com, *.cn.aptoide.com, *.ro.aptoide.com, *.mm.aptoide.com, *.pl.aptoide.com, *.rs.aptoide.com, *.hu.aptoide.com, *.gr.aptoide.com, *.bg.aptoide.com, *.nl.aptoide.com, *.ir.aptoide.com, *.jp.aptoide.com, *.kr.aptoide.com, *.ua.aptoide.com, en.aptoide.com, pt.aptoide.com, br.aptoide.com, fr.aptoide.com, es.aptoide.com, mx.aptoide.com, de.aptoide.com, it.aptoide.com, ru.aptoide.com, sa.aptoide.com, id.aptoide.com, in.aptoide.com, bd.aptoide.com, mr.aptoide.com, pa.aptoide.com, my.aptoide.com, th.aptoide.com, vn.aptoide.com, tr.aptoide.com, cn.aptoide.com, ro.aptoide.com, mm.aptoide.com, pl.aptoide.com, rs.aptoide.com, hu.aptoide.com, gr.aptoide.com, bg.aptoide.com, nl.aptoide.com, ir.aptoide.com, jp.aptoide.com, kr.aptoide.com, ua.aptoide.com, community.aptoide.com, become-a-power-gamer.aptoide.com, Mime Types: application/vnd.cm.aptoide.pt, Path Prefixes: /apkinstall, Path Patterns: /store/..*, /thank-you*, /appcoins, /using-appcoins*, /download*, /editorial/..*, /app,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	info	Base config is configured to trustbundled certs @raw/vanilla_cert.
2	*	warning	Base config is configured to trust system certificates.

CERTIFICATE ANALYSIS

HIGH: 2 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	high	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.
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 12 | WARNING: 14 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.1-4.1.2, [minSdk=16]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

2	App has a Network Security Configuration [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	Launch Mode of activity (cm.aptoide.pt.view.MainActivity) 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.
4	Activity (cm.aptoide.pt.view.MainActivity) is vulnerable to Android Task Hijacking/StrandHogg.	high	An Activity should not be having the launch mode attribute set to "singleTask". It is then possible for other applications to place a malicious activity on top of the activity stack resulting in Task Hijacking/StrandHogg 1.0 vulnerability. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" or by setting an empty taskAffinity (taskAffinity="") attribute. You can also update the target SDK version (25) of the app to 28 or higher to fix this issue at platform level.
5	TaskAffinity is set for activity (cm.aptoide.pt.wallet.WalletInstallActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
6	Service (cm.aptoide.pt.account.AccountAuthenticatorService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
7	Content Provider (cm.aptoide.pt.toolbox.ToolboxContentProvider) is not Protected. [android:exported=true]	warning	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.

8	Activity (com.facebook.CustomTabActivity) 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 (25) of the app to 29 or higher to fix this issue at platform level.
9	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.
10	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://app.aptoide.com]	high	App Link asset verification URL (http://app.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
11	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=https://app.aptoide.com]	high	App Link asset verification URL (https://app.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

12	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://webservices.aptoide.com]	high	App Link asset verification URL (http://webservices.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
13	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=https://webservices.aptoide.com]	high	App Link asset verification URL (https://webservices.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
14	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://community.aptoide.com]	high	App Link asset verification URL (http://community.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
			App Link asset verification URL (https://community.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App

15	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=https://community.aptoide.com]	high	Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
16	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=http://become-a-power-gamer.aptoide.com]	high	App Link asset verification URL (http://become-a-power-gamer.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
17	App Link assetlinks.json file not found [android:name=cm.aptoide.pt.DeepLinkIntentReceiver] [android:host=https://become-a-power-gamer.aptoide.com]	high	App Link asset verification URL (https://become-a-power-gamer.aptoide.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
18	TaskAffinity is set for activity (cm.aptoide.pt.DeepLinkIntentReceiver)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
			Activity is found to be vulnerable to StrandHogg 2.0 task

19	Activity (cm.aptoide.pt.DeepLinkIntentReceiver) is vulnerable to StrandHogg 2.0	high	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 (25) of the app to 29 or higher to fix this issue at platform level.
20	Activity (cm.aptoide.pt.DeepLinkIntentReceiver) 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.
21	Broadcast Receiver (cm.aptoide.pt.install.InstalledBroadcastReceiver) 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.
22	Broadcast Receiver (cm.aptoide.pt.notification.NotificationReceiver) 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.
23	Broadcast Receiver (cm.aptoide.pt.install.CheckRootOnBoot) 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.
24	Broadcast Receiver (cm.aptoide.pt.widget.SearchWidgetProvider) 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.
25	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:	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

	com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]		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.
26	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.
27	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 8 | INFO: 1 | SECURE: 3 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cm/aptoide/aptoideviews/common/StringUtilsKt.java cm/aptoide/aptoideviews/downloadprogressview/DownloadProgressView$stateMachine$1.java cm/aptoide/pt/app/view/AppCoinsInfoFragment.java cm/aptoide/pt/crashreports/CrashReport.java cm/aptoide/pt/editorial/EditorialFragment.java cm/aptoide/pt/editorialList/EditorialListFragment.java cm/aptoide/pt/home/HomeFragment.java cm/aptoide/pt/install/installer/Root.java cm/aptoide/pt/install/remote/RemoteInstallatio

				nSenderManager.java cm/aptoide/pt/logger/Logger.java cm/aptoide/pt/networking/image/ImageLoader.java cm/aptoide/pt/notification/NotificationWorker.java cm/aptoide/pt/root/RootShell.java cm/aptoide/pt/root/containers/RootClass.java cm/aptoide/pt/toolbox/ToolboxContentProvider.java com/airbnb/epoxy/i.java com/airbnb/epoxy/p.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/c.java com/airbnb/lottie/d.java com/airbnb/lottie/e.java com/airbnb/lottie/f.java com/airbnb/lottie/l.java com/airbnb/lottie/r/a.java com/airbnb/lottie/r/b.java com/airbnb/lottie/u/c.java com/airbnb/lottie/u/g.java com/airbnb/lottie/u/u.java com/asf/appcoins/sdk/core/util/LogInterceptor.java com/bumptech/glide/c.java com/bumptech/glide/l/d.java com/bumptech/glide/l/e.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/a0/e.java com/bumptech/glide/load/engine/a0/i.java com/bumptech/glide/load/engine/b0/a.java com/bumptech/glide/load/engine/b0/b.java com/bumptech/glide/load/engine/h.java com/bumptech/glide/load/engine/i.java com/bumptech/glide/load/engine/k.java com/bumptech/glide/load/engine/y.java com/bumptech/glide/load/engine/z/j.java com/bumptech/glide/load/engine/z/k.java com/bumptech/glide/load/m/b.java com/bumptech/glide/load/m/j.java

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/m/l.java com/bumptech/glide/load/m/o/c.java com/bumptech/glide/load/m/o/e.java com/bumptech/glide/load/n/c.java com/bumptech/glide/load/n/d.java com/bumptech/glide/load/n/f.java com/bumptech/glide/load/n/s.java com/bumptech/glide/load/n/t.java com/bumptech/glide/load/o/c/c.java com/bumptech/glide/load/o/c/j.java com/bumptech/glide/load/o/c/l.java com/bumptech/glide/load/o/c/m.java com/bumptech/glide/load/o/c/q.java com/bumptech/glide/load/o/c/w.java com/bumptech/glide/load/o/c/y.java com/bumptech/glide/load/o/g/a.java com/bumptech/glide/load/o/g/d.java com/bumptech/glide/load/o/g/j.java com/bumptech/glide/m/e.java com/bumptech/glide/m/f.java com/bumptech/glide/m/k.java com/bumptech/glide/m/l.java com/bumptech/glide/m/n.java com/bumptech/glide/m/o.java com/bumptech/glide/n/d.java com/bumptech/glide/p/j.java com/bumptech/glide/p/l/j.java com/bumptech/glide/q/a.java com/bumptech/glide/r/l/a.java com/flurry/sdk/a.java io/rakam/api/i.java l/a/k/a/a.java l/a/o/g.java l/f/b/d.java l/f/b/k/f.java l/h/e/c.java l/h/e/e.java l/h/e/f.java l/h/e/g.java l/h/e/j.java l/h/e/k.java l/h/j/b.java

				l/h/k/b.java l/h/l/b.java l/h/l/d0.java l/h/l/e0/c.java l/h/l/f.java l/h/l/h.java l/h/l/v.java l/h/l/w.java l/h/l/y.java l/j/a/c.java l/l/a/b.java l/l/b/c.java l/m/a/a.java l/n/a.java l/n/b.java l/o/a/b.java l/q/a/c.java l/r/a/c.java l/s/i0.java l/s/y.java l/t/a/a/i.java n/b/a/a/a.java n/e/b/b/m/h.java n/e/b/b/w/d.java n/e/b/b/x/b.java n/e/b/b/z/g.java n/f/a/a/a.java q/b/g/a.java q/b/g/b.java q/b/g/d/a/a.java t/b/g/j.java
2	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	cm/aptoide/pt/account/view/PhotoFileGenerator.java l/n/b.java
				cm/aptoide/pt/BuildConfig.java cm/aptoide/pt/DeepLinkIntentReceiver.java cm/aptoide/pt/account/AccountAnalytics.java cm/aptoide/pt/account/AndroidAccountManagerPersistence.java

3	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	cm/aptoide/pt/account/view/LoginSignUpCredentialsFragment.java cm/aptoide/pt/app/view/MoreBundleFragment.java cm/aptoide/pt/bottomNavigation/BottomNavigationActivity.java cm/aptoide/pt/database/room/RoomNotification.java cm/aptoide/pt/database/room/RoomStore.java cm/aptoide/pt/dataprovider/WebService.java cm/aptoide/pt/dataprovider/model/v3/CheckUserCredentialsJson.java cm/aptoide/pt/home/HomeFragment.java cm/aptoide/pt/home/bundles/BundlesRepository.java cm/aptoide/pt/networking/Pnp1AuthorizationInterceptor.java cm/aptoide/pt/preferences/LocalPersistenceAdultContent.java cm/aptoide/pt/preferences/managed/ManagedKeys.java cm/aptoide/pt/promotions/ClaimPromotionDialogFragment.java cm/aptoide/pt/themes/ThemeManager.java cm/aptoide/pt/view/DeepLinkManager.java cm/aptoide/pt/view/app/ListStoreAppsFragment.java cm/aptoide/pt/view/fragment/GridRecyclerSwipeWithToolbarFragment.java cm/aptoide/pt/view/settings/SettingsFragment.java com/bumptech/glide/load/engine/d.java com/bumptech/glide/load/engine/p.java com/bumptech/glide/load/engine/w.java com/bumptech/glide/load/h.java q/b/l/g/k.java
4	App can read/write to External Storage. Any App can read data written to	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage	cm/aptoide/pt/ApplicationModule.java cm/aptoide/pt/database/room/RoomInstalled.java cm/aptoide/pt/install/installer/DefaultInstaller.java

	External Storage.		OWASP MASVS: MSTG-STORAGE-2	cm/aptoide/pt/view/ActivityModule.java com/flurry/sdk/i4.java q/b/g/d/a/a.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	cm/aptoide/pt/BuildConfig.java r/a/g/l.java
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	cm/aptoide/pt/ads/AdsRepository.java cm/aptoide/pt/utils/AptoideUtils.java io/sentry/connection/l.java r/a/g/h.java r/a/g/l.java
7	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	cm/aptoide/pt/download/FileDownloadTask.java cm/aptoide/pt/utils/AptoideUtils.java n/h/a/f0/f.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	cm/aptoide/pt/ApplicationModule.java cm/aptoide/pt/abtesting/ABTestServiceProvider.java cm/aptoide/pt/dataprovider/WebService.java com/aptoide/authentication/network/RemoteAuthenticationService.java com/asf/appcoins/sdk/contractproxy/AppCoinsAddressProxyBuilder.java com/flurry/sdk/l1.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	com/liulishuo/filedownloader/services/b.java com/liulishuo/filedownloader/services/c.java io/rakam/api/b.java l/q/a/g/a.java
10	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	cm/aptoide/pt/preferences/PRNGFixes.java cm/aptoide/pt/utils/AptoideUtils.java

			OWASP MASVS: MSTG-CRYPTO-4	
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	q/b/g/d/a/a.java
12	This App uses SafetyNet API.	secure	OWASP MASVS: MSTG-RESILIENCE-7	cm/aptoide/pt/analytics/FirstLaunchAnalytics.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/24	android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_WIFI_STATE, android.permission.GET_ACCOUNTS, android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	3/45	com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.AUTHENTICATE_ACCOUNTS, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_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
twitter.com	ok	**IP:** 104.244.42.193 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
www.youtube.com	ok	**IP:** 172.253.62.93 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ws75-primary.aptoide.com	ok	**IP:** 37.48.77.161 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

docs.sentry.io	ok	IP: 76.76.21.9 Country: United States of America Region: California City: Walnut Latitude: 34.015400 Longitude: -117.858223 View: Google Map
api.aptoide.com	ok	IP: 54.76.219.178 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190 View: Google Map
cdn6.aptoide.com	ok	IP: 104.22.10.83 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
www.slf4j.org	ok	IP: 159.100.250.151 Country: Switzerland Region: Vaud City: Lausanne Latitude: 46.515999 Longitude: 6.632820 View: Google Map
placeimg.com	ok	IP: 159.65.240.55 Country: United States of America Region: New Jersey City: Clifton Latitude: 40.858429 Longitude: -74.163757 View: Google Map

www.instagram.com	ok	**IP:** 157.240.229.174 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
webservices.aptoide.com	ok	**IP:** 37.48.77.181 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
imgs.aptoide.com	ok	**IP:** 37.48.77.180 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
api.blockchainds.com	ok	**IP:** 52.19.9.97 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

api.indicative.com	ok	**IP:** 34.98.104.50 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
apichain.blockchainds.com	ok	**IP:** 18.200.218.46 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
www.aptoide.com	ok	**IP:** 18.203.38.6 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
m.aptoide.com	ok	**IP:** 37.48.77.161 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
play.google.com	ok	**IP:** 142.250.31.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991

		Longitude: -122.078514 **View:** Google Map
impression.appsflyer.com	ok	**IP:** 3.162.112.20 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
catappult.io	ok	**IP:** 13.249.39.44 **Country:** United States of America **Region:** Virginia **City:** Dulles **Latitude:** 38.951668 **Longitude:** -77.448059 **View:** Google Map
diagnostics.rakam.io	ok	**IP:** 172.67.215.225 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.example.com	ok	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
pool.img.aptoide.com	ok	**IP:** 104.22.11.83 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700

		Longitude: -122.395203 **View:** Google Map
sentry.aptoide.com	ok	**IP:** 99.81.19.121 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
data.flurry.com	ok	**IP:** 74.6.138.65 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
ws75.aptoide.com	ok	**IP:** 54.74.52.93 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
blog.aptoide.com	ok	**IP:** 37.48.77.171 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
facebook.com	ok	**IP:** 157.240.229.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031

		Longitude: 4.889690 **View:** Google Map
apichain-dev.blockchainds.com	ok	No Geolocation information available.
aptoi.de	ok	**IP:** 52.23.47.7 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

EMAILS

EMAIL	FILE
filipo@emailo.como	com/aptoide/authentication/mock/MockAuthenticationService.java
485bb7b111d41f17e0f8@sentry.aptoide	cm/aptoide/pt/BuildConfig.java
support@aptoide.com	cm/aptoide/pt/AptoideApplication.java
aptoide@aptoide.com suport@aptoide.com support@aptoide.com 请通过suport@aptoide.com与技术支持人员	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL

Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Flurry	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/25
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"password" : "Password"
"search_suggestion_provider_authority" : "cm.aptoide.pt.provider.SearchSuggestionProvider"
"store_suggestion_provider_authority" : "cm.aptoide.pt.provider.StoreSearchSuggestionProvider"
"store_username" : "Nickname"
"username" : "Email"
"password" : "گذرواژه"
"com_facebook_device_auth_instructions" : "facebook.com/deviceにアクセスして、上のコードを入力してください。"
"nothing_inserted_user" : "ニックネームと写真（任意）を入れて、プロフィールを作成"

"password" : "パスワード"

"recover_password" : "あなたのパスワードを回復します"

"store_username" : "ニックネーム"

"username" : "Eメール"

"password" : "ਪਾਸਵਰਡ"

"store_username" : "ਉਪਨਾਮ"

"username" : "ਈਮੇਲ"

"password" : "Passwort"

"store_username" : "Nick"

"username" : "E-Mail"

"password" : "Парола"

"store_username" : "Прякор"

"username" : "Имейл"

"nothing_inserted_user" : "โปรดใส่ชื่อผู้ใช้และรูปภาพ(ทางเลือก)เพื่อสร้างโปรไฟล์ของคุณ"

"password" : "รหัสผ่าน"

"recover_password" : "รื้อฟื้นรหัสผ่านของคุณ"

"social_timeline_users_private" : "%dเป็นส่วนตัว"

"store_username" : "ชื่อเล่น"

"store_username" : "ชื่อเล่น"
"username" : "อีเมล"
"password" : "Salasana"
"store_username" : "Nimimerkki"
"username" : "Sähköposti"
"password" : "पासवर्ड"
"store_username" : "उपनाम"
"store_username" : "Nickname"
"password" : "Пароль"
"store_username" : "Псевдонім"
"store_username" : "Ψευδώνυμο"
"username" : "Email"
"password" : "Wachtwoord"
"store_username" : "Weergavenaam"
"username" : "E-mail"
"password" : "Hasło"
"store_username" : "Pseudonim"
"username" : "Email"

"password" : "পাসওয়ার্ড"

"store_username" : "ডাকনাম"

"username" : "ইমেইল"

"username" : "Email"

"password" : "패스워드"

"store_username" : "별명"

"username" : "이메일"

"password" : "Parolă"

"store_username" : "Pseudonim"

"username" : "E-mail"

"store_username" : "Pseudo"

"username" : "Email"

"password" : "पासवर्ड"

"username" : "इमेल"

"password" : "Lozinka"

"store_username" : "Nadimak"

"username" : "E-pošta"

"password" : "Šifre"

"password" : "şifre"
"username" : "E-posta"
"password" : "Contraseña"
"store_username" : "Apodo"
"username" : "E-mail"
"username" : "E-mel"
"password" : "Password"
"store_username" : "Nickname"
"password" : "Palavra-passe"
"store_username" : "Alcunha"
"username" : "E-mail"
"password" : "Jelszó"
"store_username" : "Becenév"
"username" : "E-mail"
"password" : "Пароль"
"store_username" : "Никнейм"
"username" : "E-mail"
"password" : "လျှို့ဝှက်စကားလုံး"

"store_username" : "အမည္ေပ်ာက္"

"username" : "အီးေမးလ္"

"com_facebook_device_auth_instructions" : "请访问facebook.com/device并输入以上验证码。"

"nothing_inserted_user" : "请插入昵称和照片（可选）以创建资料"

"password" : "密码"

"recover_password" : "找回密码"

"store_username" : "昵称"

"username" : "电子邮件"

"password" : "Palavra-passe"

"store_username" : "Apelido"

"username" : "E-mail"

"com_facebook_device_auth_instructions" : "前往facebook.com/device</b&gt，並輸入上方顯示的代碼。"

"password" : "密碼"

"recover_password" : "尋回您的密碼"

"store_username" : "Nickname"

"username" : "電子郵件"

"com_facebook_device_auth_instructions" : "前往facebook.com/device</b&gt，並輸入上方顯示的代碼。"

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
1b2ec33c1a5a485bb7b111d41f17e0f8
2OUUc7NT0WkEjmK9+FJMealFwLTaZNBfYG9mkUVQmhidcpLE5upPJKg2uqM0WUBe
3pegtvj7nkb7e3rwh5b+3dnQATJj6aqtaosJ3DkOYPzNGN2w+CoarbJEsY1UQgeA
E112a13984c2eF19DBeE98E3eDa79e90DB51f0e6
5e8f16062ea3cd2c4a0d547876baa6f38cabf625
Bl3RSPeFXX48+A41tWFMGRj6+1eT4NHtkwATNUdtNkM=
RDFKlEPOT0aQT6ARmaMKbVy+V0L7x+JIeY4JSh39pzY=
e3NEybi6UG3v8IfP2IiRsp6KKM0H99WDhy4AYfUmNolCq+mgpr0V0zn7xdgcLXPM
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
bfce038c5ef7f0c99d0a6317a549edf0
Tx+r89A46YvA23pzmXogrUOA3X/vGVWSwDDb1CKb3SB+k9Zvmo8EcgSe2zWDveRy
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18=
ubLcgigmx4nAmM3gRNIgYeeALxilkZ+lc3aGgQ+rkRY=

pORZNbNq0Oj61ZjvW9kWzatiK7LMxOR6JjGIN24dRVcLieCRVYuov8581WrmSeOY
ace60f6352f6dd9289843b5b0b2ab3d4
r05ido8PpVZ2h2V1HWb8y18UjWvZxnyZOvYK4Y06JVkYZsi7FS/S9aZJacgWNWb+
UZJDjsNp1+4M5x9cbbdflB779y5YRBcV6Z6rBMLIrO4=
RLH60+LqkTN+fFoMkyZr3rdaQt8CbwdFGeiAHk8G/Y1GpQIgUmMEvr7Qzmd4S0T8
3CA30A86d04e65E6E388922deCe3eBD0F100F5d0
3ad378b027fe45aa8bfbc5bacf56344e
kd3av/xIh4WVmhBCVqo9sHJVJ1Nfp9EEBESbqmCB4V8=
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
Wd8xe/qfTwq3ylFNd3IpaqLHZbh2ZNCLluVzmeNkcpw=
gjATLq4PR4tBy0NKJBUs0hq7sitSgRlGcsdxPuImAoM=
pJdDeMB2kv4XBHX5K3sZ2yiaFa+GF7/AJrrVARYf41I=
308203643082024ca0030201020204503fc625300d06092a864886f70d0101050500307331 0b3009060355040613027074311030 0e0603550408130755 6e6b6e6f776e310f300d060355040713064c6973626f6e3115301306035504 0a130c436169786120 4d6167696361311030 0e060355040b13074170746f6964653118301606035504031 30f44756172746 52053696c766596972613020170d313230383330313935393335a180f32303934313031393139353933335a3073310b3009060355040613027074311030 0e060355040813075 56e6b6e6f776e310f300d060355040713064c6973626f6e3115301306035504 0a130c4361697861204d6167696361311030 0e060355040b13074170746f6964653118301606035 50403130f447561727465 2053696c766596972613082012230 0d06092a864886f70d01010105000382010f003082010a0282010100a7032cb40819b62cd596bc1c121951724e9a7 d6612222d63dab58a18970339f77911b8e2a0665aa15efb051d4dd710c99e1fcaea006a651b7c113a71649c315e27122b9e0a214a240f34559394cca116c609d5bbf670ed85c7b9 83f0026154278bffd2b53d8aea4735ed99c39ea45db004c16bee078bb0b40e38ae510cacd1955a4e3eb90347d344cdcce07bddb89d9cd2077558914179a8157a87eac86e1b1a0 7a3f697a5f3f6512e276741d76bcc0c4809117c279fbd55d8c2b3d70468fbe4869394d9f2740bcccdf727da10c06de5c6a0d2f893bce078e058604726d32ab17e3b113a3dcbe0c22f
2532738cae8cc5fa98c6b8306680b07ef8f0fca5d5910b0203010001300d06092a864886f70d0101050500038201010036115 2e42ece11bfd72e5795c9e91079b39c5280e30e339

4671ca108fd7de9c3ebef2fc2f5ba752664ba44fcddaf49e91a1d7683cafdc11275fa7c1487ae78a659a8dae5d696cd93de810c67f12756bdfab0c1962ec5ad2a3ea056bf75ad4a2ea9d388d4497b561242f090de2d3347dd32494ba6305735fa21d82f037f4355583fdfb1f46a56c19526969ba5f7f556cca9b9069cd9a9e3cd566d2b8c33138609e8794fb0abb11d33ed2c507f7f7df9ce24b3b64713ccdf2450bb5ec4efedba541dce271c8b3759b340b0467c06624cd3881b769a1d4a1b1fc0bec97d6b8561b032089ab8ca108595759bbd9b95fd43a3d28f518fb9d193125c8fa9b224f831c
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
9b8f518b086098de3d77736f9458a3d2f6f95a37
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
B3EEABB8EE11C2BE770B684D95219ECB
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
IIJxA/RzEPbEgRJQH0LQ8KVHKqG3NyhvdpUemJxyiMg=
DRYWi0TWx0xeQUvY98UNqkz37+DffrKoPBm+2dnlFUG6mCEAnCrfVx/sGMEehzhv
1db8206f0da6aa81bbdd2d99a82d9e14
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
SgMhksOnpMJMBH1JH74BErFMAiPE78L9kUpiye6ezUkIKoc+RVuDLvEf36QK5tpM
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
zu6uZ8u7nNJHsIXbotuBCEBd9hieUh9UBKC94dMPsF422AtJb3FisPSqZI3W+06A
3jRp5GOI+HfffIZaNgs5urp4INMy6m1jZanprlp8fEbfjaITI/GTtSmO29P018Ft
tJgqVBYK8iACgXDpES6chgsdiLTk4pCmM15TE0z3kgM=
WPHSlfekhaYlGJ3yiaIbiBY4HTx7YM9tPghNjV2alPYI+KXTjj+VnW7A1O7Euzu8
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3

9bH7YEZYe5itvs31c1gcj+rhSSdPNkSIQfDNYXo9ahs=

6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

FfddiHmPb383DV6rreW8JKkRsedppg8iNKEfTaDysv4=

lQFXQNWHSdYD6r5tE84uy22hnfx5d1uQHcaULCOPbM14F5cpADjDJSLZMM39MwXu

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

syWhPUhrPj9a+Sk0yzwWVrNh+MlfsynriPZ0XF+UPwU=

j+Yj7UMoEzr9M6nnqL4N+TgP7ihZaPMbtnYW3NPxsNU=

919afcc635fd11ea817c025656b09b22

BYT/lgG9eBlnAgDZzPD0oHgzdaaxxy72moL0pisX7NM=

308205653082034ca00302010202044df76b53300d06092a864886f70d0101050500307331 0b3009060355040613027074311030 0e06035504081307556e6b6e6f776e310f300d060355040713064c6973626f6131153013060355040a130c4361697861204d6167696361311030 0e060355040b1307556e6b6e6f776e311830160603550403130f4475617274652053696c7665697261302022300d06092a864886f70d01010105000382020f003082020a02820201026cfe7512fa0c40520971ee83e227208e072a1e1962a4fd0cd5c709e33dc45ce856e9ddc2b9a918394e96ec462d5fea2db81c443b9dbedd75a1031a1f1593b86eef83302f9ecdc0dfd227a3e11ccedb056e58c79b9177dbefba122a390dac88a90a317cb55a9171ab428b46c2e29b5d7fef2e823f5985b9c165a1edba7c82b4f8d5e3aa346996019cb8b7bcc768f5fdae15975add5e53c1fc022e4c99dababf3a80c5a09680ba4b8889cc4399940d92d11c289268d3f2671b98f871964f21c5870d9a1c72c8fbea65a637a06643f246e733fff37b7db4020fd2b6e7343fdbac2ddd20f8a48710d944d8f76432a3225f72c6a50c4e76247fb9256f294eeb9e24080ad28094fbfcfa6e4b5a85d652b1c5d967b39ee1272955a134a0ff1e89bb01f98d710204c72ca4c9dd44ecdd81358a8ef920fa371edd1bfc097c81678aa31b059b9218eba5c0ed2c209bd799a3ecab19e5e3b0e3d18029bf156b37e091969b4e5ae5024475b038b4d841e0e88580fd433154f606f1f7c14527f00509dd7448911e1ec44cb1e94f7dce59459e95438c4a245103d14fff047f97d14bf38f1802d84727b0f3aa98e02e8840892c629e303f76965e186de1d92263ec17e35aa224c33856d59095cf9195042ebfb5fd4703ef8add7ccf923640f266c22e432232f5c6b0873d99ebd509f9e66a77506eabef04ae1d9cf5edb40e13bc1cff39917da8b70203010001300d06092a864886f70d01010505000382020200069a29624d30983fdec4c4bf685f2f479214fda52e272a74ae8aee8bc7aae441ba79977cdd251cf5b21c56ee631dd1e17da28a2bd87d1190b4c1cc440140251e38af40aa694e6d3965c31b36ade9deccde0ca403639031f44f42e395b575a125cd210fd54e9ac760af1ed72c7b91f8f771074f6cafe0d28ab840510ee98a46eb84225be218ff6f90d036f47ec2e7dbfa067e9498cc633e5cab354ab86013b4d8047312643cdfbb6b3654dc26a87af0f4d83b2b0c6ad28d026483788daeda241c8e2631311e0e0d48c6f9284904cc4df114336c207e4c4f468f80f82f2d6917d8ec6b9e63fa2a0f126f668f8220667c92d26d55b5da7a4144b8693c0dec479a3c63b1d43eb96868eac1cb786e2f4b327bad553fc9ffe2dada3ab11bd6b1d7a623a92e821192b0dbcdabf0e4c361561bb5abb970d11e477050d56957fc8961106d2aaf1f209cbdde733a7a6e0577fd35d32f048e887b0e92c94

15871e5b0d7458fe682256494b6c9443d04a076842d56374ee4c184a5c64a71c6818eafaa6dcbd66aae917907080d4895b7b0c941a4fae00be891666c0bdeb8b9331d0ff61d7ec

2c26b8015baab4263e925dc9d8427 9bdb1e27e0403b57c14a1b2647a98c858ee20c92b967fb1eb96314 7e390958e7c914fce69e1e2eb061392 79b70a8eeabe9950ddd04223c3 343e5c9b2722635856c65593aae9d2dbf3da704f79e8145f008e
KF7kIGwoAULxxzCbY3v7c6qTHz0AzEhtAn+fEEmtiVY=
JbQbUG5JMJUoI6brnx0x3vZF6jilxsapbXGVfjhN8Fg=
SVqWumuteCQHvVIaALrOZXuzVVVeS7f4FGxxu6V+es4=
B9q/kZ3M4smaULlSVckwEJdUNHNhTESXBf44c8ZRnHeQQYAcBESnaqAhjIPahrI0
uUwZgwDOxcBXrQcntwu+kYFpkiVkOaezL0WYEZ3anJc=
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
Rd5vBa3cRt13XnZUPrTszYMRTqEgpzuKs4niQNpf2R+gTE/2OPB9o8u+o5NCRvjI
jtcoe3puh462k3igthcrkmi918i30edh47c1tksma0pe1uqmuhc2o7i3g7ansalg
0ccb1b4967115d54d18138b4f6c7c9ca
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
7VR2YqvFgyvOhGA7139KYJuSHHdzdCxudZ7JSzwex/E=
tm6XtP5M5qvCs+TffoCZhF/AF3Fx7Ow8iqgApPbgXSw=
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
c84d23ade98552f1cec71088c1f0794c
mfDIsnw62VUq5CrwQygwwDHX4oFb9NZomMa1Qv0blGOGPAtzm7d2+whMgYfVEkXw
3ps9rI142V56fUZ22VD6Aav/U6wPd6aBlBvFChUyHGs=
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
1OoeMBy/0f4cuo3Q6fO79anCMG2ySlElR0298tBh7pCa++J4MQSzo8NUX4DLdHow
SJ3SRTdt7T2FQX1UH4DWlnlLfmao1u+KeMI8XtxEgmSHdfgiJRyy0Txw8FmQ+pQw
3noVyuO3zFOuhvGfjg9nuflidaw0HmgQ5EVdw6MbLqs=
cc2751449a350f668590264ed76692694a80308a
Y/1pb58VeX4F8K6fayOs4meS93jwIQ+AMpk0KVFaduEwXDgWis9Z812p7+pIfyJn
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
305bdd41-271f-4618-a1ea-0793da9e04ef
cAajgxHlj7GTSEIzIYIQxmEloOSoJq7VOaxWHfv72QM=

Report Generated by - MobSF v3.9.4 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.