✓ APP SCORES

Security Score	50/100
Trackers Detection	6/432

FILE INFORMATION

File Name	wheelmap.apk
Size	19.96MB
MD5	c3d4298211daf80633cb87a1dfa11753
SHA1	94b3b556ef19449fd46502a4c3238e9b2920dbac
SHA256	c744c2238c34dad4e4002a5ee411a92140121d654d0b0a1f0aac2ba12a7a066f

APP INFORMATION

App Name	Aptoide				
Package Name	cm.aptoide.pt				
Main Activity	cm.aptoide.pt.view.MainActivity				
Target SDK	32	Min SDK	16	Max SDK	
Android Version Name	9.22.3.0	Android Version Code	12048		

2 / 11

EXPORTED ACTIVITIES

View All

2 / 11

EXPORTED SERVICES

View All

3 / 14

EXPORTED RECEIVERS

View All

1 / 8

EXPORTED PROVIDERS

View All

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: ST=Portugal
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2009-09-22 14:53:51+00:00
Valid To: 2034-09-16 14:53:51+00:00
Issuer: ST=Portugal
Serial Number: 0x4ab8e4ff
Hash Algorithm: sha1
md5: 99bd1872bc56b4b2619e731ae9cbdc6f
sha1: d590a7d792fd0331542d99faf9997641790773a9
sha256: 73534d45c1345a4783c7eff2cf6038551ab5fdf09673f32c68c3b0864baa80e4
sha512: 8a5562a7825800df284d47dab79fcae1ccde0c3c46b1a181696809ed270576b92718130131ffef402f4d2822e235879de1e91224d91f0f4c0a0b58d2d2bc5b43
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: aae7fc687c60f98a8b14c3a3b9da6abc420f3a320de9309f960ce7b628a3063e
Found 1 unique certificates
```

☰ APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.	
android.permission.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.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.	
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.	
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.	
android.permission.INSTALL_PACKAGES	SignatureOrSystem	directly install applications	Allows an application to install new or updated Android packages. Malicious applications can use this to add new applications with arbitrarily powerful permissions.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.	

Showing 1 to 10 of 23 entries

Previous 1 2 3 Next

ANDROID API

Search:

API	FILES
Android Notifications	
Base64 Decode	
Base64 Encode	
Certificate Handling	
Content Provider	
Crypto	
Dynamic Class and Dexloading	

API	FILES
Execute OS Command	
Get Android Advertising ID	
Get Installed Applications	

Showing 1 to 10 of 33 entries

Previous 1 2 3 4 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
cm.aptoide.pt.DeepLinkIntentReceiver	**Schemes**: file://, http://, aptoide://, aptoiderepo://, aptoideinstall://, aptoideauth://, aptoidesearch://, aptoidefeature://, market://, https://, **Hosts:** *.aptoide.com, app.aptoide.com, **Mime Types:** application/vnd.cm.aptoide.pt, **Paths:** /appcoins, /app, **Path Prefixes:** /download, **Path Patterns:** /editorial/.*,
com.facebook.CustomTabActivity	**Schemes**: @string/fb_login_protocol_scheme://, fbconnect://, **Hosts:** cct.cm.aptoide.pt,

Showing 1 to 2 of 2 entries

Previous 1 Next

NETWORK SECURITY

HIGH	WARNING	INFO	SECURE
0	**1**	**1**	**0**

Search:

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

Showing 1 to 2 of 2 entries

Previous 1 Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
1	**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.
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 3 of 3 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
1	12	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable upatched Android version Android 4.1-4.1.2, [minSdk=16]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.	
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.	
3	Launch Mode of activity (cm.aptoide.pt.view.MainActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
4	TaskAffinity is set for activity (cm.aptoide.pt.wallet.WalletInstallActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.	
5	**Content Provider** (cm.aptoide.pt.toolbox.ToolboxContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
6	**Activity** (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
7	TaskAffinity is set for activity (cm.aptoide.pt.DeepLinkIntentReceiver)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.	
8	**Activity** (cm.aptoide.pt.DeepLinkIntentReceiver) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
9	**Broadcast Receiver** (cm.aptoide.pt.install.InstalledBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
10	**Broadcast Receiver** (cm.aptoide.pt.widget.SearchWidgetProvider) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	

Showing 1 to 10 of 14 entries

Previous 1 2 Next

CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
1	**9**	**1**	**3**	**0**

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
1	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		
2	MD5 is a weak hash known to have hash collisions.	warning	**CWE:** CWE-327: Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	cm/aptoide/pt/download/FileDownloadTask.java cm/aptoide/pt/utils/AptoideUtils.java e/h/a/k0/f.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
3	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	cm/aptoide/pt/preferences/PRNGFixes.java cm/aptoide/pt/utils/AptoideUtils.java io/sentry/util/u.java	
4	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		
5	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		
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		
7	IP Address disclosure	warning	**CWE:** CWE-200: Information Exposure **OWASP MASVS:** MSTG-CODE-2	cm/aptoide/pt/BuildConfig.java i/a/g/l.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	**OWASP MASVS:** MSTG-NETWORK-4		
9	App creates temp file. Sensitive information should never be written into a temp file.	warning	**CWE:** CWE-276: Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	c/n/b.java cm/aptoide/pt/account/view/PhotoFileGenerator.java	
10	This App uses SafetyNet API.	secure	**OWASP MASVS:** MSTG-RESILIENCE-7	cm/aptoide/pt/analytics/FirstLaunchAnalytics.java	

Showing 1 to 10 of 14 entries

Previous 1 2 Next

SHARED LIBRARY BINARY ANALYSIS

Search:

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libsentry-android.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.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libsentry.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.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	x86/libsentry-android.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.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86/libsentry.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.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libsentry-android.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.	**True** info The binary has the following fortified functions: ['__vsnprintf_chk']	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	arm64-v8a/libsentry.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.	**True** info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__memmove_chk']	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86_64/libsentry-android.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.	**True** info The binary has the following fortified functions: ['__vsnprintf_chk']	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/libsentry.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.	**True** info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__memmove_chk']	**True** info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	armeabi-v7a/libsentry-android.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.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi-v7a/libsentry.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.

Showing 1 to 10 of 16 entries

Previous 1 2 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/HY.pem

Showing 1 to 1 of 1 entries

Previous 1 Next

FIREBASE DATABASE ANALYSIS

Search:

TITLE	SEVERITY	DESCRIPTION
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

MALWARE LOOKUP

VirusTotal Report	Triage Report	MetaDefender Report	Hybrid Analysis Report

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 Build.SERIAL check network operator name check device ID check
Compiler	r8

Showing 1 to 2 of 2 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
SIM operator check
network operator name 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>
<tr><td>classes3.dex</td><td>Search:
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
Showing 1 to 1 of 1 entries
Previous 1 Next</td></tr>
</table>

Showing 1 to 3 of 3 entries

Previous 1 Next

BEHAVIOUR ANALYSIS

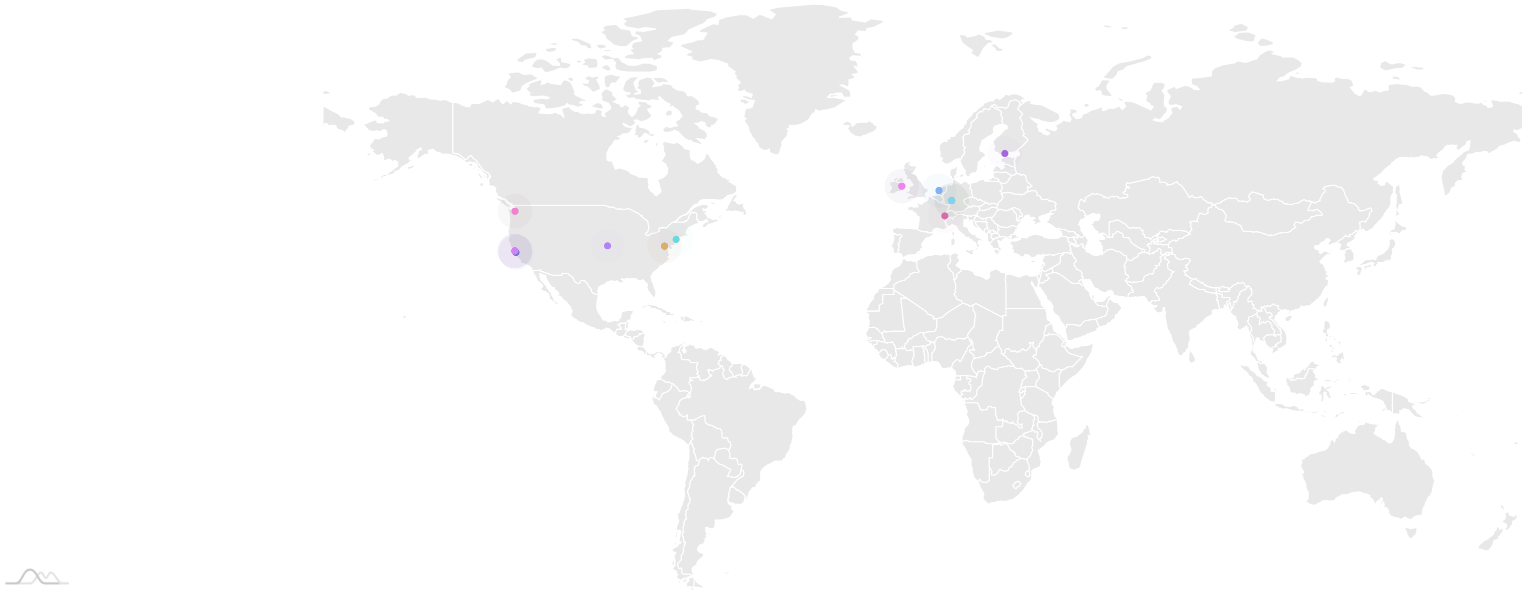
Search:

RULE ID	BEHAVIOUR	LABEL	FILES
00009	Put data in cursor to JSON object	file	io/rakam/api/b.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	cm/aptoide/pt/account/view/ImageInfoProvider.java
00012	Read data and put it into a buffer stream	file	
00013	Read file and put it into a stream	file	
00016	Get location info of the device and put it to JSON object	location collection	com/flurry/sdk/y5.java io/rakam/api/g.java
00022	Open a file from given absolute path of the file	file	
00023	Start another application from current application	reflection control	cm/aptoide/pt/utils/AptoideUtils.java
00030	Connect to the remote server through the given URL	network	
00034	Query the current data network type	collection network	com/flurry/sdk/w.java
00035	Query the list of the installed packages	reflection	cm/aptoide/pt/utils/AptoideUtils.java

Showing 1 to 10 of 30 entries

Previous 1 2 3 Next

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
api.aptoide.com	ok	**IP:** 18.165.122.76 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.indicative.com	ok	**IP:** 34.98.104.50 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
aptoi.de	ok	**IP:** 52.23.47.7 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
aptoide-mmp.aptoide.com	ok	**IP:** 52.17.172.88 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
blog.aptoide.com	ok	**IP:** 37.48.77.171 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
catappult.io	ok	**IP:** 3.164.68.17 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
cdn6.aptoide.com	ok	**IP:** 104.22.11.83 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
data.flurry.com	ok	**IP:** 74.6.138.66 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
diagnostics.rakam.io	ok	**IP:** 104.21.35.78 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
facebook.com	ok	**IP:** 157.240.205.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

Showing 1 to 10 of 30 entries

Previous 1 2 3 Next

URLS

Search:

URL	FILE
data:image	com/bumptech/glide/load/n/e.java
http://localhost/	retrofit2/Response.java
http://m.aptoide.com	cm/aptoide/pt/link/CustomTabsHelper.java
http://m.aptoide.com/account/password-recovery	cm/aptoide/pt/view/ActivityModule.java

URL	FILE
http://pool.img.aptoide.com/asf-store/ace60f6352f6dd9289843b5b0b2ab3d4_icon.png https://placeimg.com/640/480/any	cm/aptoide/pt/home/bundles/FakeBundleDataSource.java
http://schemas.android.com/apk/res/android	cm/aptoide/pt/util/PreferencesXmlParser.java
http://www.aptoide.com https://github.com/aptoide http://blog.aptoide.com/remote-tv-install http://www.aptoide.com/ http://aptoi.de/tv https://www.aptoide.com/legal/privacy?header=0&menu=0 http://www.aptoide.com/page/about https://www.aptoide.com/legal/terms?header=0&menu=0 https://www.aptoide.com/company/legal/account/delete?email=%s	Android String Resource
http://www.example.com http://m.aptoide.com	cm/aptoide/pt/link/CustomTabNativeReceiver.java
http://www.slf4j.org/codes.html#substitutelogger http://www.slf4j.org/codes.html#version_mismatch http://www.slf4j.org/codes.html#multiple_bindings http://www.slf4j.org/codes.html#replay http://www.slf4j.org/codes.html#unsuccessfulinit http://www.slf4j.org/codes.html#staticloggerbinder	k/b/c.java
https://89014bfa01a24259b961735ba5eda557@sentry.aptoide.com/23	cm/aptoide/pt/BuildConfig.java

Showing 1 to 10 of 38 entries

Previous 1 2 3 4 Next

EMAILS

Search:

EMAIL	FILE
4259b961735ba5eda557@sentry.aptoide	cm/aptoide/pt/BuildConfig.java
aptoide@aptoide.com support@aptoide.com 请通过suport@aptoide.com与技术支持人员 suport@aptoide.com	Android String Resource
filipo@emailo.como	com/aptoide/authentication/mock/MockAuthenticationService.java
support@aptoide.com	cm/aptoide/pt/AptoideApplication.java

Showing 1 to 4 of 4 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Flurry	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/25
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

TRACKER NAME ▲	CATEGORIES ♦	URL ♦
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

Showing 1 to 6 of 6 entries

Previous 1 Next

POSSIBLE HARDCODED SECRETS

▶ Show all **158** secrets

A STRINGS

From APK Resource

▶ Show all **37361** strings

From Code

▶ Show all **24222** strings

From Shared Objects

apktool_out/lib/armeabi-v7a/libsentry-android.so

▶ Show all **33** strings

apktool_out/lib/armeabi-v7a/libsentry.so

▶ Show all **1090** strings

apktool_out/lib/x86/libsentry-android.so

▶ Show all **33** strings

apktool_out/lib/x86/libsentry.so

▶ Show all **1100** strings

apktool_out/lib/arm64-v8a/libsentry-android.so

▶ Show all **33** strings

apktool_out/lib/arm64-v8a/libsentry.so

▶ Show all **1097** strings

apktool_out/lib/x86_64/libsentry-android.so

▶ Show all **33** strings

apktool_out/lib/x86_64/libsentry.so

▶ Show all **1096** strings

lib/armeabi-v7a/libsentry-android.so

▶ Show all **33** strings

lib/armeabi-v7a/libsentry.so

▶ Show all **1090** strings

lib/x86/libsentry-android.so

▶ Show all **33** strings

lib/x86/libsentry.so

▶ Show all **1100** strings

lib/arm64-v8a/libsentry-android.so

▶ Show all **33** strings

lib/arm64-v8a/libsentry.so

▶ Show all **1097** strings

lib/x86_64/libsentry-android.so

▶ Show all **33** strings

lib/x86_64/libsentry.so

▶ Show all **1096** strings

ACTIVITIES

▼ Showing all **11** activities

cm.aptoide.pt.view.MainActivity
cm.aptoide.pt.wallet.WalletInstallActivity
cm.aptoide.pt.account.view.LoginActivity

com.facebook.FacebookActivity
com.facebook.CustomTabActivity
cm.aptoide.pt.DeepLinkIntentReceiver
cm.aptoide.aptoideviews.base.MockActivity
com.facebook.CustomTabMainActivity
com.google.android.gms.auth.api.signin.internal.SignInHubActivity
com.google.android.gms.common.api.GoogleApiActivity
com.google.android.gms.ads.AdActivity

SERVICES

▼ Showing all **11** services

cm.aptoide.pt.account.AccountAuthenticatorService
cm.aptoide.pt.notification.PullingContentService
cm.aptoide.pt.install.DownloadService
cm.aptoide.pt.install.InstalledIntentService
com.google.android.gms.auth.api.signin.RevocationBoundService
androidx.work.impl.background.systemalarm.SystemAlarmService
androidx.work.impl.background.systemjob.SystemJobService
androidx.work.impl.foreground.SystemForegroundService
androidx.room.MultiInstanceInvalidationService
com.liulishuo.filedownloader.services.FileDownloadService$SharedMainProcessService
com.liulishuo.filedownloader.services.FileDownloadService$SeparateProcessService

RECEIVERS

▼ Showing all **14** receivers

cm.aptoide.pt.install.InstalledBroadcastReceiver
cm.aptoide.pt.link.CustomTabNativeReceiver
cm.aptoide.pt.install.CheckRootOnBoot
cm.aptoide.pt.install.RootInstallNotificationEventReceiver
cm.aptoide.pt.widget.SearchWidgetProvider
com.facebook.CurrentAccessTokenExpirationBroadcastReceiver

androidx.work.impl.utils.ForceStopRunnable$BroadcastReceiver
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryChargingProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryNotLowProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$StorageNotLowProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$NetworkStateProxy
androidx.work.impl.background.systemalarm.RescheduleReceiver
androidx.work.impl.background.systemalarm.ConstraintProxyUpdateReceiver
androidx.work.impl.diagnostics.DiagnosticsReceiver

PROVIDERS

▼ Showing all **8** providers

cm.aptoide.pt.toolbox.ToolboxContentProvider
androidx.core.content.FileProvider
com.facebook.internal.FacebookInitProvider
com.google.android.gms.ads.MobileAdsInitProvider
io.sentry.android.core.SentryInitProvider
io.sentry.android.core.SentryPerformanceProvider
androidx.lifecycle.ProcessLifecycleOwnerInitializer
com.flurry.android.agent.FlurryContentProvider

LIBRARIES

▼ Showing all **1** libraries

org.apache.http.legacy

SBOM

▼ Showing all **53** Versioned Packages

androidx.activity:activity@1.0.0
androidx.annotation:annotation-experimental@1.1.0
androidx.appcompat:appcompat-resources@1.2.0
androidx.appcompat:appcompat@1.2.0

```
androidx.arch.core:core-runtime@2.1.0
androidx.asynclayoutinflater:asynclayoutinflater@1.0.0
androidx.browser:browser@1.0.0
androidx.cardview:cardview@1.0.0
androidx.coordinatorlayout:coordinatorlayout@1.1.0
androidx.core:core-ktx@1.2.0
androidx.core:core@1.6.0
androidx.cursoradapter:cursoradapter@1.0.0
androidx.customview:customview@1.0.0
androidx.documentfile:documentfile@1.0.0
androidx.drawerlayout:drawerlayout@1.0.0
androidx.fragment:fragment@1.1.0
androidx.interpolator:interpolator@1.0.0
androidx.legacy:legacy-support-core-ui@1.0.0
androidx.legacy:legacy-support-core-utils@1.0.0
androidx.legacy:legacy-support-v13@1.0.0
androidx.legacy:legacy-support-v4@1.0.0
androidx.lifecycle:lifecycle-livedata-core@2.1.0
androidx.lifecycle:lifecycle-livedata@2.1.0
androidx.lifecycle:lifecycle-process@2.2.0
androidx.lifecycle:lifecycle-runtime@2.2.0
androidx.lifecycle:lifecycle-service@2.1.0
androidx.lifecycle:lifecycle-viewmodel@2.1.0
androidx.loader:loader@1.0.0
androidx.localbroadcastmanager:localbroadcastmanager@1.0.0
androidx.media:media@1.0.0
androidx.palette:palette@1.0.0
androidx.preference:preference@1.1.0
androidx.print:print@1.0.0
androidx.recyclerview:recyclerview@1.1.0
androidx.room:room-runtime@2.2.5
androidx.room:room-rxjava2@2.2.4
androidx.savedstate:savedstate@1.0.0
androidx.slidingpanelayout:slidingpanelayout@1.0.0
androidx.sqlite:sqlite-framework@2.1.0
androidx.sqlite:sqlite@2.1.0
androidx.startup:startup-runtime@1.0.0
androidx.swiperefreshlayout:swiperefreshlayout@1.0.0
```

androidx.tracing:tracing@1.0.0
androidx.transition:transition@1.2.0
androidx.vectordrawable:vectordrawable-animated@1.1.0
androidx.vectordrawable:vectordrawable@1.1.0
androidx.versionedparcelable:versionedparcelable@1.1.1
androidx.viewpager2:viewpager2@1.0.0
androidx.viewpager:viewpager@1.0.0
androidx.work:work-runtime-ktx@2.7.1
androidx.work:work-runtime@2.7.1
com.google.android.material:material@1.2.0-beta01
com.google.dagger:dagger@2.40

▼ Showing all **85** Packages

b.a.a
b.b.a
bolts
c.a
c.b.a.a
c.b.a.b
c.b.a.c
c.c
c.d
c.e
c.f.a.a
c.f.a.b
c.f.b
c.g
c.h
c.i.a
c.j.a
c.k.a.a
c.l.a
c.l.b
c.m.a
c.n
c.o.a
c.p
c.q.a
c.r.a

c.s

c.t.a.a

cm.aptoide.accountmanager

cm.aptoide.analytics

cm.aptoide.analyticsimplementation

cm.aptoide.aptoideanalyticscore

cm.aptoide.aptoideviews

cm.aptoide.pt

com.airbnb.epoxy

com.airbnb.lottie

com.aptoide.aptoide_ab_testing

com.aptoide.authentication

com.aptoide.authenticationrx

com.astuetz

com.bumptech.glide

com.fasterxml.jackson.annotation

com.fasterxml.jackson.core

com.fasterxml.jackson.databind

com.flurry.android.agent

com.flurry.sdk

com.liulishuo.filedownloader.exception

com.liulishuo.filedownloader.message

com.liulishuo.filedownloader.model

com.liulishuo.filedownloader.services

com.trello.rxlifecycle

d.a.a

defpackage

e.a.a

e.b.a.a

e.c.a.a.a.base

e.d.a

e.e.a

e.e.b.a.a

e.e.b.b

e.e.c.a.a

e.f.a.a

e.g.a.a

e.g.a.b.a.a

e.g.a.b.b.a
e.g.a.b.c.a
e.g.a.c
e.g.a.d
e.g.b
e.h.a
e.i
f
g.a.a.a
h.a
i.a
io.rakam.api
io.reactivex.exceptions
io.sentry
j
javax.inject
k.a
k.b
org.parceler
retrofit2
rx

FILES

▶ Show all **4061** files

Version v4.2.7