APP SCORES

Security Score 41/100

Trackers Detection 10/432

FILE INFORMATION

File Name HBL.apk

Size 40.29MB

MD5 f5e6af752c2834bc07b09d4ddcbff66e

SHA1 8850165445bfc8af73b63dfe298474aeaa1fdb3b

SHA256 6855f3265343aa208f2e64c0fbf1c3dd693dd80bc4889f86f30a8a550914096d

APP INFORMATION

App Name HBL Mobile

Package Name com.hbl.android.hblmobilebanking

Main Activity com.hbl.android.hblmobilebanking.activity.SplashActivity

Target SDK 33 Min SDK 23 Max SDK

Android Version Name 2.12.8 Android Version Code 172

PLAYSTORE INFORMATION

Title HBL Mobile

Score 4.6130652 Installs 10,000,000+ Price 0 Android Version Support Category Finance Play Store URL com.hbl.android.hblmobilebanking

Developer HBL, Developer ID HBL

Developer Address None

Developer Website http://www.hbl.com

Developer Email hblidapp@gmail.com

Release Date Mar 28, 2016 Privacy Policy Privacy link

Description

```
HBL Mobile is a safe and convenient way to bank with HBL. You can effortlessly perform various financial and non-financial transactions online such as bill payments, funds transfer, view details of your accounts and loan etc., whenever and wherever you want with the help of your smartphone.
HBL Mobile Features:
- View and download statement of your Accounts & HBL CreditCard
- View your transaction history
- Funds transfer between HBL accounts as well as 1LINK and M-net member bank accounts
- Payments [Utility Bills, Mobile Top-ups & Bills (Prepaid/Postpaid), e-Vouchers, Broadband Bill Payment, Educational Payments, Zakat/ Donations, Online Shopping, eIPO,]
- Credit Card payments
- Purchase movie, bus and event tickets
- Order food online
- QR payments
- Investment in HBL mutual funds and term deposit
- Apply for travel & accidental insurance
- Manage blocking and unblocking of HBL DebitCard & CreditCard
- Setup standing instructions for bill payments and fund transfers
- Multiple bill payments in a single transaction
- Locate your nearest HBL branches & ATMs
- Locate deals and discounts on your HBL DebitCard & CreditCard
- Generate your withholding tax certificate
- Request for cheque book & banker’s cheque
- Link and de-link your accounts
- Manage your transaction limits
- View details of your loans
- Apply NOC for HBL PersonalLoan
- Save and share transaction receipts
And many more…

Download the application now and experience banking at your fingertips with HBL Mobile.
Leave your feedback and rate our app so we can serve you better.
```

277

ACTIVITIES

View

19

SERVICES

View

10

RECEIVERS

View

9

PROVIDERS

View

Exported Activities
5

Exported Services
4

Exported Receivers
3

Exported Providers
1

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, O=Symantec Corporation, OU=Android Applications, CN=Symantec CA for Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-04-05 00:00:00+00:00
Valid To: 2049-12-30 23:59:59+00:00
Issuer: C=US, O=Symantec Corporation, CN=Symantec Root for Code Signing
Serial Number: 0x4c4599aa185b98cb73a9c41b26d47fc
Hash Algorithm: sha256
md5: 96555790cc5c68d4f10c6f2e6b53681b
sha1: 177290de2154b1f8ba5836a728f38209ab9f7ed5
sha256: a6e286fb2c53c6428312bda556f527a434a26f68d059c11a95c8a9760a4071c7
sha512:
6037ed5721503851b5ff83ddf8c0a126f0fea2db3b758ddd9a2f5b9c120ff5204d5fa6c302f50fa059b032b25ffa362fdf34d4cd27ee99242186adc9bda
c32bb
X.509 Subject: C=US, O=Symantec Corporation, CN=Symantec Root for Code Signing
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-04-05 00:00:00+00:00
Valid To: 2049-12-31 23:59:59+00:00
Issuer: C=US, O=Symantec Corporation, CN=Symantec Root for Code Signing
Serial Number: 0x6ede6f254943dcd25265c651e5e20df1
Hash Algorithm: sha256
md5: 9ad3b82b7b3e37059cb5030bb74eaa0f
sha1: 5f80657825a480f6fa34ab7ad8ebf80f613d3efe
sha256: 7c579e67bbf0ebb5ead2e2c469b4967dfe00fb36b1fe75910856bc7ccc4e8b10
sha512:
5458cac3c6275155f3d731823760c6661c07e8caa0e610077fb3fd505f0d4cb1b288b38638a937a05b42ccda5a8e72d607c308f05c9addc24e5877d35a0
4761a
X.509 Subject: C=PK, ST=Sindh, L=Karachi, O=Habib Bank Limited, OU=['Innovation & Financial Inclusion', 'Android Code
Signing'], CN=Habib Bank Limited
```

```
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-02-10 13:58:44+00:00
Valid To: 2041-02-05 23:42:23+00:00
Issuer: C=US, O=Symantec Corporation, OU=Android Applications, CN=Symantec CA for Android
Serial Number: 0x117
Hash Algorithm: sha256
md5: b63380319bb900d79bef5944858bd2dd
sha1: 6a8cfb52222963b11cd39e596e9b24ce520763f0
sha256: 0595294102751e0912be7f2c0b169a7f6842bc778236baaf91e9c7b0abb1f9ff
sha512:
bb4cf9ff8a9859538f1dd650db7342a3cd79ea3e0312849dc75bb7678537b37bf00c764ac58da6e75924ea1f3800d3ec2ae2ee5c04637552ff8012a81ab
634e9
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 727c4fa56594edce872c98982e33627eafdcc26557a0f3640cf3399b6dcf3ef2
Found 3 unique certificates
```

☰ APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.	
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.	
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.	
android.permission.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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.	
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.	
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	

Showing 1 to 10 of 34 entries

Previous 1 2 3 4 Next

ANDROID API

Search:

API	FILES
Android Notifications	
Base64 Decode	
Base64 Encode	
Certificate Handling	
Content Provider	
Crypto	
Dynamic Class and Dexloading	
Execute OS Command	
Get Installed Applications	
Get Network Interface information	

Showing 1 to 10 of 33 entries

Previous 1 2 3 4 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

🔒 NETWORK SECURITY

HIGH	WARNING	INFO	SECURE
1	0	4	0

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
1	10.6.226.40 10.9.167.13 10.9.167.14 10.6.229.74 10.6.226.49 10.6.226.85 10.6.226.86 10.6.226.52 10.6.229.36 10.6.226.47 10.6.226.90 10.6.226.188 10.16.221.76 10.16.221.27 10.16.221.33 10.16.221.109 10.6.229.204 10.6.229.94	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

NO	SCOPE	SEVERITY	DESCRIPTION
2	10.6.226.40 10.9.167.13 10.9.167.14 10.6.229.74 10.6.226.49 10.6.226.85 10.6.226.86 10.6.226.52 10.6.229.36 10.6.226.47 10.6.226.90 10.6.226.188 10.16.221.76 10.16.221.27 10.16.221.33 10.16.221.109 10.6.229.204 10.6.229.94	info	Domain config is configured to trust bundled certs @raw/hblbbappjuly2022.

NO	SCOPE	SEVERITY	DESCRIPTION
3	10.6.226.40 10.9.167.13 10.9.167.14 10.6.229.74 10.6.226.49 10.6.226.85 10.6.226.86 10.6.226.52 10.6.229.36 10.6.226.47 10.6.226.90 10.6.226.188 10.16.221.76 10.16.221.27 10.16.221.33 10.16.221.109 10.6.229.204 10.6.229.94	info	Domain config is configured to trust bundled certs @raw/hblbbapp2023.

NO	SCOPE	SEVERITY	DESCRIPTION
4	10.6.226.40 10.9.167.13 10.9.167.14 10.6.229.74 10.6.226.49 10.6.226.85 10.6.226.86 10.6.226.52 10.6.229.36 10.6.226.47 10.6.226.90 10.6.226.188 10.16.221.76 10.16.221.27 10.16.221.33 10.16.221.109 10.6.229.204 10.6.229.94	info	Domain config is configured to trust bundled certs @raw/hblibankjuly2022.

NO	SCOPE	SEVERITY	DESCRIPTION
5	10.6.226.40 10.9.167.13 10.9.167.14 10.6.229.74 10.6.226.49 10.6.226.85 10.6.226.86 10.6.226.52 10.6.229.36 10.6.226.47 10.6.226.90 10.6.226.188 10.16.221.76 10.16.221.27 10.16.221.33 10.16.221.109 10.6.229.204 10.6.229.94	info	Domain config is configured to trust bundled certs @raw/hblibank2023.

Showing 1 to 5 of 5 entries

Previous 1 Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
0	1	1

Search:

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

Showing 1 to 2 of 2 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
2	13	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	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	OPTIONS
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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.	
4	**Activity** (com.hbl.android.hblmobilebanking.qr_operations.RequestMoneyQrActivity) 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	OPTIONS
5	**Activity** (com.hbl.android.hblmobilebanking.qr_operations.QrGenerationActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
6	**Activity** (com.hbl.android.hblmobilebanking.tokenization.TokenizationWidget) 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	OPTIONS
7	**Broadcast Receiver** (com.hbl.android.hblmobilebanking.utils.AutoReadUtil) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** com.google.android.gms.auth.api.phone.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	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
			set to signature, only applications signed with the same certificate can obtain the permission.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
8	**Service** (com.hbl.android.hblmobilebanking.tokenization.contactless.HCEService) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** android.permission.BIND_NFC_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,	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
			only applications signed with the same certificate can obtain the permission.	
9	**Activity** (com.hbl.android.hblmobilebanking.login.LoginActivityNew) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
10	**Activity** (com.tilismtech.tellotalk_news.ui.activities.NewListActivity) 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.	

Showing 1 to 10 of 18 entries

Previous 1 2 Next

CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
5	9	3	2	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
1	The App logs information. Sensitive information should never be logged.	info	**CWE:** CWE-532: Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
2	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		
3	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	io/grpc/okhttp/internal/Util.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
4	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		
5	IP Address disclosure	warning	**CWE:** CWE-200: Information Exposure **OWASP MASVS:** MSTG-CODE-2		
6	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	**OWASP MASVS:** MSTG-CRYPTO-1	org/greenrobot/greendao/database/SqlCipherEncryptedHelper.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
7	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		
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	**OWASP MASVS:** MSTG-NETWORK-4		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
9	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		
10	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	**CWE:** CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-3	com/huawei/agconnect/config/a/i.java com/huawei/agconnect/credential/obs/z.java	

Showing 1 to 10 of 19 entries

Previous 1 2 Next

SHARED LIBRARY BINARY ANALYSIS

No Shared Objects found.

Search:

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
No data available in table								

Showing 0 to 0 of 0 entries

Previous Next

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
1	Certificate/Key files hardcoded inside the app.	res/raw/hblbbapp2023.cer res/raw/hblbbappjuly2022.cer res/raw/hblibank2023.cer res/raw/hblibank2024.cer res/raw/hblibankjuly2022.cer
2	Hardcoded Keystore found.	assets/grs_sp.bks assets/hmsincas.bks assets/hmsrootcas.bks

Showing 1 to 2 of 2 entries

Previous 1 Next

APKiD ANALYSIS

Search:

DEX	DETECTIONS
classes.dex	

Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible VM check
Compiler	r8
Obfuscator	unreadable field names unreadable method names

Showing 1 to 3 of 3 entries

Previous 1 Next

<table>
<tr><th>DEX</th><th>DETECTIONS</th></tr>
<tr><td>classes2.dex</td><td>
Search:
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
Showing 1 to 3 of 3 entries

Previous 1 Next
</td></tr>
</table>

DEX	DETECTIONS
classes3.dex	

Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check ro.kernel.qemu check
Compiler	r8 without marker (suspicious)

Showing 1 to 2 of 2 entries

Previous 1 Next

<table>
<tr><th>DEX</th><th>DETECTIONS</th></tr>
<tr><td>classes4.dex</td><td>
Search:
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>Obfuscator</td><td>unreadable field names
unreadable method names</td></tr>
</table>
Showing 1 to 3 of 3 entries

Previous 1 Next
</td></tr>
</table>

<table>
<tr><th>DEX</th><th>DETECTIONS</th></tr>
<tr><td>classes5.dex</td><td>Search:
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>Obfuscator</td><td>unreadable field names
unreadable method names</td></tr>
</table>
Showing 1 to 2 of 2 entries
Previous 1 Next</td></tr>
</table>

Showing 1 to 5 of 5 entries

Previous 1 Next

Q QUARK ANALYSIS

Search:

POTENTIAL MALICIOUS BEHAVIOUR	EVIDENCE
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

ABUSED PERMISSIONS

Top Malware Permissions **15**/24

android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.INTERNET, android.permission.VIBRATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.GET_TASKS, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.ACCESS_WIFI_STATE, android.permission.READ_CONTACTS, android.permission.WAKE_LOCK

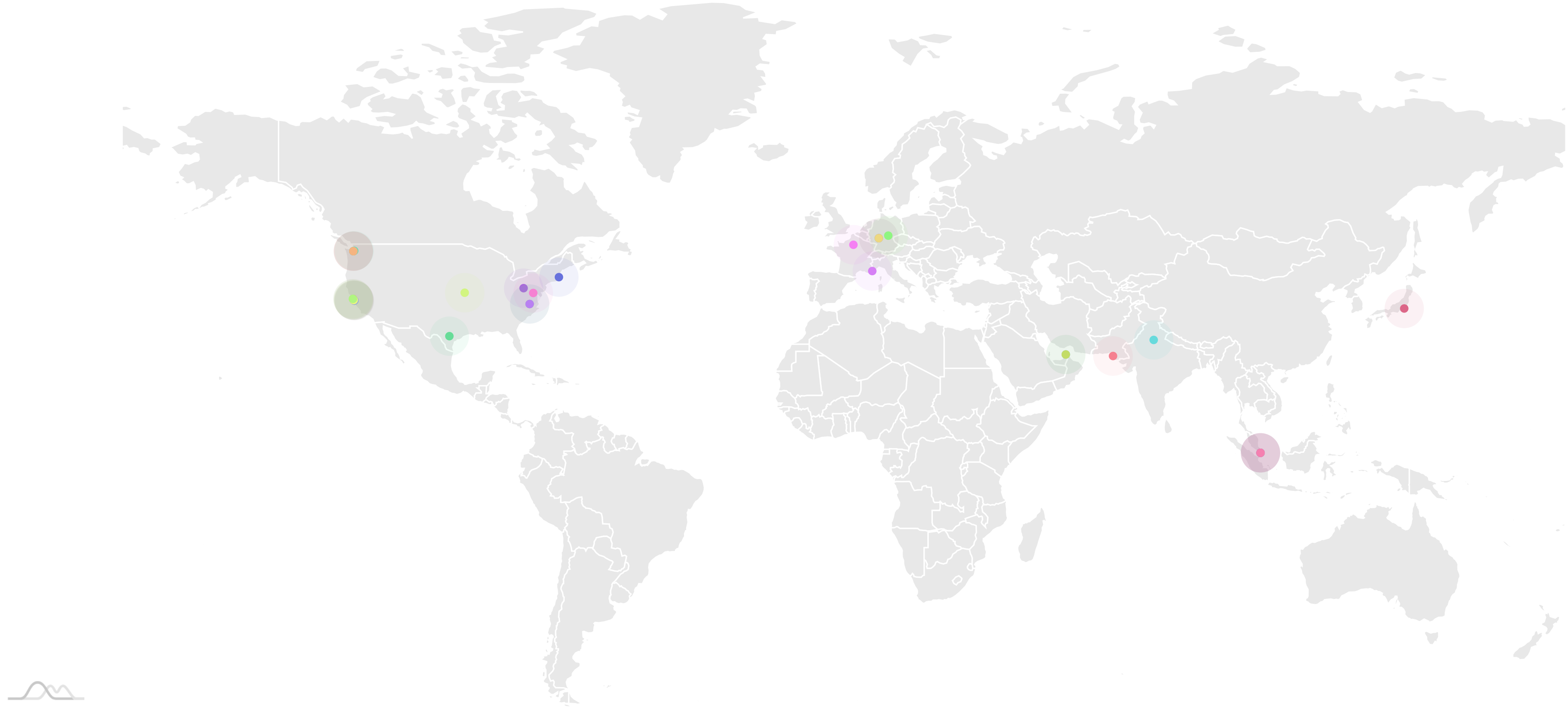
Other Common Permissions **7**/4

android.permission.FLASHLIGHT, android.permission.FOREGROUND_SERVICE, android.permission.CALL_PHONE, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVIC

Malware Permissions are the top permissions that are widely abused by known malware.

Other Common Permissions are permissions that are commonly abused by known malware.

SERVER LOCATIONS



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

Search:

DOMAIN	COUNTRY/REGION
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

DOMAIN MALWARE CHECK

Search:

DOMAIN	STATUS	GEOLOCATION
appgallery.cloud.huawei.com	ok	**IP:** 159.138.86.75 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
appgallery.huawei.com	ok	**IP:** 159.138.102.231 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
cipa.jp	ok	**IP:** 118.82.81.189 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
digitalbankingportal.hbl.com	ok	**IP:** 45.60.79.176 **Country:** United States of America **Region:** California **City:** Redwood City **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
faceoffauthentication.azurewebsites.net	ok	**IP:** 13.77.82.141 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
faceoffmobilebackend.azurewebsites.net	ok	**IP:** 13.77.82.141 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
github.com	ok	**IP:** 20.207.73.82 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
greenrobot.org	ok	**IP:** 85.13.163.69 **Country:** Germany **Region:** Thuringen **City:** Friedersdorf **Latitude:** 50.604919 **Longitude:** 11.035770 **View:** Google Map
hapi.dbp-stg.thalescloud.io	ok	**IP:** 99.83.203.154 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
hapi.dbp.thalescloud.io	ok	**IP:** 99.83.181.131 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

Showing 1 to 10 of 43 entries

Previous 1 2 3 4 5 Next

URLS

Search:

URL	FILE
data:image	com/bumptech/glide/load/model/DataUrlLoader.java
file:///android_asset/	com/bumptech/glide/load/model/AssetUriLoader.java
file:///android_res/	com/huawei/secure/android/common/util/UrlUtil.java
http://javax.xml.xmlconstants/feature/secure-processing	com/fasterxml/jackson/databind/ext/DOMDeserializer.java
http://localhost	com/huawei/agconnect/credential/Server.java
http://localhost/	retrofit2/Response.java
http://localhost/agc/apigw/oauth2/v1/token	com/huawei/agconnect/credential/obs/o.java
http://ns.adobe.com/pdf/1.3/	com/itextpdf/text/xml/xmp/PdfSchema.java
http://ns.adobe.com/xap/1.0/	com/itextpdf/text/xml/xmp/XmpBasicSchema.java
http://ns.adobe.com/xap/1.0/mm/	com/itextpdf/text/xml/xmp/XmpMMSchema.java

Showing 1 to 10 of 112 entries

Previous 1 2 3 4 5 … 12 Next

FIREBASE DATABASE

Search:

FIREBASE URL	DETAILS
https://hblmobiledomestic.firebaseio.com	info App talks to a Firebase database.

Showing 1 to 1 of 1 entries

Previous 1 Next

EMAILS

Search:

EMAIL	FILE
abc@xyz.com customer.complaints@hbl.com	Android String Resource

EMAIL	FILE
b9zp@ut.ijbwy	com/hbl/android/hblmobilebanking/payment/PayBeneficiariesSC1New.java
m@50y.l7	com/hbl/android/hblmobilebanking/readycash/views/ReadyCashAccountStatementActivity.java
na@l.66	com/itextpdf/text/pdf/security/DigestAlgorithms.java
u001cq@11.vip	util/h/xy/ar/ma.java

Showing 1 to 5 of 5 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67

TRACKER NAME	CATEGORIES	URL
Facebook Places		https://reports.exodus-privacy.eu.org/trackers/69
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333

Showing 1 to 10 of 10 entries

Previous 1 Next

POSSIBLE HARDCODED SECRETS

▶ Show all **412** secrets

STRINGS

From APK Resource

▶ Show all **4827** strings

From Code

▶ Show all **60032** strings

From Shared Objects

ACTIVITIES

▶ Show all **277** activities

SERVICES

▼ Showing all **19** services

com.hbl.android.hblmobilebanking.utils.FCMService
com.hbl.android.hblmobilebanking.utils.HMSService
com.gemalto.mfs.mwsdk.provisioning.push.CPSCommService
com.gemalto.mfs.mwsdk.mobilegateway.MGConfigurationChangeService
com.gemalto.mfs.mwsdk.dcm.broadcast.DCMBroadcastService
com.hbl.android.hblmobilebanking.tokenization.contactless.HCEService
com.huawei.hms.support.api.push.service.HmsMsgService
com.google.android.play.core.assetpacks.AssetPackExtractionService
com.google.android.gms.auth.api.signin.RevocationBoundService

com.google.firebase.components.ComponentDiscoveryService
com.google.firebase.messaging.FirebaseMessagingService
com.google.android.gms.analytics.AnalyticsService
com.google.android.gms.analytics.AnalyticsJobService
com.google.android.gms.measurement.AppMeasurementService
com.google.android.gms.measurement.AppMeasurementJobService
com.google.mlkit.common.internal.MlKitComponentDiscoveryService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService
com.huawei.agconnect.core.ServiceDiscovery

RECEIVERS

▼ Showing all **10** receivers

com.hbl.android.hblmobilebanking.utils.AutoReadUtil
com.huawei.hms.support.api.push.PushMsgReceiver
com.huawei.hms.support.api.push.PushReceiver
com.huawei.hms.analytics.receiver.HiAnalyticsSvcEvtReceiver
com.google.firebase.iid.FirebaseInstanceIdReceiver
com.google.android.gms.analytics.AnalyticsReceiver
com.google.android.gms.measurement.AppMeasurementReceiver
com.facebook.CurrentAccessTokenExpirationBroadcastReceiver
com.facebook.CampaignTrackingReceiver
com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver

PROVIDERS

▼ Showing all **9** providers

androidx.core.content.FileProvider

com.huawei.hms.support.api.push.PushProvider

com.huawei.hms.analytics.provider.AnalyticsInitializeProvider

com.unikrew.faceoff.fingerprint.SecureStorage.SecureStorageProvider

com.facebook.internal.FacebookInitProvider

com.google.mlkit.common.internal.MlKitInitProvider

com.google.firebase.provider.FirebaseInitProvider

com.huawei.hms.aaid.InitProvider

com.huawei.agconnect.core.provider.AGConnectInitializeProvider

LIBRARIES

▼ Showing all **1** libraries

org.apache.http.legacy

FILES

▶ Show all **2221** files

Version v4.0.7