

ANDROID STATIC ANALYSIS REPORT



Remitly (6.28.1)

File Name:	Remitly.apk
Package Name:	com.remitly.androidapp
Scan Date:	Nov. 14, 2024, 8:35 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	8/432

FINDINGS SEVERITY

ॠ HIGH	▲ MEDIUM	i INFO	✓ SECURE	® HOTSPOT
4	20	4	4	3

FILE INFORMATION

File Name: Remitly.apk

Size: 49.47MB

MD5: 34fbfb2305c596e4bc28e6540b74e7b7

SHA1: 5e67031b51190ff2421b3a8f092463aae985ec9d

\$HA256: c5f46f092578e0f913fbb2ccb88409e170a2f5757089985a7d29d54ab2381377

i APP INFORMATION

App Name: Remitly

Package Name: com.remitly.androidapp

Main Activity: com.remitly.androidapp.MainActivity

Target SDK: 34 Min SDK: 26 Max SDK:

Android Version Name: 6.28.1

EE APP COMPONENTS

Activities: 27 Services: 22 Receivers: 16 Providers: 14

Exported Activities: 3
Exported Services: 2
Exported Receivers: 2
Exported Providers: 0

***** CERTIFICATE INFORMATION

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

X.509 Subject: C=US, ST=Wa, L=Seattle, O=Remitly

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2013-07-26 01:11:02+00:00 Valid To: 2038-07-20 01:11:02+00:00 Issuer: C=US, ST=Wa, L=Seattle, O=Remitly

Serial Number: 0x51f1cca6 Hash Algorithm: sha1

md5: 5e00c29efbcce07c633418506cfab146

sha1: 1e6a71c6b1105d22840c29a311cfd59d5077552e

sha256: 048b6bf833c839e994829caac6a640cc51d395996b2defa8414516635c5d6869

sha512: 6c16c82cf5a4afc8b2f0b243da49f5aaafad5233206898018f1a0526b8ca8e2ad19d2a3d672a37158bf3bc4d8ec9e0f85fca72bb54683240d430cca51dc1403b

PublicKey Algorithm: rsa

Bit Size: 1024

Fingerprint: 7828a891a75e6ebaa09217c058198fb4e997c04d0edfd7c31c0ac627a5f51cb7

Found 1 unique certificates

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.

PERMISSION	STATUS	INFO	DESCRIPTION
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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_REMOTE_MESSAGING	normal	allows foreground services for remote messaging.	Allows a regular application to use Service.startForeground with the type "remoteMessaging".
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.remitly.androidapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

M APKID ANALYSIS

FILE	DETAILS		
34fbfb2305c596e4bc28e6540b74e7b7.apk	FINDINGS	DETAILS	
341b1b2505c550c4bc20c0340b74c7b7.apk	Anti-VM Code	possible VM check	

FILE	DETAILS		
	FINDINGS	DETAILS	
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check network operator name check ro.kernel.qemu check possible ro.secure check	
classes.dex	Compiler	r8	

FILE	DETAILS	
	FINDINGS	DETAILS
classes2.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Obfuscator	unreadable field names
	Compiler	r8 without marker (suspicious)

FILE	DETAILS		
	FINDINGS	DETAILS	
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check network operator name check	
classes3.dex	Compiler	r8 without marker (suspicious)	
	FINDINGS	DETAILS	
classes4.dex	Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.TAGS check possible ro.secure check	
	Compiler	r8 without marker (suspicious)	

FILE	DETAILS	
	FINDINGS	DETAILS
classes5.dex	Anti-VM Code	Build.MANUFACTURER check possible ro.secure check
	Compiler	r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.remitly.androidapp.MainActivity	Schemes: remitly://, https://, Hosts: remitly.onelink.me, remitlypreprod.onelink.me,
com.plaid.internal.LinkRedirectActivity	Schemes: plaid://, Hosts: complete, redirect, resume,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.remitly.androidapp,
net.openid.appauth.RedirectUriReceiverActivity	Schemes: remitly.auth://,



NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

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

Q MANIFEST ANALYSIS

HIGH: 0 | WARNING: 9 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	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.
2	Activity (com.plaid.internal.LinkRedirectActivity) 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.
3	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
4	Activity (net.openid.appauth.RedirectUriReceiverActivity) 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	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	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.
7	TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity)	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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	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.
9	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.

</> CODE ANALYSIS

HIGH: 2 | WARNING: 10 | INFO: 3 | SECURE: 3 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ch/qos/logback/classic/joran/action/Configur ationAction.java ch/qos/logback/classic/sift/ContextBasedDisc

				riimiator.java
NO	ISSUE	SEVERITY	STANDARDS	ch/qos/logback/core/CoreConstants.java ch/qos/logback/core/net/ssl/SSL.java
				ch/qos/logback/core/rolling/helper/DateToke
				nConverter.java
				ch/qos/logback/core/rolling/helper/IntegerTo
				kenConverter.java
				com/amplitude/reactnative/AmplitudeReactN ativeModule.java
				com/appsflyer/reactnative/RNAppsFlyerConst
				ants.java
				com/braze/configuration/BrazeConfig.java
				com/braze/enums/CardKey.java
				com/bugsnag/android/EventFilenameInfo.jav
				a
				com/bugsnag/android/SessionFilenameInfo.j
				ava
				com/klarna/mobile/sdk/core/ui/dialog/Dialog
				Abstraction.java
				com/newrelic/agent/android/SavedState.java
				com/newrelic/agent/android/distributedtraci
				ng/TracePayload.java
				com/newrelic/agent/android/harvest/AgentH
				ealth.java
				com/newrelic/agent/android/harvest/Harvest
				Configuration.java
				com/newrelic/agent/android/util/Constants.ja
				va
				com/newrelic/agent/android/util/PersistentU
				UID.java
				com/onfido/android/sdk/capture/common/p
				ermissions/PermissionsManagementFragmen
				t.java
				com/onfido/android/sdk/capture/core/config
				/FlowFragment.java
				com/onfido/android/sdk/capture/internal/an
				alytics/inhouse/domain/AnalyticsPropertyKey
				s.java
				com/onfido/android/sdk/capture/internal/an
				alytics/inhouse/trackers/NfcEvents.java
			CWE: CWE-312: Cleartext Storage of Sensitive	com/onfido/android/sdk/capture/internal/ui/
	<u>Files may contain hardcoded</u>		La Constantina	to the second of

1	sensitive information like usernames,	warning	miormation	countryselection/CountryselectionFragment.j
NO	Sensitive information like discrimines,	SEVERITY	SWAND AR 19: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	គីវីដ៏ES com/onfido/android/sdk/capture/internal/util
				/logging/RemoteLoggerTree.java
				com/onfido/android/sdk/capture/token/Toke
				nExpirationHandlerService.java
				com/onfido/android/sdk/capture/ui/camera/
				CaptureActivity.java
				com/onfido/android/sdk/capture/ui/camera/l
				QSUploadErrorParser.java
				com/onfido/android/sdk/capture/ui/camera/
	_			selfie/SelfieCaptureViewModel.java
				com/onfido/android/sdk/capture/ui/nfc/NfcD
				eviceNotSupportedFragment.java
				com/onfido/android/sdk/capture/ui/nfc/NfcS
				canFailFragment.java
				com/onfido/android/sdk/capture/ui/nfc/scan
				/NfcCanEntryFragment.java
				com/onfido/android/sdk/capture/ui/nfc/scan
				/NfcScanFragment.java
				com/onfido/android/sdk/capture/ui/proofOf
				Address/host/PoaHostFragment.java
				com/onfido/api/client/data/NfcProperties.jav
				a
				com/plaid/internal/core/crashreporting/inter
				nal/models/CrashApiOptions.java
				com/plaid/internal/core/crashreporting/inter
	_			nal/models/User.java
	_			com/plaid/internal/g1.java
				com/salesforce/android/chat/core/internal/fil
				etransfer/FileUploadRequestComposer.java
				com/salesforce/android/service/common/live
				agentclient/request/LiveAgentRequest.java
				fg/b.java
				gg/e.java
				gg/w.java
				gm/RefreshPayload.java
				gm/RegisterPayload.java
				h4/ImageRequest.java
				h4/Parameters.java
	1			h4/i.java

NO	ISSUE	SEVERITY	STANDARDS	IS/ImmutableConfig.java pVEpt y.java org/jmrtd/lds/PACEDomainParameterInfo.jav
				a p3/Preference.java
2	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	om/a.java siftscience/android/DevicePropertiesCollector .java
3	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/bugsnag/android/RootDetector.java eg/i.java mf/w.java om/b.java siftscience/android/DevicePropertiesCollector .java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	fj/a.java hb/b.java org/ejbca/cvc/CVCObjectIdentifiers.java org/jmrtd/lds/ActiveAuthenticationInfo.java org/jmrtd/lds/CardSecurityFile.java org/jmrtd/lds/SODFile.java org/jmrtd/lds/SecurityInfo.java org/jmrtd/lds/SignedDataUtil.java w9/a.java xb/a.java xb/f.java xb/g.java xb/m.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	a6/b.java bo/app/cg0.java bo/app/e50.java bo/app/fv.java bo/app/gy.java bo/app/hr.java bo/app/jr.java bo/app/jr.java bo/app/jr.java bo/app/la0.java bo/app/re0.java bo/app/re0.java bo/app/xs.java bo/app/xs.java bo/app/xs.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/managers/BrazeGeofenceManager.java com/klarna/mobile/sdk/core/io/assets/util/AssetsUtil.java com/remitly/rnappconfig/b.java f9/d0.java u5/j.java
				a2/c.java b3/e.java bd/f0.java bg/g.java c1/d.java cd/b1.java cd/e1.java

NO	ISSUE	SEVERITY	STANDARDS	cd/g1.java Ed ៤ គ្រីស a
				ch/gos/logback/classic/android/LogcatAppen
				der.java
				ch/qos/logback/classic/net/SimpleSocketServ
				er.java
				ch/qos/logback/classic/pattern/TargetLength
				BasedClassNameAbbreviator.java
				ch/qos/logback/classic/spi/ThrowableProxy.ja
				va
				ch/qos/logback/core/joran/util/Configuration
				WatchListUtil.java
				ch/qos/logback/core/net/DefaultSocketConne
				ctor.java
				ch/qos/logback/core/net/SocketConnectorBas
				e.java
				ch/qos/logback/core/recovery/ResilientOutpu
				tStreamBase.java
				ch/qos/logback/core/spi/ContextAwareBase.j
				ava
				ch/qos/logback/core/spi/ContextAwareImpl.ja
				va
				ch/qos/logback/core/subst/Node.java com/airbnb/android/react/lottie/LottieAnimat
				ionViewManager.java
				com/appsflyer/internal/AFb1vSDK.java
				com/appsflyer/internal/AFc1qSDK.java
				com/appsflyer/internal/AFf1hSDK.java
				com/appsflyer/internal/AFf1jSDK.java
				com/appsflyer/internal/AFf1kSDK.java
				com/bugsnag/android/j1.java
				com/newrelic/agent/android/AndroidAgentIm
				pl.java
				com/newrelic/agent/android/ApplicationExit
				Monitor.java
				com/newrelic/agent/android/NewRelic.java
				com/newrelic/agent/android/SavedState.java
				com/newrelic/agent/android/agentdata/Agent
				DataController.java
				com/newrelic/agent/android/analytics/Analyti

NO	ISSUE	SEVERITY	STANDARDS	csControllerImpl.java Fdhr Sewrelic/agent/android/analytics/Event ManagerImpl.java
6	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/newrelic/agent/android/crash/Uncaught ExceptionHandler.java com/newrelic/agent/android/harvest/Harvest .java com/newrelic/agent/android/hybrid/data/Dat aController.java com/newrelic/agent/android/instrumentation /LogInstrumentation.java com/newrelic/agent/android/instrumentation /io/CountingInputStream.java com/newrelic/agent/android/logging/Android AgentLog.java com/newrelic/agent/android/logging/Console AgentLog.java com/newrelic/agent/android/logging/LogFor warder.java com/newrelic/agent/android/logging/LogRep orter.java com/newrelic/agent/android/logging/LogRep orting.java com/newrelic/agent/android/logging/Logger.j ava com/newrelic/agent/android/logging/Logger.j ava com/newrelic/agent/android/sample/Sampler .java com/newrelic/agent/android/stores/SharedPr efsAnalyticsAttributeStore.java com/newrelic/agent/android/tracing/ActivityT race.java com/newrelic/agent/android/tracing/ActivityT race.java com/newrelic/agent/android/tracing/TraceMa chine.java com/newrelic/agent/android/tracing/TraceMa chine.java com/newrelic/agent/android/sdk/capture/internal/util /logging/Timber.java com/onfido/android/sdk/capture/internal/util /logging/Timber.java com/onfido/reactnative/sdk/OnfidoSdkModul

NO	ISSUE	SEVERITY	STANDARDS	e.java பெட்டு aid/PlaidModule\$onActivityResult\$link
	 			Handler\$1.java
ļ				com/plaid/PlaidModule\$onActivityResult\$link
ļ				Handler\$2.java
ļ				com/plaid/internal/y1.java
ļ				com/salesforce/android/service/common/util
ļ				ities/lifecycle/LifecycleEvaluator.java
ļ				com/salesforce/android/service/common/util
ļ				ities/lifecycle/LifecycleMetricWatcher.java
ļ				com/salesforce/android/service/common/util
ļ				ities/lifecycle/LifecycleStateWatcher.java
ļ				d0/a0.java
ļ				d1/c.java
ļ				d1/k.java
ļ				d1/l.java
ļ				d2/a.java
ļ				e3/m.java
ļ				es/e.java
ļ				f0/d.java
ļ				f1/f.java
ļ				fd/a.java
ļ				g2/d.java
ļ				gn/g.java
ļ				h1/a.java
ļ				h1/b.java
ļ				h1/c.java
ļ				h2/a.java
l				i2/a.java
ļ				ic/a.java
ļ				ie/a.java
ļ				j3/a.java
ļ				jd/n.java
ļ				jd/o.java
ļ				ke/a.java
ļ				kl/c.java
ļ				le/a.java
ļ				m1/d.java
ļ				mf/i.java
ļ				ne/b.java
ļ		1		

NO	ISSUE	SEVERITY	STANDARDS	ne/j0.java 6le/E Sca/cvc/example/FileHelper.java org/ejbca/cvc/example/GenerateCert.java
				org/ejbca/cvc/example/GenerateRequest.java
				org/ejbca/cvc/example/Parse.java
				org/slf4j/helpers/r.java
				os/g.java
				p1/c.java
				qf/n0.java
				r/r0.java
				r2/j.java
				s2/d.java
				sr/a.java
				t2/a.java
				ur/c.java
				v3/d.java
				w2/a.java
				w3/o.java
				w5/m.java
				x0/b.java
				x2/m0.java
				zc/a0.java
				zc/c.java
				zc/j.java

zc/t.java zc/x.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	ch/qos/logback/classic/android/SQLiteAppen der.java com/newrelic/agent/android/instrumentation /SQLiteInstrumentation.java com/plaid/internal/workflow/persistence/dat abase/WorkflowDatabase_Impl.java com/reactnativecommunity/asyncstorage/a.ja va com/reactnativecommunity/asyncstorage/f.ja va com/reactnativecommunity/asyncstorage/ne xt/StorageDb_Impl.java com/reactnativecommunity/asyncstorage/ne xt/a.java mc/m0.java mc/t0.java s2/c.java
8	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/w30.java com/appsflyer/internal/AFa1zSDK.java com/appsflyer/internal/AFb1hSDK.java com/appsflyer/internal/AFc1fSDK.java com/braze/support/IntentUtils.java com/newrelic/agent/android/util/Util.java hs/d.java hs/h.java jm/d.java org/jmrtd/lds/CBEFFDataGroup.java org/jmrtd/protocol/BACProtocol.java v8/t0.java zo/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/mrousavy/camera/o.java com/mrousavy/camera/p.java com/mrousavy/camera/q.java com/onfido/android/sdk/capture/internal/ca mera/Camera1Api.java com/onfido/android/sdk/capture/internal/ca mera/VideoFileBuilder.java com/onfido/android/sdk/capture/utils/FileUti ls.java com/reactnativecommunity/webview/RNCWe bViewModule.java e6/a.java t/u.java zg/c.java
10	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	ch/qos/logback/core/android/AndroidContext Util.java com/newrelic/agent/android/AndroidAgentIm pl.java com/reactnativecommunity/cameraroll/Came raRollModule.java com/reactnativecommunity/webview/RNCWe bViewModule.java com/salesforce/android/chat/ui/internal/filetr ansfer/ImageContentResolver.java e6/a.java io/invertase/firebase/utils/ReactNativeFirebas eUtilsModule.java p6/a.java v8/t0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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/bugsnag/android/j0.java e9/a.java org/jmrtd/protocol/EACCAProtocol.java org/jmrtd/protocol/EACTAProtocol.java s6/c.java zg/b.java
12	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ch/qos/logback/core/net/ssl/SSLContextFacto ryBean.java com/onfido/api/client/OnfidoFetcher.java ds/c.java ds/d.java ds/i.java ds/j.java nm/h.java
13	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFb1vSDK.java
14	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/klarna/mobile/sdk/core/ui/dialog/intern albrowser/BaseInternalBrowserDialogFragme nt.java com/plaid/internal/c1.java com/plaid/internal/yf.java mk/c.java
15	This app has capabilities to prevent tapjacking attacks.	secure	OWASP MASVS: MSTG-PLATFORM-9	com/remitly/androidapp/x.java
16	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/reactnativecommunity/clipboard/Clipbo ardModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
17	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/plaid/internal/i8.java com/plaid/internal/pf.java
18	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/braze/support/StringUtils.java com/remitly/rnappconfig/b.java o5/e.java w5/m.java

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
				5250 1.0.t

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	bo/app/hr.java com/amplitude/reactnative/a.java com/appsflyer/internal/AFh1cSDK.java com/newrelic/agent/android/util/Connectivity.java siftscience/android/DevicePropertiesCollector.java tb/i.java v8/t0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00065	Get the country code of the SIM card provider	collection	siftscience/android/DevicePropertiesCollector.java
00162	Create InetSocketAddress object and connecting to it	socket	com/newrelic/agent/android/util/Reachability.java ds/b.java ds/j.java
00163	Create new Socket and connecting to it	socket	com/newrelic/agent/android/util/Reachability.java ds/b.java ds/j.java
			a6/a.java bo/app/pr.java bo/app/pr.java bo/app/wc0.java c3/a.java c6/b.java ch/qos/logback/core/joran/GenericConfigurator.java ch/qos/logback/core/joran/action/PropertyAction.java ch/qos/logback/core/rolling/helper/Compressor.java ch/qos/logback/core/util/FileUtil.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1nSDK.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/bugsnag/android/RootDetector.java com/bugsnag/android/i3.java com/bugsnag/android/t1.java com/microsoft/codepush/react/j.java com/microsoft/codepush/react/n.java com/newrelic/agent/android/logging/LogReporter.java com/newrelic/agent/android/util/Streams.java com/onfido/android/sdk/capture/utils/yearclass/DeviceInfo.java

d file and put it into a stream HAVIOUR	file LABEL	com/reactnativecommunity/asyncstorage/c.java com/reactnativecommunity/cameraroll/CameraRollModule.java FILES eg/a0.java
HAVIOUR	LABEL	Ell EC
		l eg l'alo. ava
		fg/f.java
		jg/e.java
		I5/k.java
		l8/d.java
		lb/t.java
		lg/a.java
		o5/g.java
		okio/OkioJvmOkioKt.java
		org/ejbca/cvc/example/FileHelper.java
		p2/b.java
		r1/m.java
		t/u.java
		tb/j.java
		to/k.java
		v8/k0.java
		w4/g.java
		w4/h.java
		w5/m.java
		wb/d.java
		ws/a.java
		x5/j.java
		x8/k.java
		x9/a.java
		zg/c.java
		bo/app/bj0.java
		bo/app/ea.java
		bo/app/fa.java
		bo/app/gp.java
		bo/app/yd0.java
		bo/app/zc.java
		ch/qos/logback/classic/android/SQLiteAppender.java
		ch/qos/logback/core/FileAppender.java
		ch/qos/logback/core/android/AndroidContextUtil.java
		ch/qos/logback/core/rolling/helper/Compressor.java
		ch/qos/logback/core/rolling/helper/FileFinder.java
		ch/qos/logback/core/rolling/helper/RenameUtil.java
		com/appsflyer/internal/AFg1nSDK.java

			com/braze/e0.java
RULE			
ID	BEHAVIOUR	LABEL	com/braze/support/BrazeImageUtils.java FILES com/braze/support/WebContentUtils.java
וט			com/bugsnag/android/n1.java
			com/bugsnag/android/ndk/NativeBridge.java
			com/bugsnag/android/s.java
			com/klarna/mobile/sdk/core/io/assets/manager/wrapper/index/KpWrapperManager.java
			com/microsoft/codepush/react/a.java
			com/microsoft/codepush/react/j.java
			com/microsoft/codepush/react/k.java
			com/microsoft/codepush/react/n.java
			com/mrousavy/camera/p.java
			com/mrousavy/camera/q.java
			com/newrelic/agent/android/logging/LogForwarder.java
	Open a file from given absolute path		com/newrelic/agent/android/logging/LogReporter.java
00022	of the file	file	com/newrelic/agent/android/ndk/AgentNDK.java
			com/newrelic/agent/android/ndk/ManagedContext.java
			com/newrelic/agent/android/util/OfflineStorage.java
			com/onfido/android/sdk/capture/component/active/video/capture/presentation/capture/c
			amera/camera2/recorder/RecorderWrapperCommon.java
			com/onfido/android/sdk/capture/internal/camera/Camera1Api.java
			com/onfido/android/sdk/capture/internal/camera/camerax/CameraXTakeVideoUseCase.ja
			va
			com/onfido/android/sdk/capture/ui/camera/view/CameraSourcePreview.java
			com/onfido/android/sdk/capture/utils/ImageUtils.java
			com/reactnativecommunity/cameraroll/CameraRollModule.java
			e6/f.java
			fg/f.java
			io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java
			j6/c.java
			m4/m.java
			of/f.java
			of/k.java
			of/o.java
			p6/a.java
			qf/g.java
			r1/m.java
			s2/d.java
			t/u.java
			v3/d.java
1	I	1	

RULE ID	BEHAVIOUR	LABEL	v3/f.java v3/g.java FILES w4/g.java w4/h.java
00096	Connect to a URL and set request method	command network	ah/c.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1sSDK.java com/newrelic/agent/android/agentdata/AgentDataSender.java com/newrelic/agent/android/harvest/HarvestConnection.java com/plaid/internal/e.java com/plaid/internal/o1.java mb/c.java q5/g.java siftscience/android/Uploader.java w4/b.java
00030	Connect to the remote server through the given URL	network	com/appsflyer/internal/AFb1uSDK.java com/plaid/internal/e.java siftscience/android/Uploader.java w4/b.java
00014	Read file into a stream and put it into a JSON object	file	a6/a.java com/appsflyer/internal/AFg1nSDK.java fg/f.java lg/a.java x5/j.java x8/k.java x9/a.java zg/c.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFg1nSDK.java com/microsoft/codepush/react/k.java fg/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1;SDK.java com/appsflyer/internal/AFc1;SDK.java com/appsflyer/internal/AFc1;SDK.java com/braze/Braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/inappmessage/views/InAppMessageHtmlBaseView.java com/braze/ui/support/UriUtils.java com/braze/ui/support/UriUtils.java com/klarna/mobile/sdk/core/natives/browser/SandboxBrowserController.java com/klarna/mobile/sdk/core/natives/browser/SandboxBrowserController.java com/klarna/mobile/sdk/core/natives/delegates/ExternalAppDelegate.java com/klarna/mobile/sdk/core/util/platform/IntentUtils.java com/klarna/mobile/sdk/core/util/platform/UriUtils.java com/plaid/internal/link/LinkActivity.java com/plaid/internal/kk.java com/plaid/internal/kh.java com/remitly/androidapp/receivers/BrazeBroadcastReceiver.java com/rappauth/RNAppAuthModule.java com/salesforce/android/chat/ui/internal/chatfeed/viewholder/ReceivedLinkPreviewMessag eViewHolder.java f9/c.java kl/c.java net/openid/appauth/c.java v3/a.java v8/b.java v8/b.java v8/b.java v8/b.java v8/b.java v8/b.java v8/b.java v8/y0.java v8/y0.java v8/y0.java v8/y0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	ah/c.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/bugsnag/android/g0.java com/microsoft/codepush/react/h.java com/newrelic/agent/android/harvest/HarvestConnection.java com/plaid/internal/e.java com/plaid/internal/o1.java e9/c.java mb/c.java q5/g.java siftscience/android/Uploader.java
00012	Read data and put it into a buffer stream	file	ch/qos/logback/core/rolling/helper/Compressor.java ch/qos/logback/core/util/FileUtil.java com/microsoft/codepush/react/n.java com/onfido/android/sdk/capture/ui/proofOfAddress/documentSubmission/PoaDocument SubmissionViewModel.java o5/g.java w5/m.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1jSDK.java com/braze/push/BrazeNotificationUtils.java com/braze/reactbridge/BrazeReactBridgeImpl.java com/onfido/android/sdk/capture/ui/OnfidoActivity.java com/onfido/android/sdk/capture/ui/OnfidoSplashActivity.java com/onfido/android/sdk/capture/ui/camera/CaptureActivity.java com/plaid/internal/ih.java com/remitly/androidapp/auth/AuthModule.java f9/i0.java net/openid/appauth/AuthorizationManagementActivity.java v8/m0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	b6/a.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1sSDK.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java com/reactnativecommunity/toolbarandroid/b.java e4/c.java kl/c.java la/a.java v3/d.java v8/b.java v8/t0.java v8/t0.java v8/u0.java
00202	Make a phone call	control	com/plaid/internal/link/LinkActivity.java
00203	Put a phone number into an intent	control	com/plaid/internal/link/LinkActivity.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/plaid/internal/link/LinkActivity.java kl/c.java v8/t0.java v8/u0.java w3/h.java
00026	Method reflection	reflection	pp/a.java pp/b.java
00183	Get current camera parameters and change the setting.	camera	com/getbouncer/scan/camera/Camera1Adapter.java com/onfido/android/sdk/capture/ui/camera/view/CameraSource.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	ah/c.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFc1sSDK.java com/appsflyer/internal/AFc1sSDK.java com/appsflyer/internal/AFc1osDK.java com/appsflyer/internal/AFc1osDK.java com/bugsnag/android/g0.java com/newrelic/agent/android/agentdata/AgentDataSender.java com/newrelic/agent/android/crash/CrashSender.java com/newrelic/agent/android/harvest/HarvestConnection.java com/plaid/internal/e.java com/plaid/internal/o1.java mb/c.java q5/g.java rc/d.java siftscience/android/Uploader.java xc/f.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java com/reactnativecommunity/cameraroll/CameraRollModule.java v3/d.java
00015	Put buffer stream (data) to JSON object	file	v8/t0.java
00009	Put data in cursor to JSON object	file	com/amplitude/reactnative/b.java com/reactnativecommunity/asyncstorage/a.java v8/t0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1qSDK.java com/reactnativecommunity/cameraroll/CameraRollModule.java v8/b.java v8/m0.java v8/t0.java
00056	Modify voice volume	control	com/onfido/android/sdk/capture/audio/VolumeManager.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/salesforce/android/chat/ui/internal/filetransfer/ContentQueryHelper.java s6/f.java v8/m0.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/salesforce/android/chat/ui/internal/filetransfer/ContentQueryHelper.java s6/f.java v8/m0.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java com/reactnativecommunity/cameraroll/CameraRollModule.java v8/m0.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFi1oSDK.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/salesforce/android/chat/ui/internal/filetransfer/ContentQueryHelper.java s6/f.java v8/m0.java

RULE ID	BEHAVIOUR	LABEL	FILES	
00187	Query a URI and check the result	collection sms calllog calendar	com/reactnativecommunity/cameraroll/CameraRollModule.java com/salesforce/android/chat/ui/internal/filetransfer/ContentQueryHelper.java v8/m0.java	
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFi1oSDK.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/salesforce/android/chat/ui/internal/filetransfer/ContentQueryHelper.java s6/f.java v8/m0.java	
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java com/reactnativecommunity/cameraroll/CameraRollModule.java v8/m0.java	
00175	Get notification manager and cancel notifications	com/salesforce/android/service/common/utilities/internal/android/notification/ NotificationManager.java		
00024	Write file after Base64 decoding reflection file v3/f.java v3/g.java			
00004	Get filename and put it to JSON object	file collection	b9/a.java x5/f.java x8/c.java	
00125	Check if the given file path exist	file	com/onfido/android/sdk/capture/ui/camera/liveness/LivenessConfirmationFragment.java com/onfido/android/sdk/capture/ui/proofOfAddress/documentSubmission/PoaDocument SubmissionFragment.java x5/f.java	

RULE ID	BEHAVIOUR	LABEL	FILES	
00123	Save the response to JSON after connecting to the remote server	network command	com/appsflyer/internal/AFb1uSDK.java net/openid/appauth/h.java	
00043	Calculate WiFi signal strength	collection wifi	ql/e.java	
00094	Connect to a URL and read data from it	command network	com/newrelic/agent/android/harvest/HarvestConnection.java com/plaid/internal/e.java ig/a.java siftscience/android/Uploader.java	
00108	Read the input stream from given URL	network command	com/newrelic/agent/android/harvest/HarvestConnection.java com/newrelic/agent/android/payload/PayloadSender.java com/plaid/internal/e.java siftscience/android/Uploader.java	
00003	Put the compressed bitmap data into JSON object	camera	r5/l.java	
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/reactnativecommunity/cameraroll/CameraRollModule.java	
00033	Query the IMEI number	collection	com/newrelic/agent/android/util/PersistentUUID.java	
00195	Set the output path of the recorded file	record file	com/onfido/android/sdk/capture/component/active/video/capture/presentation/capture/c amera/camera2/recorder/RecorderWrapperCommon.java	
00199	Stop recording and release recording resources	record	com/onfido/android/sdk/capture/component/active/video/capture/presentation/capture/c amera/camera2/recorder/RecorderWrapperCommon.java com/onfido/android/sdk/capture/ui/camera/view/CameraSource.java	

RULE ID	BEHAVIOUR	LABEL	FILES
00198	Initialize the recorder and start recording	record	com/onfido/android/sdk/capture/component/active/video/capture/presentation/capture/c amera/camera2/recorder/RecorderWrapperCommon.java com/onfido/android/sdk/capture/ui/camera/view/CameraSource.java
00194	Set the audio source (MIC) and recorded file format	record	com/onfido/android/sdk/capture/component/active/video/capture/presentation/capture/c amera/camera2/recorder/RecorderWrapperCommon.java com/onfido/android/sdk/capture/ui/camera/view/CameraSource.java
00197	Set the audio encoder and initialize the recorder	record	com/onfido/android/sdk/capture/component/active/video/capture/presentation/capture/c amera/camera2/recorder/RecorderWrapperCommon.java com/onfido/android/sdk/capture/ui/camera/view/CameraSource.java
00007	Use absolute path of directory for the output media file path	file	com/onfido/android/sdk/capture/component/active/video/capture/presentation/capture/c amera/camera2/recorder/RecorderWrapperCommon.java
00196	Set the recorded file format and output path	record file	com/onfido/android/sdk/capture/component/active/video/capture/presentation/capture/c amera/camera2/recorder/RecorderWrapperCommon.java com/onfido/android/sdk/capture/ui/camera/view/CameraSource.java
00114	Create a secure socket connection to the proxy address	network command	yr/f.java
00072	Write HTTP input stream into a file	command network file	com/microsoft/codepush/react/h.java mb/c.java
00132	Query The ISO country code	telephony collection	com/amplitude/reactnative/a.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/onfido/android/sdk/capture/utils/ImageUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES	
00002	Open the camera and take picture camera		com/onfido/android/sdk/capture/ui/camera/view/CameraSource.java	
00039	39 Start a web server control network		ch/qos/logback/classic/net/SimpleSocketServer.java	

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://beamitmobile-com-remitly.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/946464332815/namespaces/firebase:fetch? key=AlzaSyCKGTQx5GFsYMzVcCmxCWbpot40gA2a950. This is indicated by the response: The response code is 403

***: ::** ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.VIBRATE, android.permission.READ_PHONE_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	6/44	android.permission.FLASHLIGHT, com.google.android.gms.permission.AD_ID, android.permission.CHANGE_NETWORK_STATE, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, 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	
plaid.com	IP: 52.84.45.79 Country: Hong Kong Region: Hong Kong City: Hong Kong	
app.singpass.gov.sg	IP: 52.84.45.78 Country: Hong Kong Region: Hong Kong City: Hong Kong	

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
plaid.com	ok	IP: 52.84.45.79 Country: Hong Kong Region: Hong Kong City: Hong Kong Latitude: 22.285521 Longitude: 114.157692 View: Google Map
accounts.google.com	ok	IP: 108.177.119.84 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.remitly.com	ok	IP: 54.193.60.70 Country: United States of America Region: California City: San Francisco Latitude: 37.774929 Longitude: -122.419418 View: Google Map
smonitorsdk.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
app.singpass.gov.sg	ok	IP: 52.84.45.78 Country: Hong Kong Region: Hong Kong City: Hong Kong Latitude: 22.285521 Longitude: 114.157692 View: Google Map
cards.remitly.io	ok	IP: 54.183.60.27 Country: United States of America Region: California City: San Francisco Latitude: 37.774929 Longitude: -122.419418 View: Google Map
dust.k8s.test-001.d-usw-2.braze.com	ok	No Geolocation information available.
frontend-event-router-eu.staging.c2c.klarna.net	ok	IP: 10.164.43.163 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
api.onfido.com	ok	IP: 18.161.97.119 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
svalidate.s	ok	No Geolocation information available.
schemas.android.com	ok	No Geolocation information available.
pagead2.googlesyndication.com	ok	IP: 142.250.187.98 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
clients3.google.com	ok	IP: 216.58.214.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
bugsnag.com	ok	IP: 3.164.182.112 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.singpassmobile.sg	ok	IP: 104.21.74.144 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
mock.base.url	ok	No Geolocation information available.
www.w3.org	ok	IP: 104.18.22.19 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
github.com	ok	IP: 140.82.121.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
sars.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
production.plaid.com	ok	IP: 100.26.69.162 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
efr.remitly.com	ok	IP: 52.42.40.38 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
twitter.com	ok	IP: 104.244.42.1 Country: United States of America Region: California City: San Francisco Latitude: 37.773968 Longitude: -122.410446 View: Google Map
react-native-vision-camera.com	ok	IP: 76.76.21.9 Country: United States of America Region: California City: Walnut Latitude: 34.015400 Longitude: -117.858223 View: Google Map
iamcache.braze	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sattr.s	ok	No Geolocation information available.
api.remitly.io	ok	IP: 54.219.144.103 Country: United States of America Region: California City: San Francisco Latitude: 37.774929 Longitude: -122.419418 View: Google Map
www.braze.com	ok	IP: 104.17.227.60 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
scdn-ssettings.s	ok	No Geolocation information available.
auth.remitly.com	ok	IP: 54.176.231.18 Country: United States of America Region: California City: San Francisco Latitude: 37.774929 Longitude: -122.419418 View: Google Map

DOMAIN	STATUS	GEOLOCATION
facebook.com	ok	IP: 157.240.9.35 Country: Bulgaria Region: Sofia (stolitsa) City: Sofia Latitude: 42.697510 Longitude: 23.324150 View: Google Map
issuetracker.google.com	ok	IP: 172.217.169.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.facebook.com	ok	IP: 157.240.9.35 Country: Bulgaria Region: Sofia (stolitsa) City: Sofia Latitude: 42.697510 Longitude: 23.324150 View: Google Map
device.payfone.com	ok	IP: 74.63.181.56 Country: United States of America Region: North Carolina City: Charlotte Latitude: 35.137260 Longitude: -80.936119 View: Google Map
graph-video.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
slaunches.s	ok	No Geolocation information available.
codepush.appcenter.ms	ok	IP: 52.232.227.249 Country: United States of America Region: Virginia City: Boydton Latitude: 36.667641 Longitude: -78.387497 View: Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
docs.bugsnag.com	ok	IP: 3.160.196.129 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
graph.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
.facebook.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developers.facebook.com	ok	IP: 157.240.9.18 Country: Bulgaria Region: Sofia (stolitsa) City: Sofia Latitude: 42.697510 Longitude: 23.324150 View: Google Map
docs.google.com	ok	IP: 142.251.141.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
validate.remitly.io	ok	IP: 54.183.60.27 Country: United States of America Region: California City: San Francisco Latitude: 37.774929 Longitude: -122.419418 View: Google Map
development.plaid.com	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
beamitmobile-com-remitly.firebaseio.com	ok	IP: 34.120.206.254 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
cdn.plaid.com	ok	IP: 52.222.144.109 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map
x.klarnacdn.net	ok	IP: 3.164.85.15 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
parasol.remitly.io	ok	IP: 54.219.144.103 Country: United States of America Region: California City: San Francisco Latitude: 37.774929 Longitude: -122.419418 View: Google Map

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	ok	IP: 142.250.187.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
dashboard.plaid.com	ok	IP: 3.164.85.90 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
plus.google.com	ok	IP: 142.250.184.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
sessions.bugsnag.com	ok	IP: 35.190.88.7 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	IP: 142.251.140.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
api.getbouncer.com	ok	No Geolocation information available.
notify.bugsnag.com	ok	IP: 35.186.205.6 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
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
sdlsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sandbox.plaid.com	ok	IP: 54.161.141.215 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
sviap.s	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
api3.siftscience.com	ok	IP: 35.244.208.123 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
xml.org	ok	IP: 104.239.240.11 Country: United States of America Region: Texas City: Windcrest Latitude: 29.499678 Longitude: -98.399246 View: Google Map

DOMAIN	STATUS	GEOLOCATION
sdk.onfido.com	ok	IP: 54.230.112.33 Country: France Region: Provence-Alpes-Cote-d'Azur City: Marseille Latitude: 43.296951 Longitude: 5.381070 View: Google Map
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
simpression.s	ok	No Geolocation information available.
logback.qos.ch	ok	IP: 159.100.250.151 Country: Switzerland Region: Vaud City: Lausanne Latitude: 46.515999 Longitude: 6.632820 View: Google Map
klarna.com	ok	IP: 99.83.187.101 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	IP: 172.217.169.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
sinapps.s	ok	No Geolocation information available.
analytics.plaid.com	ok	IP: 34.225.228.255 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
sconversions.s	ok	No Geolocation information available.
firebase-settings.crashlytics.com	ok	IP: 142.250.187.131 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	IP: 195.15.222.169 Country: Switzerland Region: Basel-Stadt City: Basel Latitude: 47.558399 Longitude: 7.573270 View: Google Map
eu.klarnaevt.com	ok	IP: 54.229.255.134 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190 View: Google Map
assets.onfido.com	ok	IP: 216.137.52.84 Country: Japan Region: Tokyo City: Tokyo Latitude: 35.689507 Longitude: 139.691696 View: Google Map
sregister.s	ok	No Geolocation information available.
pinterest.com	ok	IP: 151.101.128.84 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map



EMAIL	FILE
■ @- ■ a. ■ b	com/plaid/internal/core/protos/clients/LinkCustomizations\$LinkCustomization.java
this@cardverifyactivity.applicatio	com/getbouncer/cardverify/ui/zerofraud/CardVerifyActivity.java
android-sdk@onfido.com	com/onfido/android/sdk/capture/OnfidoImpl\$handleActivityResult\$corruptedResultCallback\$1.java

A TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Bugsnag	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/207
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

TRACKER	CATEGORIES	URL
New Relic	Analytics	https://reports.exodus-privacy.eu.org/trackers/130

HARDCODED SECRETS

POSSIBLE SECRETS	
"cardverify_api_key" : "xTnj2GbVivwn_G0w6dzvzFP1mnG4PQs0"	
"code_push_deployment_key" : "p-pSurQhF84AREfEywnK8BhkPcTTB1xxcZ0JQ"	
"com.google.firebase.crashlytics.mapping_file_id" : "0d4b88dcb3fc46de87adaea9fe5a9bef"	
"com_braze_api_key" : "818c726e-fc41-4e1c-8338-93700222690d"	
"com_braze_firebase_cloud_messaging_sender_id" : "946464332815"	
"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"	
"facebook_client_token" : "b9fb8be3d10cf726be600c55875ff473"	
"firebase_database_url" : "https://beamitmobile-com-remitly.firebaseio.com"	
"google_api_key" : "AlzaSyCKGTQx5GFsYMzVcCmxCWbpot40gA2a950"	

POSSIBLE SECRETS "google_crash_reporting_api_key": "AlzaSyCKGTQx5GFsYMzVcCmxCWbpot40gA2a950" "plaid_sentry_android_link_sdk_api_key": "e7bf46248ac14774aecfe3a24811e6b4" "shared_prefs_app_id_key_klarna_inapp_sdk": "sdk-application-id" 0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D 28091019353058090096996979000309560759124368558014865957655842872397301267595 10099790675505530477208181553592522486984108257205345787482351587557714799052927277724415285269929879648335669968284202797289605274717 31754805904856071347468521419286809125615028022221856475391909026561163678472701450190667942909301854462163997308722217328898303231940 97355403213400972588322876850946740663962 0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD33 6747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928 0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C8 13F0DF45BE8112F4 0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01 7B425ED097B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864 030024266E4EB5106D0A964D92C4860E2671DB9B6CC5 3826F008A8C51D7B95284D9D03FF0E00CE2CD723A

D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27

13407807929942597099574024998205846127479365820592393377723561443721764030073546976801874298166903427690031858186486050853753882811946 569946433649006084095

A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353

55066263022277343669578718895168534326250603453777594175500187360389116729240

7503CFE87A836AE3A61B8816E25450E6CE5E1C93ACF1ABC1778064FDCBEFA921DF1626BE4FD036E93D75E6A50E3A41E98028FE5FC235F5B889A589CB5215F2A4

04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34

MQVwithSHA512KDFAndSharedInfo

e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe 9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf

127971af8721782ecffa3

020A601907B8C953CA1481EB10512F78744A3205FD

91771529896554605945588149018382750217296858393520724172743325725474374979801

c49d360886e704936a6678e1139d26b7819f7e90

040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883

EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15 DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3

DB7C2ABF62F35F668076BFAD208B

POSSIBLE SECRETS	
79885141663410976897627118935756323747307951916507639758300472692338873533959	
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773	
324A6EDDD512F08C49A99AE0D3F961197A76413E7BE81A400CA681E09639B5FE12E59A109F78BF4A373541B3B9A1	
c56fb7d591ba6704df047fd98f535372fea00211	
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374	
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0	
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	
044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32	
e8b4011604095303ca3b8099982be09fcb9ae616	
005DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2	
68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43	
7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9	
b28ef557ba31dfcbdd21ac46e2a91e3c304f44cb87058ada2cb815151e610046	
D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311	

POSSIBLE SECRETS
9162fbe73984472a0a9d0590
040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD
6BA06FE51464B2BD26DC57F48819BA9954667022C7D03
BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985
00E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B
FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A
4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F
E95E4A5F737059DC60DF5991D45029409E60FC09
13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79
3FA8124359F96680B83D1C3EB2C070E5C545C9858D03ECFB744BF8D717717EFC
1E589A8595423412134FAA2DBDEC95C8D8675E58
0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1
F5CE40D95B5EB899ABBCCFF5911CB8577939804D6527378B8C108C3D2090FF9BE18E2D33E3021ED2EF32D85822423B6304F726AA854BAE07D0396E9A9ADDC40F
046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
714114B762F2FF4A7912A6D2AC58B9B5C2FCFE76DAEB7129

POSSIBLE SECRETS	
D2C0FB15760860DEF1EEF4D696E6768756151754	
5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B	
255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e	
10938490380737342745111123907668055699362075989516837489945863944959531161507350160137087375737596232485921322967063133094384525315910 12912142327488478985984	
2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B	
70390085352083305199547718019018437840920882647164081035322601458352298396601	
115792089237316195423570985008687907853269984665640564039457584007908834671663	
026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D	
c48a5844dd44e9362f76f04c757515f7f65870e480a748828caeef19c03da586	
5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72	
42941826148615804143873447737955502392672345968607143066798112994089471231420027060385216699563848719957657284814898909770759462613437 66945636488273037083893479108083593264797677860191534347440096103423131667257868692048219493287863336020338479709268434224762105576023 5016132614780652761028509445403338652341	
5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557	
687D1B459DC841457E3E06CF6F5E2517B97C7D614AF138BCBF85DC806C4B289F3E965D2DB1416D217F8B276FAD1AB69C50F78BEE1FA3106EFB8CCBC7C5140116	
04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5	

POSSIBLE SECRETS	
6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40	
31a92ee2029fd10d901b113e990710f0d21ac6b6	
04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9l	
E2E31EDFC23DE7BDEBE241CE593EF5DE2295B7A9CBAEF021D385F7074CEA043AA27272A7AE602BF2A7B9033DB9ED3610C6FB85487EAE97AAC5BC7928C1950148	
14201174159756348119636828602231808974327613839524373876287257344192745939351271897363116607846760036084894662356762579528277471921224 19290710461342083806363940845126918288940005715246254452957693493567527289568315417754417631393844571917550968471078465956625479423122 93338483924514339614727760681880609734239	
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF	
9B9F605F5A858107AB1EC85E6B41C8AACF846E86789051D37998F7B9022D759B	
b8adf1378a6eb73409fa6c9c637ba7f5	
0217C05610884B63B9C6C7291678F9D341	
662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04	
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3	
9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DC F028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C4866 772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB	
5D9306BACD22B7FAEB09D2E049C6E2866C5D1677762A8F2F2DC9A11C7F7BE8340AB2237C7F2A0	
2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC	

POSSIBLE SECRETS	
7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee	
2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE	
00E8BEE4D3E2260744188BE0E9C723	
28792665814854611296992347458380284135028636778229113005756334730996303888124	
0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205	
b05e367cc67e6caaadf5a14d5c557670	
26617408020502170632287687167233609607298591687569731477066713684188029449964278084915450806277719023520942412250655586621571135455709 16814161637315895999846	
00E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D	
7fmduHKTdHHrlMvldlEqAllSfii1tl35bxj1OXN5Ve8c4lU6URVu4xtSHc3BVZxS6WWJnxMDhlfQN0N0K2NDJg==	
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00	
74D59FF07F6B413D0EA14B344B20A2DB049B50C3	
023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10	
68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633211138647686124403 80340372808892707005449	
216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA	
ea51ca5c693a4b8733b1cf1a63557a713a13fabf0bcb724385077694e63a51a7	

5F49EB26781C0EC6B8909156D98ED435E45FD59918

a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc 036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536 57896044618658097711785492504343953927102133160255826820068844496087732066703 C196BA05AC29E1F9C3C72D56DFFC6154A033F1477AC88EC37F09BE6C5BB95F51C296DD20D1A28A067CCC4D4316A4BD1DCA55ED1066D438C35AEBAABF57E7DAE4 28782A95ECA1C143DB701FD48533A3C18F0FE23557EA7AE619ECACC7E0B51652A8776D02A425567DED36EABD90CA33A1E8D988F0BBB92D02D1D20290113BB562C E1FC856EEB7CDD92D33EEA6F410859B179E7E789A8F75F645FAE2E136D252BFFAFF89528945C1ABE705A38DBC2D364AADE99BE0D0AAD82E5320121496DC65B3930 E38047294FF877831A16D5228418DE8AB275D7D75651CEFED65F78AFC3EA7FE4D79B35F62A0402A1117599ADAC7B269A59F353CF450E6982D3B1702D9CA83 51DEF1815DB5ED74FCC34C85D709 046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C B99B99B099B323E02709A4D696E6768756151751 1053CDE42C14D696E67687561517533BF3F83345 MQVwithSHA384KDFAndSharedInfo d67afc830dab717fd163bfcb0b8b88423e9a1a3b B10B8F96A080E01DDE92DE5EAE5D54EC52C99FBCFB06A3C69A6A9DCA52D23B616073E28675A23D189838EF1E2EE652C013ECB4AEA906112324975C3CD49B83BFAC CBDD7D90C4BD7098488E9C219A73724EFFD6FAE5644738FAA31A4FF55BCCC0A151AF5F0DC8B4BD45BF37DF365C1A65E68CFDA76D4DA708DF1FB2BC2E4A4371

072546B5435234A422E0789675F432C89435DE5242

033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097

0667ACEB38AF4E488C407433FFAE4F1C811638DF20

0693bf1962715e32f8d85ffefd8be9971d84ed554f25f4060aca2ca1f82c955b

29C41F568B77C617FFF5902F11DB96FA9613CD8D03DB08DA

cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953

4E13CA542744D696E67687561517552F279A8C84

C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297

POSSIBLE SECRETS b3fb3400dec5c4adceb8655d4c94 DB7C2ABF62E35E668076BEAD2088 9b8f518b086098de3d77736f9458a3d2f6f95a37 0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C AC4032EF4F2D9AE39DF30B5C8FFDAC506CDEBE7B89998CAF74866A08CFE4FFE3A6824A4E10B9A6F0DD921F01A70C4AFAAB739D7700C29F52C57DB17C620A8652BE 5E9001A8D66AD7C17669101999024AF4D027275AC1348BB8A762D0521BC98AE247150422EA1ED409939D54DA7460CDB5F6C6B250717CBEF180EB34118E98D11952 9A45D6F834566F3025F316A330FFBB77A86F0C1AB15B051AF3D428C8F8ACB70A8137150B8FFB10F183FDD19963DDD9F263F4770589FF6AA21F7F5F2FF381B539CCF 3409D13CD566AFBB48D6C019181E1BCFE94B30269EDFE72FE9B6AA4BD7B5A0F1C71CFFF4C19C418E1F6EC017981BC087F2A7065B384B890D3191F2BFA 115792089237316195423570985008687907853269984665640564039457584007913129639316 03375D4CE24FDE434489DE8746E71786015009E66E38A926DD D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F 0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA 9C77877AAAC6AC7D35245D1692E8EE1 b956059a88e9dfb420dc5fb101fd3156 DC9203E514A721875485A529D2C722FB187BC8980EB866644DE41C68E143064546E861C0E2C9EDD92ADE71F46FCF50FF2AD97F951FDA9F2A2EB6546F39689BD3 02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7 0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB

043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE

790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16

64033881142927202683649881450433473985931760268884941288852745803908878638612

29818893917731240733471273240314769927240550812383695689146495261604565990247

96341f1138933bc2f503fd44

27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575

0123456789abcdefABCDEF

5EEEFCA380D02919DC2C6558BB6D8A5D

3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723

038D16C2866798B600F9F08BB4A8E860F3298CE04A5798

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

a4739fa49caa3ff88e7ff1145c9334ee4cbf64354e91131d02d98d7bfd4c35cf

5E5CBA992E0A680D885EB903AEA78E4A45A469103D448EDE3B7ACCC54D521E37F84A4BDD5B06B0970CC2D2BBB715F7B82846F9A0C393914C792E6A923E2117AB8 05276A975AADB5261D91673EA9AAFFEECBFA6183DFCB5D3B7332AA19275AFA1F8EC0B60FB6F66CC23AE4870791D5982AAD1AA9485FD8F4A60126FEB2CF05DB8A7F 0F09B3397F3937F2E90B9E5B9C9B6EFEF642BC48351C46FB171B9BFA9EF17A961CE96C7E7A7CC3D3D03DFAD1078BA21DA425198F07D2481622BCE45969D9C4D606 3D72AB7A0F08B2F49A7CC6AF335E08C4720E31476B67299E231F8BD90B39AC3AE3BE0C6B6CACEF8289A2E2873D58E51E029CAFBD55E6841489AB66B5B4B9BA6E2F 784660896AFF387D92844CCB8B69475496DE19DA2E58259B090489AC8E62363CDF82CFD8EF2A427ABCD65750B506F56DDE3B988567A88126B914D7828E2B63A6D7 ED0747EC59E0E0A23CE7D8A74C1D2C2A7AFB6A29799620F00E11C33787F7DED3B30E1A22D09F1FBDA1ABBBFBF25CAE05A13F812E34563F99410E73B

0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05

883423532389192164791648750360308885314476597252960362792450860609699839

115792089210356248762697446949407573529996955224135760342422259061068512044369

3071c8717539de5d5353f4c8cd59a032

1b9fa3e518d683c6b65763694ac8efbaec6fab44f2276171a42726507dd08add4c3b3f4c1ebc5b1222ddba077f722943b24c3edfa0f85fe24d0c8c01591f0be6f63

26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6

FFFFFFE0000000075A30D1B9038A115

3E1AF419A269A5F866A7D3C25C3DF80AE979259373FF2B182F49D4CE7E1BBC8B

04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD

91A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20

A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377

CFA0478A54717B08CE64805B76E5B14249A77A4838469DF7F7DC987EFCCFB11D

2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988

7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826

12702124828893241746590704277717644352578765350891653581281750726570503126098509849742318833348340118092599999512098893413065920561499 67242541210492743493570749203127695614516892241105793112488126102296785346384016935200132889950003622606842227508135323070045173416336 85004541062586971416883686778842537820383

0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9

9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511

010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967

04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3

10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1

0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D

06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA936ECE454D2C

985BD3ADBAD4D696E676875615175A21B43A97E3

7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE

027d29778100c65a1da1783716588dce2b8b4aee8e228f1896

37a6259cc0c1dae299a7866489dff0bd

04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD4 2A5A0989D1EE71B1B9BC0455FB0D2C3

1243ae1b4d71613bc9f780a03690e

04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7 E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B32 0430C8591984F601CD4C143EF1C7A3

AD107E1E9123A9D0D660FAA79559C51FA20D64E5683B9FD1B54B1597B61D0A75E6FA141DF95A56DBAF9A3C407BA1DF15EB3D688A309C180E1DE6B85A1274A0A66 D3F8152AD6AC2129037C9EDEFDA4DF8D91E8FEF55B7394B7AD5B7D0B6C12207C9F98D11ED34DBF6C6BA0B2C8BBC27BE6A00E0A0B9C49708B3BF8A317091883681 286130BC8985DB1602E714415D9330278273C7DE31EFDC7310F7121FD5A07415987D9ADC0A486DCDF93ACC44328387315D75E198C641A480CD86A1B9E587E8BE60 E69CC928B2B9C52172E413042E9B23F10B0E16E79763C9B53DCF4BA80A29E3FB73C16B8E75B97EF363E2FFA31F71CF9DE5384E71B81C0AC4DFFE0C10E64F

A4D1CBD5C3FD34126765A442EFB99905F8104DD258AC507FD6406CFF14266D31266FEA1E5C41564B777E690F5504F213160217B4B01B886A5E91547F9E2749F4D7FBD7D3B9A92EE1909D0D2263F80A76A6A24C087A091F531DBF0A0169B6A28AD662A4D18E73AFA32D779D5918D08BC8858F4DCEF97C2A24855E6EEB22B3B2E5

0095E9A9EC9B297BD4BF36E059184F

POSSIBLE SECRETS
023b1660dd701d0839fd45eec36f9ee7b32e13b315dc02610aa1b636e346df671f790f84c5e09b05674dbb7e45c803dd
55eea0d57239a7e92904fb15209963f7236bd06919275bdeb0a765a94b559c97
659EF8BA043916EEDE8911702B22
E95E4A5F737059DC60DFC7AD95B3D8139515620C
04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321
0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B
115792089237316195423570985008687907852837564279074904382605163141518161494337
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294
4D41A619BCC6EADF0448FA22FAD567A9181D37389CA
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
03F7061798EB99E238FD6F1BF95B48FEEB4854252B
8D91E471E0989CDA27DF505A453F2B7635294F2DDF23E3B122ACC99C9E9F1E14
da38f755-c46c-40d3-8300-8285f2e416c2
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

POSSIBLE SECRETS 1AB597A5B4477F59E39539007C7F977D1A567B92B043A49C6B61984C3FE3481AAF454CD41BA1F051626442B3C10 bb85691939b869c1d087f601554b96b80cb4f55b35f433c2 04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB 517cc1b727220a94fe13abe8fa9a6ee0 04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F 8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F E8C2505DEDFC86DDC1BD0B2B6667F1DA34B82574761CB0E879BD081CFD0B6265EE3CB090F30D27614CB4574010DA90DD862EF9D4EBEE4761503190785A71C760 9B9F605F5A858107AB1EC85E6B41C8AA582CA3511EDDFB74F02F3A6598980BB9 520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6 7ffffffffffffffffff800000cfa7e8594377d414c03821bc582063 c469684435deb378c4b65ca9591e2a5763059a2e 1A62BA79D98133A16BBAE7ED9A8E03C32E0824D57AEF72F88986874E5AAE49C27BED49A2A95058068426C2171E99FD3B43C5947C857D 10C0FB15760860DEF1EEF4D696E676875615175D 003088250CA6E7C7FE649CE85820F7 04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA783

24ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706

13407807929942597099574024998205846127479365820592393377723561443721764030073546976801874298166903427690031858186486050853753882811946 569946433649006084096

F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03

64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1

03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012

3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4

0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D

044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97

A59A749A11242C58C894E9E5A91804E8FA0AC64B56288F8D47D51B1EDC4D65444FECA0111D78F35FC9FDD4CB1F1B79A3BA9CBEE83A3F811012503C8117F98E5048 B089E387AF6949BF8784EBD9EF45876F2E6A5A495BE64B6E770409494B7FEE1DBB1E4B2BC2A53D4F893D418B7159592E4FFFDF6969E91D770DAEBD0B5CB14C00AD 68EC7DC1E5745EA55C706C4A1C5C88964E34D09DEB753AD418C1AD0F4FDFD049A955E5D78491C0B7A2F1575A008CCD727AB376DB6E695515B05BD412F5B8C2F4C 77EE10DA48ABD53F5DD498927EE7B692BBBCDA2FB23A516C5B4533D73980B2A3B60E384ED200AE21B40D273651AD6060C13D97FD69AA13C5611A51B9085

00689918DBEC7E5A0DD6DFC0AA55C7

02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7F FEFF7F2955727A

BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F

7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03

04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D

POSSIBLE SECRETS
c84564bf856358fbb2995c962ef5dd4a892dcaa593b61bf540324475db26afef
0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9
801C0D34C58D93FE997177101F80535A4738CEBCBF389A99B36371EB
0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7
2AA058F73A0E33AB486B0F610410C53A7F132310
03E5A88919D7CAFCBF415F07C2176573B2
00F50B028E4D696E676875615175290472783FB1
4D696E676875615175985BD3ADBADA21B43A97E2
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F0
0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B
3086d221a7d46bcde86c90e49284eb153dab
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380
e43bb460f0b80cc0c0b075798e948060f8321b7d

64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1 389C9738-A761-44DE-8A66-1668CFD67DA1 6b8cf07d4ca75c88957d9d670591 6C01074756099122221056911C77D77E77A777E7E7E7F7FCB 68363196144955700784444165611827252895102170888761442055095051287550314083023 0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052 048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F04699 7 BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5 041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD5526 2B70B29FFFC5864F19C054FF99129280F4646217791811142820341263C5315 9CA8B57A934C54DEEDA9E54A7BBAD95E3B2E91C54D32BE0B9DF96D8D35 470fa2b4ae81cd56ecbcda9735803434cec591fa 57896044618658097711785492504343953926634992332820282019728792003956564823190 0091A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20 26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087

D09E8800291CB85396CC6717393284AAA0DA64BA

114ca50f7a8e2f3f657c1108d9d44cfd8

0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F82 27DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892

027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5

A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7

95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706 dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc 73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec 667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b

0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5B D66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD1 6650

39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319

0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92

115792089237316195423570985008687907853073762908499243225378155805079068850323

340282366920938463463374607431768211455

401028774D7777C7B7666D1366EA432071274F89FF01E718

POSSIBLE SECRETS
e973d14c97f1c647a41b0aff5c0c1a26
e4a5c87c-2ed8-52a7-abcc-2fad074ef6f0
0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521
10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50
04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F
E87579C11079F43DD824993C2CEE5ED3
00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9
00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE
115792089237316195423570985008687907853269984665640564039457584007913129639936
00FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681
BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE
0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166 43812574028291115057148

42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76
137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586
d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b
035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a

340282366920938463463374607431768211456

115792089237316195423570985008687907853269984665640564039457584007913129639935

108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9

4099B5A457F9D69F79213D094C4BCD4D4262210B

01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B

7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA

3FCDA526B6CDF83BA1118DF35B3C31761D3545F32728D003EEB25EFE96

8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a9 78d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f

C2173F1513981673AF4892C23035A27CE25E2013BF95AA33B22C656F277E7335

c2a39c9034a9f0073933488021676c46910cec0d1bf330ac22a908dcd7dd448a

68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166 43812574028291115057151

71FF1AF926CF847989FFFF8DB459F66394D90F32AD3F15F8

POSSIBLE SECRETS
dZozdop5rgKNxjbrQAd5nntAGpgh9w84O1Xgg==
C49D360886E704936A6678E1139D26B7819F7E90
7A1F6653786A68192803910A3D30B2A2018B21CD54
04A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F
60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788
43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64B0C2AFE42CADAB8F93D92394C79A79755437B56995136
115792089210356248762697446949407573530086143415290314195533631308867097853948
002757A1114D696E6768756151755316C05E0BD4
6127C24C05F38A0AAAF65C0EF02C
E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B
04B8266A46C55657AC734CE38F018F2192

12511cfe811d0f4e6bc688b4d

8a3c4b262d721acd49a4bf97d5213199c86fa2b9

04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035D A5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332

044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2

040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150

8d8e3f79aa0783ab0cfa5c8d65d663a9da6ba99401efb2298aaaee387c3b00d6

036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

9B9F605F5A858107AB1EC85E6B41C8AACF846E86789051D37998F7B9022D7598

F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1

0108B39E77C4B108BED981ED0E890E117C511CF072

90066455B5CFC38F9CAA4A48B4281F292C260FEEF01FD61037E56258A7795A1C7AD46076982CE6BB956936C6AB4DCFE05E6784586940CA544B9B2140E1EB523F009
D20A7E7880E4E5BFA690F1B9004A27811CD9904AF70420EEFD6EA11EF7DA129F58835FF56B89FAA637BC9AC2EFAAB903402229F491D8D3485261CD068699B6BA58A
1DDBBEF6DB51E8FE34E8A78E542D7BA351C21EA8D8F1D29F5D5D15939487E27F4416B0CA632C59EFD1B1EB66511A5A0FBF615B766C5862D0BD8A3FE7A0E0DA0FB
2FE1FCB19E8F9996A8EA0FCCDE538175238FC8B0EE6F29AF7F642773EBE8CD5402415A01451A840476B2FCEB0E388D30D4B376C37FE401C2A2C2F941DAD179C540C
1C8CE030D460C4D983BE9AB0B20F69144C1AE13F9383EA1C08504FB0BF321503EFE43488310DD8DC77EC5B8349B8BFE97C2C560EA878DE87C11E3D597F1FEA742D
73EEC7F37BE43949EF1A0D15C3F3E3FC0A8335617055AC91328EC22B50FC15B941D3D1624CD88BC25F3E941FDDC6200689581BFEC416B4B2CB73

02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614

1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F

678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4

004D696E67687561517512D8F03431FCE63B88F4

6277101735386680763835789423207666416083908700390324961279

B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4

db92371d2126e9700324977504e8c90e

3086d221a7d46bcde86c90e49284eb15

0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD

1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

POSSIBLE SECRETS
040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D9 27E1E7769C8EEC2D19037BF27342DA639B6DCCFFFEB73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B 16E2F1516E23DD3C1A4827AF1B8AC15B
70390085352083305199547718019018437841079516630045180471284346843705633502616
91E38443A5E82C0D880923425712B2BB658B9196932E02C78B2582FE742DAA28
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a
020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf

10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618

FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212

4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D

04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886

D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24

F518AA8781A8DF278ABA4E7D64B7CB9D49462353

E95E4A5F737059DC60DFC7AD95B3D8139515620F

B4E134D3FB59EB8BAB57274904664D5AF50388BA

6db14acc9e21c820ff28b1d5ef5de2b0

EE353FCA5428A9300D4ABA754A44C00FDFEC0C9AE4B1A1803075ED967B7BB73F 41058363725152142129326129780047268409114441015993725554835256314039467401291 6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296 71169be7330b3038edb025f1 30470 ad 5a 005 fb 14 ce 2 d 9 d cd 87 e 38 b c 7 d 1 b 1 c 5 fa c baec be 95 f 190 aa 7 a 31 d 23 c 4 d b b c be 06 17 45 44 40 1 a 5 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 36 68 44 577 1 f 7 4 b a 08 4 d 20 29 d 83 c 1 c 15 85 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 36 68 44 577 1 f 7 4 b a 08 4 d 20 29 d 83 c 1 c 15 85 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 36 68 44 577 1 f 7 4 b a 08 4 d 20 29 d 83 c 1 c 15 85 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 36 68 44 577 1 f 7 4 b a 08 4 d 20 29 d 83 c 1 c 15 85 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 36 68 44 577 1 f 7 4 b a 08 4 d 20 29 d 83 c 1 c 15 85 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 36 68 44 577 1 f 7 4 b a 08 4 d 20 29 d 83 c 1 c 15 8 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 36 68 44 577 1 f 7 4 b a 08 4 d 20 29 d 83 c 1 c 15 8 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 36 68 44 577 1 f 7 4 b a 08 4 d 20 29 d 83 c 1 c 15 8 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 36 68 44 577 1 f 7 4 b a 08 4 d 20 29 d 83 c 1 c 15 8 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 36 68 44 577 1 f 7 4 b a 08 4 d 20 29 d 83 c 1 c 15 8 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 36 68 44 577 1 f 7 4 b a 08 4 d 20 29 d 83 c 1 c 15 8 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 36 68 44 577 1 f 7 4 b a 08 4 d 20 29 d 83 c 1 c 15 8 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 36 68 44 577 1 f 7 4 b a 08 4 d 20 29 d 83 c 1 c 15 8 b 2 c 02 09 65 d 8 c 2 b d 217 1 d 20 20 d 217 1 d 218 1 d47f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252 1A8F7EDA389B094C2C071E3647A8940F3C123B697578C213BE6DD9E6C8EC7335DCB228FD1EDF4A39152CBCAAF8C0398828041055F94CEEEC7E21340780FE41BD 040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677 71169be7330b3038edb025f1d0f9 1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1 28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93 22123dc2395a05caa7423daeccc94760a7d462256bd56916

3FB32C9B73134D0B2E77506660EDBD484CA7B18F21EF205407F4793A1A0BA12510DBC15077BE463FFF4FED4AAC0BB555BE3A6C1B0C6B47B1BC3773BF7E8C6F6290 1228F8C28CBB18A55AE31341000A650196F931C77A57F2DDF463E5E9EC144B777DE62AAAB8A8628AC376D282D6ED3864E67982428EBC831D14348F6F2F9193B5045 AF2767164E1DFC967C1FB3F2E55A4BD1BFFE83B9C80D052B985D182EA0ADB2A3B7313D3FE14C8484B1E052588B9B7D2BBD2DF016199ECD06E1557CD0915B3353B BB64E0EC377FD028370DF92B52C7891428CDC67EB6184B523D1DB246C32F63078490F00EF8D647D148D47954515E2327CFEF98C582664B4C0F6CC41659

B4C4EE28CEBC6C2C8AC12952CF37F16AC7EFB6A9F69F4B57FFDA2E4F0DE5ADE038CBC2FFF719D2C18DE0284B8BFEF3B52B8CC7A5F5BF0A3C8D2319A5312557E1

41ECE55743711A8C3CBF3783CD08C0EE4D4DC440D4641A8F366E550DFDB3BB67

 $13353181327272067343385951994831900121794237596784748689948235959936964252873471246159040332773182141032801252925387191478859899310331\\05677441361963648030647213778266568986864684632777101508094011826087702016153249904683329312949209127762411378780302243557466062839716\\59376426832674269780880061631528163475887$

393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB

010092537397FCA4F6145799D62B0A19CF06FF26AD

57896044618658097711785492504343953926634992332820282019728792003956564823193

FFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1 356D6D51C245F485B576625F7FC6F44C42F9A637FD6B0BFF5CB6F406B7FDFF386BFB5A899FA5AF9F24117C4B1FF649286651FCF45B3DC2007CB8A163BF0598DA483 61C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C18 0E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1C BA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86 A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2 699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED 1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DE C9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B3 32051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A9 7A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CC B1A313D55CDA56C9FC2FF29632387FF8D76F3C0468043F8F663F4860FF12BF2D5B0B7474D6F694F91F6DBF115974A3926F12FFF5F438777CB6A932DF8CD8BFC4D07 3B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD922222E04A40 37C0713EB57A81A23F0C73473FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6 A364597E899A0255DC164F31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5EE382

04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811

0257927098FA932F7C0A96D3FD5B706FF7F5F5C156F16B7F7C86038552F91D

8325710961489029985546751289520108179287853048861315594709205902480503199884419224438643760392947333078086511627871

8e722de3125bddb05580164bfe20b8b432216a62926c57502ceede31c47816edd1e89769124179d0b695106428815065

3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1

043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9

AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3

POSSIBLE SECRETS
14518877557776399015115874320830702024226143809848893135505709196593151770659565743590789126541491676439926842369913057775743308316665 11589145701059710742276692757882915756220901998212975756543223550490431013061082131040808010565293748926901442915057819663730454818359 472391642885328171302299245556663073719855
617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c
7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7
D6031998D1B3BBFEBF59CC9BBFF9AEE1
340E7BE2A280EB74E2BE61BADA745D97E8F7C300
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565
07B6882CAAEFA84F9554FF8428BD88E246D2782AE2
4A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11
DB7C2ABF62E35E7628DFAC6561C5
4A6E0856526436F2F88DD07A341E32D04184572BEB710
e4437ed6010e88286f547fa90abfe4c42212
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
115792089210356248762697446949407573530086143415290314195533631308867097853951
07A526C63D3E25A256A007699F5447E32AE456B50E

03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3

24B7B137C8A14D696E6768756151756FD0DA2E5C
7d7374168ffe3471b60a857686a19475d3bfa2ff
10E723AB14D696E6768756151756FEBF8FCB49A9
5FF6108462A2DC8210AB403925E638A19C1455D21
ABi2fbt8vkzj7SJ8aD5jc4xJFTDFntdkMrYXL3itsvqY1Qlw
0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA
FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681
FFFFFFF00000000FFFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
FFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1 356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA483 61C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA237327FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A
8CF83642A709A097B447997640129DA299B1A47D1EB3750BA308B0FE64F5FBD3
48439561293906451759052585252797914202762949526041747995844080717082404635286
115792089237316195423570985008687907853269984665640564039457584007913129639319

2866537B676752636A68F56554E12640276B649EF7526267

9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a

1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10

000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F

00C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E

36134250956749795798585127919587881956611106672985015071877198253568414405109

C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1

03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a

37571800257700204635455072244911836035944551347697624866945677796155444774405563166912344050129455395621444445372894285225856667291965 80810124344277578376784

87A8E61DB4B6663CFFBBD19C651959998CEEF608660DD0F25D2CEED4435E3B00E00DF8F1D61957D4FAF7DF4561B2AA3016C3D91134096FAA3BF4296D830E9A7C20
9E0C6497517ABD5A8A9D306BCF67ED91F9E6725B4758C022E0B1EF4275BF7B6C5BFC11D45F9088B941F54EB1E59BB8BC39A0BF12307F5C4FDB70C581B23F76B63A
CAE1CAA6B7902D52526735488A0EF13C6D9A51BFA4AB3AD8347796524D8EF6A167B5A41825D967E144E5140564251CCACB83E6B486F6B3CA3F7971506026C0B857
F689962856DED4010ABD0BE621C3A3960A54E710C375F26375D7014103A4B54330C198AF126116D2276E11715F693877FAD7EF09CADB094AE91E1A1597

5DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2

2305e610-cd11-4856-a889-c4df218f84ef

fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768

AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E 8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA9 7B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E 7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73

c97445f45cdef9f0d3e05e1e585fc297235b82b5be8ff3efca67c59852018192

32670510020758816978083085130507043184471273380659243275938904335757337482424

0432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0

36DF0AAFD8B8D7597CA10520D04B

6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF

00FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069

04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83

FFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1 82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99 C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6 9FF86D2BC522363A0DABC521979B0DFADA1DBF9A42D5C4484F0ABCD06BFA53DDFF3C1B20FF3FD59D7C25F41D2B669F1FF16F6F52C3164DF4FB7930F9F4F58857B 6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1 A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23 BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855 322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C 1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C 6272B045B3B71F9DC6B80D63FDD4A8F9ADB1F6962A69526D43161C1A41D570D7938DAD4A40F329CCFF46AAA36AD004CF600C8381F425A31D951AF64FDB23FCFC 9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C 35F5C59160CC046FD8251541FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95 F9D5B8019488D9C0A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA 6BBFDF530677F0D97D11D49F7A8443D0822F506A9F4614F011F2A94838FF88CD68C8BB7C5C6424CFFFFFFFFFFFFFFFF

fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7

962eddcc369cba8ebb260ee6b6a126d9346e38c5

70B5E1E14031C1F70BBEFE96BDDE66F451754B4CA5F48DA241F331AA396B8D1839A855C1769B1EA14BA53308B5E2723724E090E02DB9

047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44

6b8cf07d4ca75c88957d9d67059037a4

7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E

021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F

90EAF4D1AF0708B1B612FF35E0A2997EB9E9D263C9CE659528945C0D

POSSIBLE SECRETS
7d73d21f1bd82c9e5268b6dcf9fde2cb
MQVwithSHA256KDFAndSharedInfo
3045AE6FC8422f64ED579528D38120EAE12196D5
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
295F9BAE7428ED9CCC20E7C359A9D41A22FCCD9108E17BF7BA9337A6F8AE9513
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
000E0D4D696E6768756151750CC03A4473D03679
9760508f15230bccb292b982a2eb840bf0581cf5
103FAEC74D696E676875615175777FC5B191EF30
77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE
E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D
8d5155894229d5e689ee01e6018a237e2cae64cd
fffffff00000000ffffffffffffbce6faada7179e84f3b9cac2fc632551
040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E 34116177DD2259
25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E

POSSIBLE SECRETS
0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D
bbbb42d6a8058409381c7dda80a54606
70390085352083305199547718019018437841079516630045180471284346843705633502619
10B7B4D696E676875615175137C8A16FD0DA2211
6EE3CEEB230811759F20518A0930F1A4315A827DAC
00BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE
3045AE6FC8422F64ED579528D38120EAE12196D5
32879423AB1A0375895786C4BB46E9565FDE0B5344766740AF268ADB32322E5C
A335926AA319A27A1D00896A6773A4827ACDAC73
469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9
0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E

cc2751449a350f668590264ed76692694a80308a

0307AF69989546103D79329FCC3D74880F33BBE803CB

D7C134AA264366862A18302575D1D787B09F075797DA89F57FC8C0FF

85E25BFE5C86226CDB12016F7553F9D0E693A268

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

13945487119911582560140965510769071310704170705992803179775800145437576535772298409412436852228823983303911468164807668823692122073732 26721607407477717009111345504320538046476949046861201130878162407401848004770471573366629262494235712488239685422217536601433914856808 40520336859458494803187341288580489525163

POSSIBLE SECRETS
Ht9pXZugT9b7DaEEmPUDgtG7Al3tAQC6J4fyT3TiHDc=
32010857077C5431123A46B808906756F543423E8D27877578125778AC76
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC
02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b5 47c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
1f3bdba585295d9a1110d1df1f9430ef8442c5018976ff3437ef91b81dc0b8132c8d5c39c32d0e004a3092b7d327c0e7a4d26d2c7b69b58f9066652911e457779de
C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E
00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814
c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4
07A11B09A76B562144418FF3FF8C2570B8
0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500
7c5a294ff9a1e665f07d3e64d898062e17a2348f01b0be75b2d5295988ce6a4c
040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACB F04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B

> PLAYSTORE INFORMATION

Title: Remitly: Send Money & Transfer

Score: 4.837788 Installs: 10,000,000+ Price: 0 Android Version Support: Category: Finance Play Store URL: com.remitly.androidapp

Developer Details: Remitly, 7339060940571055726, None, http://www.remitly.com, service@remitly.com,

Release Date: Jul 25, 2013 Privacy Policy: Privacy link

Description:

Join the millions of people who have trusted Remitly since 2011 to send money to friends and family overseas. More money makes it home to loved ones with Remitly's great rates, special offers, and no hidden fees. Use this easy money transfer app and your mobile phone to send money. Transfer money using your bank account, credit card, debit card, with your mobile phone. Download our secure money transfer app and send money to banks and approximately 460,000+ cash pickup locations worldwide. Safe, secure, fast: • Send money with multiple levels of security designed to keep you protected • Have questions? Get quick support in our Help Center or contact us if you need to. We're here to help 24/7. • Get the exact date and time your money transfer will arrive Save money: • Great rates to send money • No fees to receive money • Special offer on your first money transfer Send money transfers worldwide: • Serving 170+ countries worldwide, transfer money safely • Wire funds directly to our mobile money providers, including M-Pesa, MTN, Vodafone, eSewa, GCash, bKash, EasyPaisa, GoPay, and more • Send money transfers to our trusted network of banks, including Bancoppel, BBVA Bancomer, BDO, BPI, Cebuana, Banreservas, GT Bank, Bank Alfalah, Polaris Bank, ICICI, MCB, Habib Bank and more • Send for cash pickup to approximately 460,000+ locations worldwide, including Elektra / Banco Azteca, Caribe Express, Unitransfer, Palawan Pawnshop, OXXO, EbixCash, Punjab National Bank, Weizmann Forex, and more • Send money transfer to: Philippines, India, Vietnam, México, Dominican Republic, Nigeria, Pakistan, China, Ghana, Kenya, Colombia, Brazil, Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Panamá, Ecuador, Peru, Bangladesh, Indonesia, Korea, Nepal, Thailand and more Remitly helps you send money worldwide and pay using your bank account, credit card, or debit card. More money makes it home to friends and family thanks to Remitly's great rates, special offers, and no hidden fees. Remitly uses multiple levels of security designed to keep you protected. We're here to help 24/7. Talk to us or search the Help Center for support in 15 languages. Download the Remitly app and send your money transfer today. Remitly has offices around the globe. Remitly Global, Inc. is located at 1111 Third Avenue, Ste 2100 Seattle, WA 98101. Referrals must be new Remitly users and additional send requirements may be required for rewards to apply. Earn rewards for up to 20 successful referrals. Click here for program details. (https://www.remitly.com/home/referral-program-tnc).

∷ SCAN LOGS

Timestamp	Event	Error
2024-11-14 20:35:54	Generating Hashes	OK

2024-11-14 20:35:54	Extracting APK	ОК
2024-11-14 20:35:54	Unzipping	OK
2024-11-14 20:35:54	Getting Hardcoded Certificates/Keystores	OK
2024-11-14 20:35:54	Parsing APK with androguard	ОК
2024-11-14 20:35:56	Parsing AndroidManifest.xml	ОК
2024-11-14 20:35:56	Extracting Manifest Data	ОК
2024-11-14 20:35:56	Performing Static Analysis on: Remitly (com.remitly.androidapp)	ОК
2024-11-14 20:35:56	Fetching Details from Play Store: com.remitly.androidapp	ОК
2024-11-14 20:35:58	Manifest Analysis Started	OK
2024-11-14 20:35:58	Checking for Malware Permissions	ОК
2024-11-14 20:35:58	Fetching icon path	ОК

2024-11-14 20:35:58	Library Binary Analysis Started	
2024-11-14 20:35:58	Reading Code Signing Certificate	
2024-11-14 20:35:59	Running APKiD 2.1.5	
2024-11-14 20:36:04	Detecting Trackers	
2024-11-14 20:36:08	Decompiling APK to Java with JADX	
2024-11-14 20:36:49	Converting DEX to Smali	
2024-11-14 20:36:49	Code Analysis Started on - java_source	ОК
2024-11-14 20:37:20	Android SAST Completed	
2024-11-14 20:37:20	Android API Analysis Started	
2024-11-14 20:37:33	Android API Analysis Completed	
2024-11-14 20:37:33	Android Permission Mapping Started	ОК

2024-11-14 20:37:59	Android Permission Mapping Completed	
2024-11-14 20:38:05	Email and URL Extraction Completed	
2024-11-14 20:38:05	Android Behaviour Analysis Started	
2024-11-14 20:38:26	Android Behaviour Analysis Completed	
2024-11-14 20:38:26	Extracting String data from APK	
2024-11-14 20:38:26	Extracting String data from Code	
2024-11-14 20:38:26	Extracting String values and entropies from Code	
2024-11-14 20:38:32	Performing Malware check on extracted domains	
2024-11-14 20:39:09	Saving to Database	

Report Generated by - MobSF v4.1.9 $\,$

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

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