MOBSF

ANDROID STATIC ANALYSIS REPORT

Silkmobile (1.4.1)

File Name:	Silkmobile.apk
Package Name:	com.silkbank.silkbankretail
Scan Date:	Nov. 14, 2024, 9:30 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	11	2	2	2

FILE INFORMATION

File Name: Silkmobile.apk
Size: 50.54MB
MD5: 5bd14a63ef504b6248d1081fbf736950
SHA1: 83f5ab7e5d112f621a4bc76415f1b4a0bc3eb693
SHA256: 8a2c823efbb55eeb3e75b03f81a8e50af2163fde018d8003b1dd68faaf2517c1

APP INFORMATION

App Name: Silkmobile
Package Name: com.silkbank.silkbankretail
Main Activity: com.silkbank.silkbankretail.Silkmobile
Target SDK: 33
Min SDK: 19
Max SDK:
Android Version Name: 1.4.1
Android Version Code: 57

APP COMPONENTS

Activities: 9
Services: 3
Receivers: 1
Providers: 2
Exported Activities: 0
Exported Services: 1
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-05-11 07:39:14+00:00
Valid To: 2052-05-11 07:39:14+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x1a481ec167a59db866549cbd7d0b146512228695
Hash Algorithm: sha256
md5: 0c9bb193ed02482e8fb3faadd43225de
sha1: 53ff186a02cdf3ea8df541e44abd5e129ac4724c
sha256: d88b0b031869b58606d1dc33dffdd26f37967bb19dfbf152421e78abf357b607
sha512: 160a8ab7b22f57096b7190f01b58d487b68f69881fa444adcba51b92d68c6ae9c9580e78e65c6cc846796ba138de1a69e5242fd6dec745482b8361798afabe76
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 2e992cb72c8236c9d2cf90c330310f79b24ceb89691a7a1755f183785644c0da
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.silkbank.silkbankretail.permission.MAPS_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.READ_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.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check possible Build.SERIAL check FINDINGS: Obfuscator — DETAILS: Gemalto unreadable field names unreadable method names FINDINGS: Compiler — DETAILS: r8

FILE	DETAILS

classes2.dex	

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Obfuscator	Gemalto unreadable field names unreadable method names
Compiler	r8 without marker (suspicious)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.4-4.4.4, [minSdk=19]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Launch Mode of activity (com.silkbank.silkbankretail.Silkmobile) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
4	Broadcast Receiver (com.konylabs.api.sms.SMSBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
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.

CODE ANALYSIS

HIGH: 1 | WARNING: 6 | INFO: 2 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	agggggg/qgggqq.java com/kony/binarydatamanager/BinaryFileAdapterWithMetadata/constants/Constants.java com/kony/binarydatamanager/constant/BinaryDataManagerConstants.java com/kony/cms/client/KonyCMSConstants.java com/kony/logger/Constants/LoggerConstants.java com/kony/sdkcommons/CommonUtility/KNYCommonConstants.java com/kony/sdkcommons/Database/KNYDatabaseErrorMessages.java com/kony/sdkcommons/Network/NetworkCore/KNYHttpJobIntentService.java com/kony/sdkcommons/Network/NetworkCore/KNYHttpService.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java sync/kony/com/syncv2library/Android/Constants/KSPublicConstants.java sync/kony/com/syncv2library/Android/Constants/MetadataConstants.java sync/kony/com/syncv2library/Android/Constants/SyncErrorMessages.java
				Jama/examples/MagicSquareExample.java Jama/test/TestMatrix.java aggggg/dddyyd.java aggggg/qssssq.java aggggg/rrjrjr.java aggggg/ssssoo.java aggggg/sswwww.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	aggggg/swwwsw.java aggggg/uuvuvu.java aggggg/uuvvuu.java aggggg/uvuvuu.java aggggg/vvpvpv.java aggggg/vvvuvv.java aggggg/wswsss.java com/example/mvisamodule/MainActivity.java com/example/mvisamodule/QRScanParser.java com/gemalto/idp/mobile/authentication/mode/face/ui/EnrollFragment.java com/gemalto/idp/mobile/authentication/mode/face/ui/FaceManager.java com/gemalto/idp/mobile/authentication/mode/face/ui/VerifyFragment.java com/gemalto/idp/mobile/authentication/mode/face/ui/internal/manager/FaceEnrollNoStepsManager.java com/gemalto/idp/mobile/authentication/mode/face/ui/internal/manager/FaceVerifyManager.java com/gemalto/idp/mobile/authentication/mode/face/ui/internal/utils/logs/MyLog.java com/kony/CaptureSignature.java com/kony/Sign.java com/kony/cms/client/KonyLogger.java com/kony/gemaltofaceauth/FaceEnrollActivity.java com/kony/gemaltofaceauth/FaceVerifyActivity.java com/kony/gemaltofaceauth/faceui/FaceEnrollmentActivity.java com/kony/gemaltofaceauth/faceui/FaceVerificationActivity.java com/kony/location/StartLocationSettings.java com/kony/logger/Core/KonyJSFacade.java com/kony/logger/Core/KonyLoggerCore.java com/kony/logger/LogUtils/LoggerUtils.java com/kony/logger/NetworkPersistor/NetworkService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/kony/logger/NetworkPersistor/NetworkServiceTestUtil.java com/kony/sdkcommons/Logger/KNYLoggerUtility.java com/konydemo/thirdparty/intent/ScanAnyBarcode.java com/konyffi/contacts/ContactPicker.java com/konylabs/android/KonyApplication.java com/konylabs/api/db/sqlcipher/KonySQLDatabase.java com/konylabs/api/location/KonyGeoTransitionsJobIntentService.java com/konylabs/jsbindings/ClassLoaderInjector.java com/neurotec/face/verification/NFaceVerificationCameraNew.java com/neurotec/lang/NCore.java com/neurotec/view/NPropertyView.java com/sun/jna/Native.java com/sun/jna/Structure.java com/tbruyelle/rxpermissions2/RxPermissionsFragment.java net/sqlcipher/AbstractCursor.java net/sqlcipher/BulkCursorToCursorAdaptor.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/DefaultDatabaseErrorHandler.java net/sqlcipher/database/SQLiteCompiledSql.java net/sqlcipher/database/SQLiteContentHelper.java net/sqlcipher/database/SQLiteCursor.java net/sqlcipher/database/SQLiteDatabase.java net/sqlcipher/database/SQLiteDebug.java net/sqlcipher/database/SQLiteOpenHelper.java net/sqlcipher/database/SQLiteProgram.java net/sqlcipher/database/SQLiteQuery.java net/sqlcipher/database/SQLiteQueryBuilder.java net/sqlcipher/database/SqliteWrapper.java sync/kony/com/syncv2library/Android/Logger/S

NO	ISSUE	SEVERITY	STANDARDS	FILES
				yncLogger.java util/e/b.java util/r/e.java
3	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	aggggg/lwwlwl.java aggggg/ssssww.java aggggg/ududuu.java aggggg/uuuduu.java aggggg/wwssws.java aggggg/wwwsws.java aggggg/wwwwsw.java com/kony/sdkcommons/Database/SQLiteAndroidDatabaseHelper.java util/as/d.java util/cg/c.java util/dc/c.java util/dc/e.java util/k/o.java util/l/e.java util/q/e.java
4	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	aggggg/diiidd.java aggggg/hmhmhh.java aggggg/pggggg.java aggggg/sccscc.java aggggg/uddddu.java util/et/d.java util/et/e.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	util/dq/e.java util/dr/c.java util/dv/b.java util/dw/d.java util/dx/b.java util/dy/a.java util/dz/o.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	aggggg/llllww.java aggggg/wwllww.java aggggg/wwwwlw.java com/kony/sdkcommons/Network/NetworkCore/KNYPublicKeyPinningManager.java com/kony/sdkcommons/Network/NetworkCore/KNYSSLSocketFactory.java util/ae/b.java util/cz/a.java
7	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/konylabs/jsbindings/ProxyBuilder.java com/sun/jna/Native.java
8	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	util/ae/b.java util/cz/a.java
9	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	aggggg/dddyyd.java aggggg/ssssoo.java aggggg/swssww.java aggggg/uuuuvu.java aggggg/wsswww.java aggggg/wswsss.java aggggg/ydyydd.java com/kony/CaptureSignature.java com/kony/logger/LogUtils/LoggerUtils.java com/konymp/konympsocialshare/SocialShare.java net/ndctech/pdfutils/PDFUtils.java util/m/mj.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	com/kony/sdkcommons/Database/SQLiteCipherDatabaseHelper.java com/konylabs/api/db/sqlcipher/KonySQLDatabase.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	Jama/test/TestMatrix.java aggggg/ccsccc.java aggggg/ddddii.java aggggg/hhmmhh.java aggggg/iddiid.java aggggg/lllwwl.java aggggg/sssswww.java aggggg/swswww.java aggggg/vpvppv.java aggggg/wsswww.java aggggg/wwswsw.java aggggg/wwwsww.java aggggg/wwwwws.java com/kony/binary/utility/BlobFileUtils.java com/kony/binarydatamanager/uploadHandlers/BytesUploadHandlerTask.java com/kony/binarydatamanager/uploadHandlers/MultipartUploadHandlerTask.java com/kony/cms/client/KonyCMSStorageManager.java com/konylabs/vmintf/KonyJavaScriptVM.java com/neurotec/io/NStream.java util/ae/b.java util/aj/b.java util/am/a.java util/am/b.java util/am/c.java util/de/d.java util/df/e.java util/ds/bx.java util/e/d.java util/m/PRNGFixes.java util/m/mj.java
00002	Open the camera and take picture	camera	aggggg/ffoooo.java

RULE ID	BEHAVIOUR	LABEL	FILES
00183	Get current camera parameters and change the setting.	camera	aggggg/ffoooo.java aggggg/uqquuu.java com/neurotec/face/verification/NFaceVerificationCameraOld.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	aggggg/ffoooo.java aggggg/hhmmhh.java aggggg/oeoeoo.java aggggg/swssww.java aggggg/uuuuvu.java
00004	Get filename and put it to JSON object	file collection	aggggg/ssssoo.java com/kony/binarydatamanager/manager/OnlineBinaryUploadManager.java com/kony/binarydatamanager/uploadHandlers/BytesUploadHandlerTask.java com/kony/binarydatamanager/uploadHandlers/MultipartUploadHandlerTask.java
00147	Get the time of current location	collection location	aggggg/sswwww.java
00075	Get location of the device	collection location	aggggg/sswwww.java
00137	Get last known location of the device	location collection	aggggg/sswwww.java
00199	Stop recording and release recording resources	record	aggggg/sccccc.java aggggg/uqquuu.java
00198	Initialize the recorder and start recording	record	aggggg/sccccc.java aggggg/uqquuu.java
00194	Set the audio source (MIC) and recorded file format	record	aggggg/sccccc.java

RULE ID	BEHAVIOUR	LABEL	FILES
00197	Set the audio encoder and initialize the recorder	record	aggggg/sccccc.java
00196	Set the recorded file format and output path	record file	aggggg/sccccc.java
00041	Save recorded audio/video to file	record	aggggg/sccccc.java aggggg/uqquuu.java
00035	Query the list of the installed packages	reflection	aggggg/iddddi.java aggggg/ididdi.java
00189	Get the content of a SMS message	sms	aggggg/csccc s.java aggggg/swwwss.java aggggg/uuuuvu.java aggggg/wswwss.java
00188	Get the address of a SMS message	sms	aggggg/csccc s.java aggggg/swwwss.java aggggg/uuuuvu.java aggggg/wswwss.java
00200	Query data from the contact list	collection contact	aggggg/csccc s.java aggggg/swwwss.java aggggg/uuuuvu.java aggggg/wswwss.java
00187	Query a URI and check the result	collection sms calllog calendar	aggggg/swwwss.java aggggg/wswwss.java

RULE ID	BEHAVIOUR	LABEL	FILES
00201	Query data from the call log	collection calllog	aggggg/cscccs.java aggggg/swwwss.java aggggg/uuuuvu.java aggggg/wswwss.java
00128	Query user account information	collection account	aggggg/swwwss.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	aggggg/hhmmhh.java aggggg/iiidii.java aggggg/jrjjrj.java aggggg/uuuuvu.java aggggg/vuuuuu.java com/konylabs/android/KonyMain.java com/konylabs/api/ui/KonyCordovaWeb.java com/konylabs/api/ui/KonyWeb.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	aggggg/hhmmhh.java aggggg/jrjjrj.java aggggg/vuuuuu.java com/konylabs/android/KonyMain.java com/konylabs/api/ui/KonyCordovaWeb.java com/konylabs/api/ui/KonyWeb.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	aggggg/didddi.java aggggg/swswww.java aggggg/wsswww.java aggggg/wwwsww.java aggggg/xvvxxv.java com/kony/cms/client/KonyCMSStorageManager.java com/kony/logger/LogUtils/LoggerUtils.java com/konylabs/api/ui/KonyWeb.java com/konymp/konympsocialshare/SocialShare.java com/sun/jna/Native.java com/sun/jna/NativeLibrary.java util/ai/d.java
00091	Retrieve data from broadcast	collection	aggggg/iiidii.java aggggg/oosooo.java com/kony/Sign.java com/kony/push/custom/CustomPushNotificationReceiver.java com/konylabs/android/KonyMain.java com/konylabs/gcm/KonyGCMBroadcastReceiver.java com/konylabs/notification/KonyLocalNotificationBroadcastReceiver.java
00014	Read file into a stream and put it into a JSON object	file	com/kony/binarydatamanager/uploadHandlers/BytesUploadHandlerTask.java com/kony/binarydatamanager/uploadHandlers/MultipartUploadHandlerTask.java
00012	Read data and put it into a buffer stream	file	aggggg/ddddii.java aggggg/hhmmhh.java aggggg/lllwwl.java aggggg/vpvppv.java aggggg/wwwsww.java com/konylabs/vmintf/KonyJavaScriptVM.java util/ae/b.java util/m/mj.java

RULE ID	BEHAVIOUR	LABEL	FILES
00067	Query the IMSI number	collection	util/ad/a.java
00028	Read file from assets directory	file	aggggg/ddddii.java com/konylabs/vmintf/KonyJavaScriptVM.java
00024	Write file after Base64 decoding	reflection file	com/kony/binary/utility/BinaryDataUtils.java
00036	Get resource file from res/raw directory	reflection	aggggg/hhmmhh.java aggggg/mmmhhh.java aggggg/uuuuvu.java com/konylabs/android/KonyMain.java com/konylabs/api/ui/KonyCordovaWeb.java com/konylabs/api/ui/KonyWeb.java
00072	Write HTTP input stream into a file	command network file	util/ae/b.java
00089	Connect to a URL and receive input stream from the server	command network	aggggg/jrrjjj.java aggggg/lllwlw.java aggggg/llwwll.java com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java util/ae/b.java util/cz/a.java
00109	Connect to a URL and get the response code	network command	aggggg/jrrjjj.java aggggg/lllwlw.java aggggg/llwwll.java com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java util/ae/b.java util/cz/a.java
00162	Create InetSocketAddress object and connecting to it	socket	aggggg/vppppp.java util/cz/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	aggggg/jrrjjj.java aggggg/lllwlw.java aggggg/llwwll.java aggggg/vppppp.java com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java util/cz/a.java util/cz/c.java
00209	Get pixels from the latest rendered image	collection	com/neurotec/face/verification/NFaceVerificationCameraNew.java
00191	Get messages in the SMS inbox	sms	aggggg/nmnmmm.java aggggg/uuuuvu.java
00112	Get the date of the calendar event	collection calendar	aggggg/nmnmmm.java
00096	Connect to a URL and set request method	command network	aggggg/jrrjjj.java aggggg/lllwlw.java aggggg/llwwll.java com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java util/cz/a.java
00030	Connect to the remote server through the given URL	network	aggggg/jrrjjj.java aggggg/lllwlw.java aggggg/llwwll.java com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java util/cz/a.java
00094	Connect to a URL and read data from it	command network	com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java util/cz/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00108	Read the input stream from given URL	network command	com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java util/cz/a.java
00192	Get messages in the SMS inbox	sms	aggggg/jrrjjj.java aggggg/uuuuvu.java aggggg/wwlwww.java
00123	Save the response to JSON after connecting to the remote server	network command	aggggg/lllwlw.java aggggg/llwwll.java
00202	Make a phone call	control	com/konylabs/api/ui/KonyCordovaWeb.java com/konylabs/api/ui/KonyWeb.java
00203	Put a phone number into an intent	control	com/konylabs/api/ui/KonyCordovaWeb.java com/konylabs/api/ui/KonyWeb.java
00033	Query the IMEI number	collection	aggggg/hhmhhh.java
00015	Put buffer stream (data) to JSON object	file	aggggg/rururu.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	aggggg/uuuuvu.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	aggggg/uuuuvu.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	aggggg/cscccs.java aggggg/uuuuvu.java
00009	Put data in cursor to JSON object	file	com/konyffi/contacts/ContactPicker.java

RULE ID	BEHAVIOUR	LABEL	FILES
00006	Scheduling recording task	record	aggggg/uqquuu.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.GET_ACCOUNTS, android.permission.READ_CONTACTS, android.permission.READ_PHONE_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	1/44	android.permission.WRITE_CONTACTS

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.this.f8571b04420442.values	ok	No Geolocation information available.
www.this.f10862b04430443.abort	ok	No Geolocation information available.
www.m9002b041f041f041f041f041f041f	ok	No Geolocation information available.
javax.xml.xmlconstants	ok	No Geolocation information available.
www.m9013b041f041f041f041f	ok	No Geolocation information available.
www.label	ok	No Geolocation information available.
www.this.f8570b0442044204420442.f8581b0442044204420442	ok	No Geolocation information available.
www.f10896b0442044204420442	ok	No Geolocation information available.
www.m9011b041f041f041fobjarr	ok	No Geolocation information available.
www.f10310b044c044c044c044c	ok	No Geolocation information available.
www.m9209b041d041d041d041d041d	ok	No Geolocation information available.
www.m9017b041f041f041f041fobjarr	ok	No Geolocation information available.
www.switch	ok	No Geolocation information available.
www.m9220b041d041dwwlwww	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.this.m7371b041f041f041f	ok	No Geolocation information available.
www.m9006b041f041f041f041fobjarr	ok	No Geolocation information available.
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.slider	ok	No Geolocation information available.
www.box	ok	No Geolocation information available.
www.this.f8570b0442044204420442.f8584b044204420442.equalsstr	ok	No Geolocation information available.
www.m9004b041f041f041f041f041fstr2	ok	No Geolocation information available.
www.m9016b041f041f041fobjarr	ok	No Geolocation information available.
www.m9012b041f041f041f041f041f	ok	No Geolocation information available.
www.this	ok	No Geolocation information available.
www.textfield2	ok	No Geolocation information available.
www.this.f8570b0442044204420442.m7389b041f041f041flocation	ok	No Geolocation information available.
www.m9005b041f041f041f041f	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.this.m7358b041f041f041f041f	ok	No Geolocation information available.
www.richtext	ok	No Geolocation information available.
www.this.f10862b04430443	ok	No Geolocation information available.
www.this.m7372b041f041f0l	ok	No Geolocation information available.
www.this.m7369b041f041f041ftrue	ok	No Geolocation information available.
www.image	ok	No Geolocation information available.
www.m9018b041f041f041f	ok	No Geolocation information available.
www.m9008b041f041f041f041f	ok	No Geolocation information available.
www.calender	ok	No Geolocation information available.
www.listbox	ok	No Geolocation information available.
www.this.m7359b041f041f041f041ftrue	ok	No Geolocation information available.
www.this.f8570b0442044204420442.m7382b041f041f041f041f041f041fwwlwll.f10824b0438	ok	No Geolocation information available.
www.image2	ok	No Geolocation information available.
www.super.gettablewbwwww.f10310b044c044c044c044c.tostring	ok	No Geolocation information available.
www.this.m9193b041f041f041f041f041fthis.f8582b044204420442	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.m4580b041d041d041d041d	ok	No Geolocation information available.
www.f10616b0426042604260426	ok	No Geolocation information available.
www.m9004b041f041f041f041f041fstring	ok	No Geolocation information available.
www.link	ok	No Geolocation information available.
www.m9009b041f041f041f041f	ok	No Geolocation information available.
www.this.m7368b041f041f041f	ok	No Geolocation information available.
www.m9020b041f041fobjarr	ok	No Geolocation information available.
www.textarea2	ok	No Geolocation information available.
www.line	ok	No Geolocation information available.
www.f8567b0442044204420442	ok	No Geolocation information available.
www.m9019b041f041f041fobjarr	ok	No Geolocation information available.
www.this.m9194b041f041f041f041fthis.f8577b0442044204420442	ok	No Geolocation information available.
www.f10601b04260426042604260426	ok	No Geolocation information available.
www.m9015b041f041f041f	ok	No Geolocation information available.
www.m4580b041d041d041d041d.m4581b041d041d041d041d041d041d	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.1	ok	No Geolocation information available.
www.this.f8571b04420442	ok	No Geolocation information available.
www.button	ok	No Geolocation information available.
www.pickerview	ok	No Geolocation information available.
www.f10899b04420442	ok	No Geolocation information available.
www.this.f10322b044c044c044c044c	ok	No Geolocation information available.
www.this.m7374b041f041f	ok	No Geolocation information available.
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
www.m9010b041f041f041f	ok	No Geolocation information available.
www.this.f8570b0442044204420442	ok	No Geolocation information available.
www.m9220b041d041dthis.f4702b044304430443	ok	No Geolocation information available.
www.this.f8571b04420442.isempty	ok	No Geolocation information available.
www.m9215b041d041d	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.2	ok	No Geolocation information available.
www.flex	ok	No Geolocation information available.
www.m9003b041f041f041f041f041fobjarr	ok	No Geolocation information available.
www.m9014b041f041f041f041fobjarr	ok	No Geolocation information available.
www.f10623b04260426	ok	No Geolocation information available.
www.m9021b041f041f	ok	No Geolocation information available.
www.this.f8574b044204420442	ok	No Geolocation information available.
xmlpull.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.m9214b041d041d041d	ok	No Geolocation information available.
www.m4580b041d041d041d041d.m4583b041d041d041d041d041dthis.f4586b04380438043804380438	ok	No Geolocation information available.
www.this.f8570b0442044204420442.f8576b04420442044204420442	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
xvpm@rfki.aj	aggggg/ssqsqs.java
oell@l.qgyqk3qk	aggggg/ooojjj.java
jds@gf.lf	aggggg/ooojoj.java
j586@s.3p	aggggg/jojjjj.java

HARDCODED SECRETS

POSSIBLE SECRETS
000201010211021341318344332435204739953035665802
00020101021102134080873888790041553260610171607452047399530395258O2
6224070867183024030867183024630484A4E

PLAYSTORE INFORMATION

Title: SilkMobile

Score: 1 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** com.silkbank.silkbankretail

Developer Details: Silkbank Ltd., Silkbank+Ltd., None, https://www.silkbank.com.pk/, info@silkbank.com.pk,

Release Date: Apr 4, 2024 **Privacy Policy:** Privacy link

Description:

Experience a complete suite of banking services through your smartphone using the new SilkBank App. You can get information on products and services, learn about discounts and deals offered on Silkbank cards. You can perform balance inquiries, fund transfers, bill payments, mobile top-ups along with subscribing to e-statements, SMS Alerts, and placing pay order requests using our new SilkMobile.

SCAN LOGS

Timestamp	Event	Error
2024-11-14 21:30:37	Generating Hashes	OK
2024-11-14 21:30:37	Extracting APK	OK
2024-11-14 21:30:37	Unzipping	OK
2024-11-14 21:30:38	Getting Hardcoded Certificates/Keystores	OK
2024-11-14 21:30:38	Parsing APK with androguard	OK
2024-11-14 21:30:41	Parsing AndroidManifest.xml	OK
2024-11-14 21:30:41	Extracting Manifest Data	OK
2024-11-14 21:30:41	Performing Static Analysis on: Silkmobile (com.silkbank.silkbankretail)	OK

2024-11-14 21:30:41	Fetching Details from Play Store: com.silkbank.silkbankretail	OK
2024-11-14 21:30:44	Manifest Analysis Started	OK
2024-11-14 21:30:44	Checking for Malware Permissions	OK
2024-11-14 21:30:44	Fetching icon path	OK
2024-11-14 21:30:44	Library Binary Analysis Started	OK
2024-11-14 21:30:44	Reading Code Signing Certificate	OK
2024-11-14 21:30:45	Running APKiD 2.1.5	OK
2024-11-14 21:30:49	Detecting Trackers	OK
2024-11-14 21:30:50	Decompiling APK to Java with JADX	OK
2024-11-14 21:31:10	Converting DEX to Smali	OK
2024-11-14 21:31:10	Code Analysis Started on - java_source	OK

2024-11-14 21:31:19	Android SAST Completed	OK
2024-11-14 21:31:19	Android API Analysis Started	OK
2024-11-14 21:31:24	Android API Analysis Completed	OK
2024-11-14 21:31:25	Android Permission Mapping Started	OK
2024-11-14 21:31:33	Android Permission Mapping Completed	OK
2024-11-14 21:31:37	Email and URL Extraction Completed	OK
2024-11-14 21:31:37	Android Behaviour Analysis Started	OK
2024-11-14 21:31:42	Android Behaviour Analysis Completed	OK
2024-11-14 21:31:42	Extracting String data from APK	OK
2024-11-14 21:31:42	Extracting String data from Code	OK
2024-11-14 21:31:43	Extracting String values and entropies from Code	OK

2024-11-14 21:31:44	Performing Malware check on extracted domains	OK
2024-11-14 21:32:36	Saving to Database	OK

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.