MOBSF

ANDROID STATIC ANALYSIS REPORT

ES File Explorer (3.0.9.0)

File Name:	ES_File_Explorer_3.0.9.0.apk
Package Name:	com.estrongs.android.pop
Scan Date:	Feb. 4, 2026, 10:08 p.m.
App Security Score:	43/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
10	40	1	2	15

FILE INFORMATION

File Name: ES_File_Explorer_3.0.9.0.apk
Size: 3.85MB
MD5: a312049526219c769f2fe0d599fc4bc8
SHA1: e478a32cb86256cd8a07e3b15e6d08ac79f722ac
SHA256: 84b29daeda5283fe06aa93487377651c03acb67a9c654e7adeac0b7492e1ddea

APP INFORMATION

App Name: ES File Explorer
Package Name: com.estrongs.android.pop
Main Activity: com.estrongs.android.pop.view.FileExplorerActivity
Target SDK: 18
Min SDK: 5
Max SDK:
Android Version Name: 3.0.9.0
Android Version Code: 126

APP COMPONENTS

Activities: 52
Services: 4
Receivers: 4
Providers: 1
Exported Activities: 17
Exported Services: 1
Exported Receivers: 4
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=cn, ST=beijing, L=beijing, O=estrongs, OU=estrongs, CN=xiao
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2009-03-04 15:32:18+00:00
Valid To: 2063-12-06 15:32:18+00:00
Issuer: C=cn, ST=beijing, L=beijing, O=estrongs, OU=estrongs, CN=xiao
Serial Number: 0x49ae9f02
Hash Algorithm: sha1
md5: 3079a983587b13f6861dedfb6fad5502
sha1: 3b4ca20ef5761b671397099905146a592666fce4
sha256: 08e7cf9d166f82553fc89a447adaff3bf17ab53ea79b9743c250fcdfc57fa75b
sha512: e1331cedd2100844c29ab78e1d8c5138026b6920e948be3a3dadce6c9cbc22530a1b3599de1055f1b79e5f155ad4ae690210faced9a412c9ebbd61da9dc88476
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION

android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.SET_WALLPAPER	normal	set wallpaper	Allows the application to set the system wallpaper.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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_SUPERUSER	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
.PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
res/raw/netdisk_boxnet!classes.dex	FINDINGS: Compiler — DETAILS: dx
res/raw/netdisk_dropbox!classes.dex	FINDINGS: Compiler — DETAILS: dx
res/raw/netdisk_gdrive!classes.dex	FINDINGS: Compiler — DETAILS: dx
res/raw/netdisk_kanbox!classes.dex	FINDINGS — DETAILS

	Compiler: dx
res/raw/netdisk_kuaipan!classes.dex	FINDINGS: Compiler — DETAILS: dx
res/raw/netdisk_megacloud!classes.dex	FINDINGS: Compiler — DETAILS: dx
res/raw/netdisk_s3!classes.dex	FINDINGS: Compiler — DETAILS: dx
res/raw/netdisk_skydrv!classes.dex	FINDINGS: Compiler — DETAILS: dx
res/raw/netdisk_sugarsync!classes.dex	FINDINGS: Compiler — DETAILS: dx
res/raw/netdisk_ubuntu!classes.dex	FINDINGS: Compiler — DETAILS: dx

res/raw/netdisk_vdisk!classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx</td></tr></table>
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check device ID check subscriber ID check</td></tr><tr><td>Compiler</td><td>dx</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.estrongs.android.pop.app.DownloaderActivity	Schemes: http://, Hosts: dwz.cn, www.estrongs.com, Paths: /esshare,
com.estrongs.android.pop.app.BrowserDownloaderActivity	Schemes: http://, https://, ftp://, sftp://, Hosts: *, Mime Types: image/*, video/*, audio/*, text/plain, Path Patterns: .*\\.apk, .*\\.apk.*, .*\\..*\\.apk.*, .*\\..*\\..*\\.apk.*, .*\\..*\\..*\\..*\\.apk.*, .*\\..*\\..*\\..*\\..*\\.apk.*, .*\\..*\\..*\\..*\\..*\\..*\\.apk.*, .*\\..*\\..*\\..*\\..*\\..*\\..*\\.apk.*, .*\\.mp3, .*\\.mp3.*, .*\\..*\\.mp3.*, .*\\..*\\..*\\.mp3.*, .*\\..*\\..*\\..*\\.mp3.*, .*\\..*\\..*\\..*\\..*\\.mp3.*, .*\\..*\\..*\\..*\\..*\\..*\\.mp3.*, .*\\..*\\..*\\..*\\..*\\..*\\..*\\.mp3.*, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.mp3.*, .*\\.ape, .*\\.mp4, .*\\.avi, .*\\.wmv, .*\\.wav, .*\\.asf, .*\\.mpg, .*\\.3gp, .*\\.3gpp, .*\\.amr, .*\\.rm, .*\\.rmvb, .*\\.ogg, .*\\.oga, .*\\.ogv, .*\\.wma, .*\\.doc, .*\\.docx, .*\\.ppt, .*\\.pps, .*\\.ppx, .*\\.pptx, .*\\.xls, .*\\.xlsx, .*\\.chm, .*\\.txt, .*\\.zip, .*\\.zip.*, .*\\..*\\.zip.*, .*\\..*\\..*\\.zip.*, .*\\..*\\..*\\..*\\.zip.*, .*\\..*\\..*\\..*\\..*\\.zip.*, .*\\..*\\..*\\..*\\..*\\..*\\.zip.*, .*\\..*\\..*\\..*\\..*\\..*\\..*\\.zip.*, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.zip.*, .*\\.rar, .*\\.rar.*, .*\\..*\\.rar.*,

	.*\\..*\\..*\\.rar.*, .*\\..*\\..*\\..*\\.rar.*, .*\\.pdf, .*\\.torrent, .*\\.mkv, .*\\.swf, .*\\.flv, .*\\.aiff, .*\\.pcs, .*\\.mov,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 2 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	high	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 4 | WARNING: 29 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
			This application can be installed on an older version of android that has

1	App can be installed on a vulnerable unpatched Android version 2.0-2.1, [minSdk=5]	high	multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (com.estrongs.android.pop.app.compress.CompressionActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
4	Activity (com.estrongs.android.pop.app.compress.CompressionProxyActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
5	Activity (com.estrongs.android.pop.app.ESFileSharingActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
6	Activity (com.estrongs.android.pop.app.LocalFileSharingActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
7	Activity (com.estrongs.android.pop.app.PopVideoPlayer) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
8	Activity (com.estrongs.android.pop.app.PopVideoPlayerProxyActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
9	Launch Mode of activity (com.estrongs.android.pop.app.AudioPlayerProxyActivity) 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.
			An Activity should not be having the launch mode attribute set to

10	Activity (com.estrongs.android.pop.app.AudioPlayerProxyActivity) is vulnerable to Android Task Hijacking/StrandHogg.	high	"singleTask". It is then possible for other applications to place a malicious activity on top of the activity stack resulting in Task Hijacking/StrandHogg 1.0 vulnerability. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" or by setting an empty taskAffinity (taskAffinity="") attribute. You can also update the target SDK version (18) of the app to 28 or higher to fix this issue at platform level.
11	Activity (com.estrongs.android.pop.app.AudioPlayerProxyActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
12	Launch Mode of activity (com.estrongs.android.pop.app.StreamingMediaPlayer) 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.
13	Activity (com.estrongs.android.pop.app.StreamingMediaPlayer) is vulnerable to Android Task Hijacking/StrandHogg.	high	An Activity should not be having the launch mode attribute set to "singleTask". It is then possible for other applications to place a malicious activity on top of the activity stack resulting in Task Hijacking/StrandHogg 1.0 vulnerability. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" or by setting an empty taskAffinity (taskAffinity="") attribute. You can also update the target SDK version (18) of the app to 28 or higher to fix this issue at platform level.
14	Broadcast Receiver (.app.AudioPlayerService$MediaButtonReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
15	Activity (com.estrongs.android.pop.app.editor.PopNoteEditor) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
16	Launch Mode of activity (com.estrongs.android.pop.app.BTPopNoteEditor) 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.
17	Activity (com.estrongs.android.pop.app.FileChooserActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
18	Activity (com.estrongs.android.pop.app.ESContentChooserActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
19	Activity (com.estrongs.android.pop.app.ESRingtoneChooserActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
20	Activity (com.estrongs.android.pop.app.ESWallPaperChooserActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
21	Service (com.estrongs.android.pop.bt.OBEXFtpServerService) is not Protected. An intent-filter exists.	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.
22	Content Provider (com.estrongs.android.pop.app.FileContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
23	Activity (com.estrongs.android.pop.app.DownloaderActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
24	Activity (com.estrongs.android.pop.app.BrowserDownloaderActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
25	Activity (com.estrongs.android.pop.app.PopRemoteImageBrowser) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

26	Activity (com.estrongs.android.pop.ftp.ESFtpShortcut) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
27	Broadcast Receiver (com.baidu.share.message.ShareReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
28	Broadcast Receiver (com.estrongs.android.pop.EnableOEMConfig) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
29	Launch Mode of activity (.app.PopAudioPlayer) 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.
30	Activity (.app.PopAudioPlayer) is vulnerable to Android Task Hijacking/StrandHogg.	high	An Activity should not be having the launch mode attribute set to "singleTask". It is then possible for other applications to place a malicious activity on top of the activity stack resulting in Task Hijacking/StrandHogg 1.0 vulnerability. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" or by setting an empty taskAffinity (taskAffinity="") attribute. You can also update the target SDK version (18) of the app to 28 or higher to fix this issue at platform level.
31	Broadcast Receiver (.app.InstallMonitorReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
32	TaskAffinity is set for activity (.app.InstallMonitorActivity)	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.

33	Activity (.app.AppCheckUpdateList) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

</> CODE ANALYSIS

HIGH: 4 | WARNING: 9 | INFO: 1 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/b/a/a.java com/baidu/a/a/a/b/b.java com/baidu/mobstat/a/b.java com/baidu/mobstat/a/c.java com/baidu/sapi2/log/Logger.java com/baidu/share/message/ShareReceiver.java com/baidu/share/message/e.java com/baidu/share/message/token/a/a.java com/dropbox/client2/SdkVersion.java com/estrongs/a/b/e.java com/estrongs/android/c/b.java com/estrongs/android/c/c.java com/estrongs/android/c/g.java com/estrongs/android/c/i.java com/estrongs/android/d/d.java com/estrongs/android/e/a.java com/estrongs/android/ftp/a.java com/estrongs/android/ftp/h.java com/estrongs/android/ftp/i.java com/estrongs/android/ftp/k.java com/estrongs/android/pop/app/LocalFileSharingActivity.java com/estrongs/android/pop/app/a/a.java com/estrongs/android/pop/app/b/c.java

1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/estrongs/android/pop/app/b/g.java com/estrongs/android/pop/app/ed.java com/estrongs/android/pop/app/editor/PopNoteEditor.java com/estrongs/android/pop/app/editor/ad.java com/estrongs/android/pop/app/editor/ae.java com/estrongs/android/pop/app/editor/c.java com/estrongs/android/pop/app/imageviewer/BitmapManager.java com/estrongs/android/pop/app/imageviewer/CropImage.java com/estrongs/android/pop/app/imageviewer/ImageManager.java com/estrongs/android/pop/app/imageviewer/am.java com/estrongs/android/pop/app/imageviewer/gallery/c.java com/estrongs/android/pop/app/imageviewer/gallery/j.java com/estrongs/android/pop/app/j.java com/estrongs/android/pop/bt/OBEXFtpServerService.java com/estrongs/android/pop/bt/a.java com/estrongs/android/pop/bt/b.java com/estrongs/android/pop/bt/c.java com/estrongs/android/pop/bt/g.java com/estrongs/android/pop/bt/i.java com/estrongs/android/pop/m.java com/estrongs/android/pop/netfs/utils/HttpUploader.java com/estrongs/android/pop/netfs/utils/HttpUtils.java com/estrongs/android/pop/netfs/utils/LengthStreamBody.java com/estrongs/android/pop/netfs/utils/UploadOutputStream.java com/estrongs/android/pop/spfs/SPFileSystem.java

				com/estrongs/android/pop/spfs/facebook/FacebookFileSystem.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java com/estrongs/android/pop/spfs/instagram/InstagramFileSystem.java com/estrongs/android/pop/utils/aw.java com/estrongs/android/pop/view/ESRootView.java com/estrongs/android/ui/d/a.java com/estrongs/android/ui/drag/d.java com/estrongs/android/ui/e/bf.java com/estrongs/android/ui/e/er.java com/estrongs/android/ui/preference/SeekBarPreference.java com/estrongs/android/ui/theme/p.java com/estrongs/android/ui/view/NaviListView.java com/estrongs/android/ui/view/az.java com/estrongs/android/util/ai.java com/estrongs/android/util/aj.java com/estrongs/android/util/ak.java com/estrongs/android/util/aw.java com/estrongs/android/util/g.java com/estrongs/android/util/i.java com/estrongs/android/util/m.java com/estrongs/android/view/ck.java com/estrongs/android/view/m.java com/estrongs/android/widget/esswitch/a.java com/estrongs/fs/b/ag.java com/estrongs/fs/b/y.java com/estrongs/fs/d.java com/estrongs/fs/impl/g/b.java com/estrongs/fs/impl/g/c.java com/estrongs/fs/impl/local/h.java com/estrongs/fs/impl/pcs/PcsFileSystem.java com/estrongs/fs/impl/pcs/c.java com/estrongs/io/archive/d.java com/estrongs/io/archive/h.java

				com/estrongs/io/archive/rar/a.java com/gmail/yuyang226/flickr/a/a.java com/gmail/yuyang226/flickr/b/a.java com/handmark/pulltorefresh/library/a/h.java com/jcraft/jsch/ChannelDirectTCPIP.java com/jcraft/jsch/DHG1.java com/jcraft/jsch/DHGEX.java com/jcraft/jsch/KeyExchange.java com/jcraft/jsch/KnownHosts.java com/jcraft/jsch/Session.java com/jcraft/jsch/jce/MD5.java com/jcraft/jsch/jce/SHA1.java de/aflx/sardine/Version.java de/aflx/sardine/impl/SardineImpl.java de/aflx/sardine/util/Logger.java de/innosystec/unrar/a.java de/innosystec/unrar/e.java de/innosystec/unrar/unpack/ppm/l.java jcifs/smb/TestLocking.java jcifs/util/DES.java
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	com/dropbox/client2/android/AuthActivity.java com/gmail/yuyang226/flickr/oauth/a.java com/jcraft/jsch/jce/HMACSHA1.java com/jcraft/jsch/jce/HMACSHA196.java com/jcraft/jsch/jce/SHA1.java com/jcraft/jsch/jce/SignatureDSA.java com/jcraft/jsch/jce/SignatureRSA.java
				com/baidu/sapi2/BDAccountManager.java com/baidu/sapi2/YiAccountUtils.java com/baidu/sapi2/security/EncryptHelper.java com/baidu/sapi2/utils/DeviceId.java com/dropbox/client2/android/AuthActivity.java

3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/estrongs/android/pop/app/network/d.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java com/estrongs/android/pop/spfs/instagram/InstagramFileSystem.java com/estrongs/android/ui/b/gi.java jcifs/ntlmssp/Type3Message.java jcifs/smb/Dfs.java jcifs/smb/SmbComSessionSetupAndX.java jcifs/smb/SmbComTreeConnectAndX.java
				com/baidu/mobstat/a/b.java com/baidu/sapi2/loginshare/Utils.java com/baidu/sapi2/social/config/Domain.java com/estrongs/android/c/g.java com/estrongs/android/pop/a/a.java com/estrongs/android/pop/app/AudioPlayerService.java com/estrongs/android/pop/app/PopAudioPlayer.java com/estrongs/android/pop/app/PopVideoPlayer.java com/estrongs/android/pop/app/a/a.java com/estrongs/android/pop/app/b/c.java com/estrongs/android/pop/esclasses/a/a.java com/estrongs/android/pop/esclasses/a/aa.java com/estrongs/android/pop/esclasses/a/ab.java com/estrongs/android/pop/esclasses/a/ac.java com/estrongs/android/pop/esclasses/a/ad.java com/estrongs/android/pop/esclasses/a/ae.java

4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/estrongs/android/pop/esclasses/a/af.java com/estrongs/android/pop/esclasses/a/ag.java com/estrongs/android/pop/esclasses/a/ah.java com/estrongs/android/pop/esclasses/a/ai.java com/estrongs/android/pop/esclasses/a/b.java com/estrongs/android/pop/esclasses/a/c.java com/estrongs/android/pop/esclasses/a/d.java com/estrongs/android/pop/esclasses/a/e.java com/estrongs/android/pop/esclasses/a/f.java com/estrongs/android/pop/esclasses/a/g.java com/estrongs/android/pop/esclasses/a/i.java com/estrongs/android/pop/esclasses/a/j.java com/estrongs/android/pop/esclasses/a/k.java com/estrongs/android/pop/esclasses/a/l.java com/estrongs/android/pop/esclasses/a/m.java com/estrongs/android/pop/esclasses/a/n.java com/estrongs/android/pop/esclasses/a/o.java com/estrongs/android/pop/esclasses/a/p.java com/estrongs/android/pop/esclasses/a/q.java com/estrongs/android/pop/esclasses/a/r.java com/estrongs/android/pop/esclasses/a/s.java

				com/estrongs/android/pop/esclasses/a/u.java com/estrongs/android/pop/esclasses/a/v.java com/estrongs/android/pop/esclasses/a/w.java com/estrongs/android/pop/esclasses/a/x.java com/estrongs/android/pop/esclasses/a/y.java com/estrongs/android/pop/esclasses/a/z.java com/estrongs/android/ui/e/er.java com/estrongs/android/ui/view/u.java com/estrongs/android/util/ak.java com/estrongs/fs/impl/pcs/PcsFileSystem.java com/jcraft/jsch/ChannelDirectTCPIP.java com/jcraft/jsch/ChannelForwardedTCPIP.java com/jcraft/jsch/ChannelX11.java com/jcraft/jsch/PortWatcher.java com/jcraft/jsch/Session.java jcifs/UniAddress.java jcifs/netbios/NameServiceClient.java jcifs/netbios/NbtAddress.java
5	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/b/a/a/a.java com/baidu/a/a/a/b/c.java com/baidu/sapi2/DeviceCrypto.java com/baidu/sapi2/Utils.java com/baidu/sapi2/account/AccountEncrypt.java com/baidu/sapi2/security/Md5.java com/estrongs/android/pop/utils/y.java com/estrongs/fs/impl/pcs/PcsFileSystem.java com/jcraft/jsch/jce/HMACMD5.java com/jcraft/jsch/jce/HMACMD596.java com/jcraft/jsch/jce/MD5.java jcifs/smb/NtlmPasswordAuthentication.j

				ava jcifs/smb/SigningDigest.java jcifs/util/HMACT64.java
6	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/baidu/a/a/a/b/b.java com/baidu/mobstat/a/b.java com/baidu/sapi2/share/NativeCrypto.java com/baidu/sapi2/utils/DeviceId.java com/estrongs/android/pop/FexApplication.java com/estrongs/android/pop/app/diskusage/e.java com/estrongs/android/pop/app/editor/c.java com/estrongs/android/pop/app/imageviewer/ImageManager.java com/estrongs/android/pop/app/imageviewer/ac.java com/estrongs/android/pop/b.java com/estrongs/android/ui/a/ai.java com/estrongs/android/ui/a/u.java com/estrongs/android/ui/d/e.java com/estrongs/android/view/ar.java com/estrongs/android/view/e.java com/estrongs/fs/impl/f/c.java
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	com/estrongs/android/pop/app/a/ag.java com/estrongs/android/pop/app/a/ai.java com/estrongs/android/pop/spfs/facebook/FacebookFileSystemCache.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystemCache.java com/estrongs/android/pop/spfs/instagram/InstagramFileSystemCache.java com/estrongs/android/util/ax.java
				com/baidu/sapi2/PassportDomanGetter.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	com/baidu/sapi2/http/SimpleMultipartEntity.java com/baidu/sapi2/security/EncryptHelper.java com/estrongs/android/pop/app/a/a/b.java com/estrongs/android/pop/app/network/d.java com/estrongs/android/ui/drag/d.java com/estrongs/android/ui/h/a.java com/estrongs/fs/impl/pcs/PcsFileSystem.java de/a/a/a/a/e.java jcifs/smb/NtlmPasswordAuthentication.java
9	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/baidu/share/message/a.java com/estrongs/android/util/k.java com/jcraft/jsch/jce/ARCFOUR.java com/jcraft/jsch/jce/ARCFOUR128.java com/jcraft/jsch/jce/ARCFOUR256.java com/jcraft/jsch/jce/TripleDESCBC.java com/jcraft/jsch/jce/TripleDESCTR.java
10	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/estrongs/android/c/i.java com/estrongs/android/pop/bt/i.java
11	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	com/estrongs/android/pop/spfs/facebook/FacebookFileSystem.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java com/estrongs/android/pop/spfs/instagram/InstagramFileSystem.java de/aflx/sardine/impl/SardineImpl.java
12	This App uses SSL certificate pinning to detect or prevent MITM attacks in	secure		com/estrongs/android/pop/spfs/facebook/FacebookFileSystem.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java com/estrongs/android/pop/spfs/instagr

	secure communication channel.		OWASP MASVS: MSTG-NETWORK-4	am/InstagramFileSystem.java com/estrongs/fs/impl/pcs/PcsFileSystem.java de/aflx/sardine/impl/SardineImpl.java
13	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/baidu/sapi2/utils/LoginProtectActivity.java com/estrongs/android/ui/view/PcsThirdPartOAuth.java
14	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/estrongs/android/pop/view/FileExplorerActivity.java com/estrongs/fs/impl/local/h.java
15	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. 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	com/baidu/sapi2/utils/LoginProtectActivity.java
16	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/baidu/a/a/a/a/a.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
		True info The binary has NX bit set. This	Dynamic Shared Object (DSO) info The shared	True info This binary has a stack canary	Full RELRO info This shared object has full RELRO	None info The binary does not have	None info The binary does not have	False warning The binary does not have any fortified functions. Fortified	True info Symbols are stripped.

1	x86/libsapi_so_1.so	set. This marks a memory page non-executable making attacker injected shellcode non-executable.	The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	does not have run-time search path or RPATH set.	have RUNPATH set.	functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	
2	x86/libmyaes.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

			much more difficult to execute reliably.	of overflows by verifying the integrity of the canary before function return.	GOT (.got and .got.plt both) is marked as read-only.				
3	armeabi/libsapi_so_1.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
		True info The binary has NX bit set. This	Dynamic Shared Object (DSO) info The shared	True info This binary has a stack canary	Full RELRO info This shared object has full RELRO	None info The binary does not	None info The binary does not have	False warning The binary does not have any fortified functions. Fortified	True info Symbols are stripped.

4	armeabi/libmyaes.so	set. This marks a memory page non-executable making attacker injected shellcode non-executable.	The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	does not have run-time search path or RPATH set.	have RUNPATH set.	functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	
5	x86/libsapi_so_1.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

			(ROP) attacks much more difficult to execute reliably.	detection of overflows by verifying the integrity of the canary before function return.	the entire GOT (.got and .got.plt both) is marked as read-only.				
6	x86/libmyaes.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
		True info The binary has NX bit	Dynamic Shared Object (DSO) info	True info This binary has a stack	Full RELRO info This shared object has	None info The binary	None info The binary does not	False warning The binary does not have any fortified	True info Symbols are stripped

7	armeabi/libsapi_so_1.so	has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	binary does not have run-time search path or RPATH set.	does not have RUNPATH set.	have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	stripped.
8	armeabi/libmyaes.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries	True info Symbols are stripped.

			Programming (ROP) attacks much more difficult to execute reliably.	This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.			Dart/Flutter libraries.	

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
			com/baidu/sapi2/Utils.java com/baidu/sapi2/YiAccountUtils.java com/dropbox/client2/android/AndroidAuthSession.java com/dropbox/client2/android/AuthActivity.java com/estrongs/a/b/i.java com/estrongs/android/pop/app/FileChooserActivity.java com/estrongs/android/pop/app/ImageCommentActivity.java com/estrongs/android/pop/app/PopRemoteImageBrowser.java com/estrongs/android/pop/app/PopVideoPlayer.java com/estrongs/android/pop/app/ar.java com/estrongs/android/pop/app/b.java com/estrongs/android/pop/app/editor/c.java com/estrongs/android/pop/app/em.java

00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/estrongs/android/pop/app/gv.java com/estrongs/android/pop/app/hm.java com/estrongs/android/pop/app/hs.java com/estrongs/android/pop/app/hy.java com/estrongs/android/pop/app/imageviewer/ViewImage21.java com/estrongs/android/pop/app/in.java com/estrongs/android/pop/utils/bt.java com/estrongs/android/pop/utils/y.java com/estrongs/android/pop/view/bq.java com/estrongs/android/pop/view/utils/n.java com/estrongs/android/ui/b/ey.java com/estrongs/android/ui/b/ga.java com/estrongs/android/ui/e/av.java com/estrongs/android/ui/e/aw.java com/estrongs/android/ui/h/c.java com/estrongs/android/ui/notification/f.java com/estrongs/android/ui/notification/g.java com/estrongs/android/ui/pcs/as.java com/estrongs/android/ui/pcs/bv.java com/estrongs/android/ui/pcs/d.java com/estrongs/android/ui/preference/fragments/AboutPreferenceFragment.java com/estrongs/android/ui/theme/ai.java com/estrongs/android/ui/view/ax.java com/estrongs/android/util/at.java com/estrongs/android/view/cv.java com/estrongs/fs/b/ah.java com/estrongs/fs/b/al.java com/estrongs/fs/b/am.java
	Implicit intent(view a web page, make a		com/dropbox/client2/android/AndroidAuthSession.java com/estrongs/android/pop/app/FileChooserActivity.java com/estrongs/android/pop/app/PopRemoteImageBrowser.java com/estrongs/android/pop/app/PopVideoPlayer.java com/estrongs/android/pop/app/b.java com/estrongs/android/pop/app/hm.java com/estrongs/android/pop/app/hs.java com/estrongs/android/pop/app/hy.java com/estrongs/android/pop/app/in.java com/estrongs/android/pop/utils/y.java com/estrongs/android/pop/view/bq.java com/estrongs/android/ui/b/ey.java

00051	phone call, etc.) via setData	control	com/estrongs/android/ui/b/ga.java com/estrongs/android/ui/e/av.java com/estrongs/android/ui/e/aw.java com/estrongs/android/ui/notification/f.java com/estrongs/android/ui/notification/g.java com/estrongs/android/ui/pcs/bv.java com/estrongs/android/ui/pcs/d.java com/estrongs/android/ui/view/ax.java com/estrongs/android/util/at.java com/estrongs/android/view/cv.java com/estrongs/fs/b/ah.java com/estrongs/fs/b/al.java com/estrongs/fs/b/am.java
00091	Retrieve data from broadcast	collection	com/baidu/sapi2/share/ShareReceiver.java com/baidu/share/message/ShareReceiver.java com/estrongs/android/pop/app/FileChooserActivity.java com/estrongs/android/pop/app/OpenRecomm.java com/estrongs/android/pop/app/PopRemoteImageBrowser.java com/estrongs/android/pop/app/am.java com/estrongs/android/pop/app/imageviewer/CropImage.java com/estrongs/android/pop/view/FileExplorerActivity.java com/estrongs/android/pop/view/bw.java com/estrongs/android/ui/view/CreateOAuthServiceProvider.java
00043	Calculate WiFi signal strength	collection wifi	com/estrongs/android/f/j.java
00096	Connect to a URL and set request method	command network	com/baidu/sapi2/loginshare/Sharer.java com/estrongs/android/pop/spfs/OAuthUtil.java com/estrongs/android/pop/spfs/facebook/FacebookFileSystem.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java com/estrongs/android/pop/utils/bw.java com/estrongs/android/util/x.java com/estrongs/fs/impl/b/d.java jcifs/http/NtlmHttpURLConnection.java
00089	Connect to a URL and receive input stream from the server	command network	com/baidu/sapi2/loginshare/Sharer.java com/estrongs/android/pop/spfs/OAuthUtil.java com/estrongs/android/pop/spfs/facebook/FacebookFileSystem.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java com/estrongs/android/pop/utils/bw.java

			com/estrongs/android/util/x.java com/estrongs/fs/impl/b/d.java jcifs/http/NtlmHttpURLConnection.java
00030	Connect to the remote server through the given URL	network	com/baidu/sapi2/loginshare/Sharer.java com/estrongs/android/pop/spfs/OAuthUtil.java com/estrongs/android/pop/spfs/facebook/FacebookFileSystem.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java com/estrongs/android/util/x.java com/estrongs/fs/impl/b/d.java jcifs/http/NtlmHttpURLConnection.java
00109	Connect to a URL and get the response code	network command	com/baidu/sapi2/loginshare/Sharer.java com/estrongs/android/pop/spfs/OAuthUtil.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java com/estrongs/android/pop/utils/bw.java com/estrongs/android/util/x.java jcifs/http/NtlmHttpURLConnection.java
00094	Connect to a URL and read data from it	command network	com/baidu/sapi2/loginshare/Sharer.java com/estrongs/android/pop/spfs/facebook/FacebookFileSystem.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java com/estrongs/android/pop/utils/bw.java com/estrongs/android/util/x.java jcifs/http/NtlmHttpURLConnection.java
00108	Read the input stream from given URL	network command	com/baidu/sapi2/loginshare/Sharer.java com/estrongs/android/pop/spfs/facebook/FacebookFileSystem.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java com/estrongs/android/pop/utils/bw.java com/estrongs/android/util/x.java jcifs/http/NtlmHttpURLConnection.java
			com/baidu/sapi2/loginshare/FileStorage.java com/baidu/sapi2/share/ShareReceiver.java com/baidu/share/message/e.java com/baidu/share/message/token/a/a.java com/estrongs/android/c/a.java com/estrongs/android/c/i.java com/estrongs/android/d/a.java

00022	Open a file from given absolute path of the file	file	com/estrongs/android/d/b.java com/estrongs/android/d/c.java com/estrongs/android/d/e.java com/estrongs/android/d/f.java com/estrongs/android/ftp/h.java com/estrongs/android/pop/FexApplication.java com/estrongs/android/pop/app/DownloaderActivity.java com/estrongs/android/pop/app/FileChooserActivity.java com/estrongs/android/pop/app/a/ai.java com/estrongs/android/pop/app/compress/CompressionActivity.java com/estrongs/android/pop/app/compress/ap.java com/estrongs/android/pop/app/compress/aq.java com/estrongs/android/pop/app/diskusage/b.java com/estrongs/android/pop/app/diskusage/e.java com/estrongs/android/pop/app/diskusage/f.java com/estrongs/android/pop/app/diskusage/g.java com/estrongs/android/pop/app/diskusage/h.java com/estrongs/android/pop/app/diskusage/i.java com/estrongs/android/pop/app/diskusage/k.java com/estrongs/android/pop/app/diskusage/m.java com/estrongs/android/pop/app/editor/a.java com/estrongs/android/pop/app/editor/ae.java com/estrongs/android/pop/app/editor/am.java com/estrongs/android/pop/app/editor/c.java com/estrongs/android/pop/app/editor/d.java com/estrongs/android/pop/app/fo.java com/estrongs/android/pop/app/imageviewer/gallery/c.java com/estrongs/android/pop/app/is.java com/estrongs/android/pop/app/it.java com/estrongs/android/pop/b.java com/estrongs/android/pop/bt/a.java com/estrongs/android/pop/bt/c.java com/estrongs/android/pop/q.java com/estrongs/android/pop/utils/aa.java com/estrongs/android/pop/utils/aj.java com/estrongs/android/pop/utils/ao.java com/estrongs/android/pop/view/FileExplorerActivity.java com/estrongs/android/pop/view/utils/RemoteSynchronizer.java com/estrongs/android/pop/view/utils/d.java com/estrongs/android/pop/view/utils/n.java com/estrongs/android/ui/b/as.java com/estrongs/android/ui/b/av.java

			com/estrongs/android/ui/b/dn.java com/estrongs/android/ui/e/fk.java com/estrongs/android/ui/preference/fragments/f.java com/estrongs/android/ui/theme/ai.java com/estrongs/android/ui/theme/al.java com/estrongs/android/ui/theme/i.java com/estrongs/android/util/ak.java com/estrongs/android/util/at.java com/estrongs/android/view/e.java com/estrongs/android/widget/z.java com/estrongs/fs/a/b.java com/estrongs/fs/b/ab.java com/estrongs/fs/b/ac.java com/estrongs/fs/b/g.java com/estrongs/fs/b/o.java com/estrongs/fs/b/q.java com/estrongs/fs/b/t.java com/estrongs/fs/b/y.java com/estrongs/fs/c/a.java com/estrongs/fs/d.java com/estrongs/fs/impl/b/d.java com/estrongs/fs/impl/e/a.java com/estrongs/fs/impl/f/c.java com/estrongs/fs/impl/k/a.java com/estrongs/fs/impl/local/b.java com/estrongs/fs/impl/local/d.java com/estrongs/fs/impl/local/h.java com/estrongs/fs/impl/m/b.java com/estrongs/fs/impl/media/b.java com/estrongs/fs/impl/n/a.java com/estrongs/fs/impl/o/b.java com/estrongs/io/archive/aeszip/h.java com/estrongs/io/archive/aeszip/k.java com/estrongs/io/archive/g.java com/estrongs/io/archive/h.java com/estrongs/io/archive/i.java com/estrongs/io/model/ArchiveEntryFile.java com/estrongs/io/model/ExtFile.java de/innosystec/unrar/e.java
			com/baidu/mobstat/a.java com/baidu/mobstat/a/b.java

00013	Read file and put it into a stream	file	com/baidu/sapi2/account/AccountStorage.java com/baidu/sapi2/http/RequestParams.java com/baidu/sapi2/http/SimpleMultipartEntity.java com/baidu/sapi2/loginshare/FileStorage.java com/baidu/share/message/e.java com/estrongs/android/c/g.java com/estrongs/android/ftp/h.java com/estrongs/android/pop/app/a/al.java com/estrongs/android/pop/app/editor/c.java com/estrongs/android/pop/app/editor/d.java com/estrongs/android/pop/app/imageviewer/gallery/j.java com/estrongs/android/pop/bt/c.java com/estrongs/android/pop/q.java com/estrongs/android/pop/spfs/facebook/FacebookFileSystem.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java com/estrongs/android/pop/spfs/instagram/InstagramFileSystem.java com/estrongs/android/pop/utils/aa.java com/estrongs/android/pop/view/utils/RemoteSynchronizer.java com/estrongs/android/pop/view/utils/n.java com/estrongs/android/util/ak.java com/estrongs/android/util/at.java com/estrongs/fs/c/d.java com/estrongs/fs/impl/local/d.java com/estrongs/fs/impl/n/a.java com/estrongs/fs/impl/pcs/PcsFileSystem.java com/estrongs/io/archive/c.java com/estrongs/io/model/ExtFile.java jcifs/Config.java org/simpleframework/xml/core/Persister.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/estrongs/android/pop/app/editor/c.java com/estrongs/android/util/ah.java com/estrongs/android/util/j.java com/estrongs/fs/impl/media/b.java com/estrongs/fs/impl/media/e.java
00033	Query the IMEI number	collection	com/baidu/a/a/a/b/b.java com/baidu/mobstat/c.java com/baidu/sapi2/Utils.java com/baidu/sapi2/share/NativeCrypto.java com/baidu/sapi2/utils/DeviceId.java com/estrongs/android/pop/view/FileExplorerActivity.java

			com/estrongs/android/ui/b/x.java com/estrongs/android/ui/pcs/as.java
00191	Get messages in the SMS inbox	sms	com/baidu/sapi2/YiAccountUtils.java com/baidu/sapi2/loginshare/Utils.java com/estrongs/android/pop/app/editor/c.java
00130	Get the current WIFI information	wifi collection	com/baidu/mobstat/z.java com/baidu/sapi2/Utils.java com/estrongs/android/f/h.java com/estrongs/android/pop/view/FileExplorerActivity.java com/estrongs/android/util/ai.java com/estrongs/android/view/ck.java com/estrongs/fs/b/ae.java
00134	Get the current WiFi IP address	wifi collection	com/estrongs/android/util/ai.java com/estrongs/fs/b/ae.java
00012	Read data and put it into a buffer stream	file	com/estrongs/android/pop/bt/c.java
00106	Get the currently formatted WiFi IP address	collection wifi	com/estrongs/android/ui/b/gi.java
00125	Check if the given file path exist	file	com/baidu/sapi2/share/ShareReceiver.java com/estrongs/android/pop/app/DownloaderActivity.java com/estrongs/android/pop/app/imageviewer/CropImage.java com/estrongs/android/pop/view/FileExplorerActivity.java
00038	Query the phone number	collection	com/estrongs/android/pop/utils/bx.java com/estrongs/android/ui/pcs/bb.java com/estrongs/android/ui/pcs/x.java
00066	Query the ICCID number	collection	com/estrongs/android/ui/pcs/as.java
00162	Create InetSocketAddress object and	socket	com/estrongs/android/c/g.java com/estrongs/android/pop/app/b/g.java com/estrongs/fs/b/af.java

	connecting to it		com/estrongs/fs/b/ag.java com/estrongs/fs/b/at.java jcifs/smb/SmbTransport.java
00163	Create new Socket and connecting to it	socket	com/estrongs/android/c/g.java com/estrongs/android/pop/app/b/g.java com/estrongs/android/pop/spfs/facebook/FacebookFileSystem.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java com/estrongs/fs/b/af.java com/estrongs/fs/b/ag.java com/estrongs/fs/b/at.java jcifs/smb/SmbTransport.java
00014	Read file into a stream and put it into a JSON object	file	com/baidu/mobstat/a.java com/baidu/sapi2/loginshare/FileStorage.java com/baidu/share/message/e.java com/estrongs/android/pop/spfs/facebook/FacebookFileSystem.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java com/estrongs/android/pop/spfs/instagram/InstagramFileSystem.java
00005	Get absolute path of file and put it to JSON object	file	com/baidu/sapi2/loginshare/FileStorage.java com/baidu/sapi2/share/ShareReceiver.java com/baidu/share/message/e.java com/estrongs/fs/b/q.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/baidu/mobstat/z.java com/baidu/sapi2/Utils.java
00137	Get last known location of the device	location collection	com/baidu/mobstat/z.java
00115	Get last known location of the device	collection location	com/baidu/mobstat/z.java
00082	Get the current WiFi MAC address	collection wifi	com/baidu/mobstat/z.java com/baidu/sapi2/Utils.java
00121	Create a directory	file command	com/estrongs/android/pop/app/DownloaderActivity.java com/estrongs/android/pop/app/PopPreferenceActivity.java com/estrongs/android/ui/preference/FtpServerPreference.java

00153	Send binary data over HTTP	http	com/estrongs/android/pop/spfs/OAuthUtil.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java
00192	Get messages in the SMS inbox	sms	com/estrongs/android/pop/app/PopVideoPlayer.java com/estrongs/fs/impl/media/b.java
00187	Query a URI and check the result	collection sms calllog calendar	com/estrongs/android/pop/app/imageviewer/gallery/a.java com/estrongs/fs/impl/f/c.java com/estrongs/fs/impl/media/b.java com/estrongs/fs/impl/media/e.java
00023	Start another application from current application	reflection control	com/estrongs/android/pop/utils/c.java com/estrongs/android/ui/view/ax.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/estrongs/android/pop/app/editor/c.java com/estrongs/android/pop/app/imageviewer/ImageManager.java com/estrongs/fs/impl/media/b.java com/estrongs/fs/impl/media/e.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/estrongs/android/ui/d/a.java
00104	Check if the given path is directory	file	com/baidu/sapi2/share/ShareReceiver.java com/estrongs/android/pop/app/PopPreferenceActivity.java com/estrongs/android/pop/view/FileExplorerActivity.java com/estrongs/android/ui/preference/FtpServerPreference.java
00150	Send IMSI over Internet	phone	com/estrongs/android/pop/utils/bw.java
00083	Query the IMEI number	collection telephony	com/baidu/sapi2/Utils.java com/estrongs/android/pop/view/FileExplorerActivity.java
00189	Get the content of a SMS message	sms	com/estrongs/android/pop/app/editor/c.java
00188	Get the address of a SMS message	sms	com/estrongs/android/pop/app/editor/c.java
00200	Query data from the contact list	collection contact	com/estrongs/android/pop/app/editor/c.java

00201	Query data from the call log	collection calllog	com/estrongs/android/pop/app/editor/c.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/estrongs/android/pop/app/editor/c.java com/estrongs/android/util/ah.java com/estrongs/fs/impl/media/b.java
00123	Save the response to JSON after connecting to the remote server	network command	com/baidu/sapi2/loginshare/Sharer.java com/estrongs/android/pop/spfs/facebook/FacebookFileSystem.java com/estrongs/android/pop/spfs/flickr/FlickrFileSystem.java
00054	Install other APKs from file	reflection	com/estrongs/android/pop/app/b.java com/estrongs/android/pop/view/utils/AppRunner.java com/estrongs/android/ui/h/c.java com/estrongs/android/ui/theme/ai.java
00036	Get resource file from res/raw directory	reflection	com/dropbox/client2/android/AndroidAuthSession.java com/estrongs/android/ui/theme/ai.java
00004	Get filename and put it to JSON object	file collection	com/estrongs/fs/b/q.java
00039	Start a web server	control network	com/estrongs/a/b/e.java com/jcraft/jsch/PortWatcher.java
00058	Connect to the specific WIFI network	wifi control	com/estrongs/android/f/h.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.WRITE_SETTINGS, android.permission.INTERNET, android.permission.SET_WALLPAPER, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.READ_PHONE_STATE, android.permission.VIBRATE
Other		android.permission.CHANGE_WIFI_STATE, com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.BLUETOOTH,

Common Permissions	5/44	android.permission.BLUETOOTH_ADMIN, android.permission.ACCESS_SUPERUSER

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
dl.ops.baidu.com	IP: 180.97.107.48 Country: China Region: Jiangsu City: Nanjing
123.125.114.161	IP: 123.125.114.161 Country: China Region: Beijing City: Beijing
180.149.132.118	IP: 180.149.132.118 Country: China Region: Beijing City: Beijing
t.cn	IP: 123.56.139.83 Country: China Region: Zhejiang City: Hangzhou
	IP: 119.75.220.29 Country: China

119.75.220.29	Region: Beijing City: Beijing
123.125.115.81	IP: 123.125.115.81 Country: China Region: Beijing City: Beijing
dwz.cn	IP: 182.61.200.113 Country: China Region: Beijing City: Beijing
wappass.baidu.com	IP: 45.113.194.210 Country: China Region: Beijing City: Beijing
pcs.baidu.com	IP: 111.63.96.140 Country: China Region: Hebei City: Shijiazhuang
passport.baidu.com	IP: 45.113.194.250 Country: China Region: Beijing City: Beijing
hmma.baidu.com	IP: 103.235.46.195 Country: Hong Kong Region: Hong Kong City: Hong Kong
220.181.111.48	IP: 220.181.111.48 Country: China Region: Beijing City: Beijing
	IP: 39.156.66.111

openapi.baidu.com	Country: China Region: Beijing City: Beijing
m.baidu.com	IP: 103.235.46.39 Country: Hong Kong Region: Hong Kong City: Hong Kong

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
dl.ops.baidu.com	ok	**IP:** 180.97.107.48 **Country:** China **Region:** Jiangsu **City:** Nanjing **Latitude:** 32.061668 **Longitude:** 118.777779 **View:** Google Map
www.dropbox.com	ok	**IP:** 162.125.66.18 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
0.esfileexplorer.duapp.com	ok	No Geolocation information available.
api.flickr.com	ok	**IP:** 18.66.233.22 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499

		Longitude: -122.346199 **View:** Google Map
graph.facebook.com	ok	**IP:** 157.240.224.12 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.amazon.com	ok	**IP:** 13.227.147.135 **Country:** Germany **Region:** Bayern **City:** Munich **Latitude:** 48.137428 **Longitude:** 11.575490 **View:** Google Map
www.protocol	ok	No Geolocation information available.
123.125.114.161	ok	**IP:** 123.125.114.161 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
180.149.132.118	ok	**IP:** 180.149.132.118 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map

farm1s.static.flickr.com	ok	No Geolocation information available.
127.0.0.1	ok	IP: 127.0.0.1 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
v.17186.cn	ok	No Geolocation information available.
www.flickr.com	ok	IP: 18.66.233.20 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
t.cn	ok	IP: 123.56.139.83 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
update.estrongs.com	ok	IP: 138.113.136.126 Country: United States of America Region: California City: Monrovia Latitude: 34.142773 Longitude: -117.999565 View: Google Map
119.75.220.29	ok	IP: 119.75.220.29 Country: China Region: Beijing City: Beijing

		Latitude: 39.907501 **Longitude:** 116.397232 **View:** Google Map
10.23.238.184	ok	**IP:** 10.23.238.184 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
123.125.115.81	ok	**IP:** 123.125.115.81 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
dbl-chunlei-rd26.vm.baidu.com	ok	No Geolocation information available.
flickr.com	ok	**IP:** 18.66.233.20 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
dwz.cn	ok	**IP:** 182.61.200.113 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
		IP: 45.113.194.210

wappass.baidu.com	ok	**Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
pcs.baidu.com	ok	**IP:** 111.63.96.140 **Country:** China **Region:** Hebei **City:** Shijiazhuang **Latitude:** 38.041389 **Longitude:** 114.478607 **View:** Google Map
passport.qatest.baidu.com	ok	No Geolocation information available.
api.instagram.com	ok	**IP:** 157.240.224.63 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.estrongs.com	ok	**IP:** 138.113.136.126 **Country:** United States of America **Region:** California **City:** Monrovia **Latitude:** 34.142773 **Longitude:** -117.999565 **View:** Google Map
www.droid.sk	ok	**IP:** 104.21.73.231 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

passport.baidu.com	ok	IP: 45.113.194.250 Country: China Region: Beijing City: Beijing Latitude: 39.907501 Longitude: 116.397232 View: Google Map
hmma.baidu.com	ok	IP: 103.235.46.195 Country: Hong Kong Region: Hong Kong City: Hong Kong Latitude: 22.285521 Longitude: 114.157692 View: Google Map
wappass.qatest.baidu.com	ok	No Geolocation information available.
www.estongs.com	ok	No Geolocation information available.
220.181.111.48	ok	IP: 220.181.111.48 Country: China Region: Beijing City: Beijing Latitude: 39.907501 Longitude: 116.397232 View: Google Map
192.168.1.21	ok	IP: 192.168.1.21 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
passport.rdtest.baidu.com	ok	No Geolocation information available.

db-infbk-online-17.db01.baidu.com	ok	No Geolocation information available.
openapi.baidu.com	ok	**IP:** 39.156.66.111 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
m.facebook.com	ok	**IP:** 157.240.224.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
m.baidu.com	ok	**IP:** 103.235.46.39 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **View:** Google Map

EMAILS

EMAIL	FILE
contact@estrongs.com	com/estrongs/android/pop/f.java
contact@estrongs.com	com/estrongs/android/util/o.java
passw0rd@192.168	com/estrongs/android/pop/a/a.java

v.stan4ev@gmail.com	com/estrongs/android/pop/esclasses/a/b.java
___عمرumarhoj@gmail.com___شغل	com/estrongs/android/pop/esclasses/a/a.java
smachj@gmail.cz___zapno	com/estrongs/android/pop/esclasses/a/e.java
support@dropbox.com	com/dropbox/client2/android/AndroidAuthSession.java
zlib@openssh.com	com/jcraft/jsch/JSch.java
auth-agent@openssh.com	com/jcraft/jsch/Channel.java
auth-agent@openssh.com keepalive@jcraft.com zlib@openssh.com	com/jcraft/jsch/Session.java
auth-agent-req@openssh.com	com/jcraft/jsch/RequestAgentForwarding.java
auth-agent@openssh.com	com/jcraft/jsch/ChannelAgentForwarding.java

TRACKERS

TRACKER	CATEGORIES	URL
Baidu Mobile Stat	Analytics	https://reports.exodus-privacy.eu.org/trackers/101

HARDCODED SECRETS

POSSIBLE SECRETS

boundary=3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f

4fc742e0-4a10-11cf-8273-00aa004ae673

66f9c1cb708b4b9b9c96ac329260f536

3e504de3df373ce5e1080f3b9c33afba

308201e53082014ea00302010202044e17e115300d06092a864886f70d01010505003037310b3009060355040613025553311030 0e060355040a1307416e64726f69643116301406035504031 30d416e64726f69642044656275675730819f300d06092a864886f70d010101050003818d00308189028181009675 9fe5abea6a0757039b92adc68d672efa84732c3f959408e12efa264545c61f23141026a6d01eceeeaa13ec7087087e5894a3363da8bf5c69ed93657a6890738a80998e4ca22dc94848f30e2d0e1890000ae2cddf543b20c0c3828deca6c7944b5ecd21a9d18c988b2b3e54517dafbc34b48e801bb1321e0fa49e4d575d7f0203010001300d06092a864886f70d0101050500038181002b6d4b65bcfa6ec7bac97ae6d878064d47b3f9f8da654995b8ef4c385bc4fbfbb7a987f60783ef0348760c0708acd4b7e63f0235c35a4fbcd5ec41b3b4cb295feaa7d5c27fa562a02562b7e1f4776b85147be3e295714986c4a9a07183f48ea09ae4d3ea31b88d0016c65b93526b9c45f2967c3d28dee1aff5a5b29b9c2c8639

12345778-1234-abcd-ef00-0123456789ac

308202223082018b02044bd207bd300d06092a864886f70d01010405003058310b3009060355040613025553310b3009060355040813024341311630140603550407130d53616e204672616e636973636f3110300e060355040a130744726f70626f783112301006035504031309546f6d204d65796572301e170d313030343233323034393031 5a170d343030343135323034393031 5a3058310b3009060355040613025553310b3009060355040813024341311630140603550407130d53616e204672616e636973636f3110300e060355040a130744726f70626f783112301006035504031309546f6d204d6579657230819f300d06092a864886f70d010101050003818d00308189028181009ac1595d0ab278a9577f0ca5a14144f96eccde75f5616f36172c562fab0e98c48ad7d64f1091c6cc11ce084a4313d522f899378d312e112a748827545146a779defa7c31d8c00c2ed73135802f6952f59798579859e0214d4e9c0554b53b26032a4d2dfc2f62540d776df2ea70e2a6152945fb53fef5bac5344251595b729d48102030100013 00d06092a864886f70d01010405000381810055c425d94d036153203dc0bbeb3516f94563b102fff39c3d4ed91278db24fc4424a244c2e59f03bbfea59404512b8bf74662f2a32e37eafa2ac904c31f99cfc21c9ff375c977c432d3b6ec22776f28767d0f292144884538c3d5669b568e4254e4ed75d9054f75229ac9d4ccd0b7c3c74a34f07b7657083b2aa76225c0c56ffc

8a885d04-1ceb-11c9-9fe8-08002b104860

3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f

09cfe7214aec69fbda2b044b64305055

12345778-1234-abcd-ef00-0123456789ab

4b324fc8-1670-01d3-1278-5a47bf6ee188

d5b41a6c97344e3d8835e9d9a8fb17f6
BPZEkGy6js8a6M86Gw7q5E4yACTKVFqX

SCAN LOGS

Timestamp	Event	Error
2026-02-04 22:08:21	Generating Hashes	OK
2026-02-04 22:08:21	Extracting APK	OK
2026-02-04 22:08:21	Unzipping	OK
2026-02-04 22:08:21	Parsing APK with androguard	OK
2026-02-04 22:08:21	Extracting APK features using aapt/aapt2	OK
2026-02-04 22:08:21	Getting Hardcoded Certificates/Keystores	OK
2026-02-04 22:08:23	Parsing AndroidManifest.xml	OK
2026-02-04 22:08:23	Extracting Manifest Data	OK

2026-02-04 22:08:23	Manifest Analysis Started	OK
2026-02-04 22:08:23	Performing Static Analysis on: ES File Explorer (com.estrongs.android.pop)	OK
2026-02-04 22:08:24	Fetching Details from Play Store: com.estrongs.android.pop	OK
2026-02-04 22:08:25	Checking for Malware Permissions	OK
2026-02-04 22:08:25	Fetching icon path	OK
2026-02-04 22:08:25	Library Binary Analysis Started	OK
2026-02-04 22:08:25	Analyzing lib/x86/libsapi_so_1.so	OK
2026-02-04 22:08:25	Analyzing lib/x86/libmyaes.so	OK
2026-02-04 22:08:25	Analyzing lib/armeabi/libsapi_so_1.so	OK
2026-02-04 22:08:25	Analyzing lib/armeabi/libmyaes.so	OK
2026-02-04 22:08:25	Analyzing apktool_out/lib/x86/libsapi_so_1.so	OK

2026-02-04 22:08:25	Analyzing apktool_out/lib/x86/libmyaes.so	OK
2026-02-04 22:08:25	Analyzing apktool_out/lib/armeabi/libsapi_so_1.so	OK
2026-02-04 22:08:25	Analyzing apktool_out/lib/armeabi/libmyaes.so	OK
2026-02-04 22:08:25	Reading Code Signing Certificate	OK
2026-02-04 22:08:25	Running APKiD 3.0.0	OK
2026-02-04 22:08:27	Detecting Trackers	OK
2026-02-04 22:08:27	Decompiling APK to Java with JADX	OK
2026-02-04 22:08:42	Converting DEX to Smali	OK
2026-02-04 22:08:42	Code Analysis Started on - java_source	OK
2026-02-04 22:08:42	Android SBOM Analysis Completed	OK
2026-02-04 22:08:45	Android SAST Completed	OK
2026-02-04 22:08:45	Android API Analysis Started	OK

2026-02-04 22:08:46	Android API Analysis Completed	OK
2026-02-04 22:08:47	Android Permission Mapping Started	OK
2026-02-04 22:08:50	Android Permission Mapping Completed	OK
2026-02-04 22:08:51	Android Behaviour Analysis Started	OK
2026-02-04 22:08:53	Android Behaviour Analysis Completed	OK
2026-02-04 22:08:53	Extracting Emails and URLs from Source Code	OK
2026-02-04 22:08:56	Email and URL Extraction Completed	OK
2026-02-04 22:08:56	Extracting String data from APK	OK
2026-02-04 22:08:56	Extracting String data from SO	OK
2026-02-04 22:08:56	Extracting String data from Code	OK
2026-02-04 22:08:56	Extracting String values and entropies from Code	OK

2026-02-04 22:08:56	Performing Malware check on extracted domains	OK
2026-02-04 22:09:08	Saving to Database	OK

Report Generated by - MobSF v4.4.5

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.