✓ APP SCORES

Security Score **38/100**

Trackers Detection

0/432

FILE INFORMATION

File Name 5251a356421340a45c8dc6d431ef8a8cbca4078a0305a87f4fbd552e9fc0793e.apk

Size 2.69MB

MD5 2ddbc785cd696041c5b0c3bd1a8af552

SHA1 1269636a5197ee7a1402e406c91177bf6a149652

SHA256 5251a356421340a45c8dc6d431ef8a8cbca4078a0305a87f4fbd552e9fc0793e

APP INFORMATION

App Name Free Followers

Package Name com.XPhantom.id

Main Activity com.XPhantom.id.MainActivity

Target SDK 21 **Min SDK** 8 **Max SDK**

Android Version Name 1.0 **Android Version Code** 1

1

ACTIVITIES

View

1

SERVICES

View

1

RECEIVERS

View

0

PROVIDERS

View

Exported Activities **0**

Exported Services **0**

Exported Receivers **1**

Exported Providers **0**

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=debugging
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-09-23 11:57:06+00:00
Valid To: 3015-01-25 11:57:06+00:00
Issuer: C=debugging
Serial Number: 0x333a0b9b
Hash Algorithm: sha256
md5: c13f92d0397da7423a4142bfa9a5873e
sha1: d122d9adc3e5d5ff346b32c0413f5cf3a3cc4658
sha256: 022a1ed9feb0e6c9826df99c58350b7789a71ad51f142f40449f91d58c0278c1
sha512:
f8ac9decdd241b79396dddeb68c9f2d3d1c909bcee3a32f43e286b7ab8211de05d8f1c9e3e8328c85fd4c948e7edeb2b90c45a09f09050
d40433d5b2a90c6e4d
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: a09cf4ea0b0d8f9b0db4f186cc988aa8b975f458a68003aea0a6af81570420ca
Found 1 unique certificates
```

☰ APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.	
android.permission.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.INTERNET	normal	full Internet access	Allows an application to create network sockets.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.	
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.	
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.	
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.REQUEST_INSTALL_PACKAGE	unknown	Unknown permission	Unknown permission from android reference	
android.permission.SET_WALLPAPER	normal	set wallpaper	Allows the application to set the system wallpaper.	
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.	

Showing 1 to 10 of 12 entries

Previous 1 2 Next

ANDROID API

Search:

API	FILES
Execute OS Command	

API	FILES
Get System Service	
Inter Process Communication	
Java Reflection	
Local File I/O Operations	
Sending Broadcast	
Starting Service	

Showing 1 to 7 of 7 entries

Previous 1 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

NETWORK SECURITY

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
No data available in table			

Showing 0 to 0 of 0 entries

Previous Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
0	1	1

Search:

TITLE	SEVERITY	DESCRIPTION

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

Showing 1 to 2 of 2 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
2	2	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable upatched Android version Android 2.2-2.2.3, [minSdk=8]	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	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.	
3	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
4	**Broadcast Receiver** (com.XPhantom.id.BootReceiver) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** android.permission.RECEIVE_BOOT_COMPLETED [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.	

Showing 1 to 4 of 4 entries

Previous 1 Next

CODE ANALYSIS

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

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
1	Debug configuration enabled. Production builds must not be debuggable.	high	**CWE:** CWE-919: Weaknesses in Mobile Applications **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-RESILIENCE-2	com/XPhantom/id/BuildConfig.java	

Showing 1 to 1 of 1 entries

Previous 1 Next

SHARED LIBRARY BINARY ANALYSIS

No Shared Objects found.

Search:

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

Showing 0 to 0 of 0 entries

Previous Next

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

APKiD ANALYSIS

Search:

<table>
<tr><th>DEX</th><th>DETECTIONS</th></tr>
<tr><td>classes.dex</td><td>Search:
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
Showing 1 to 1 of 1 entries
Previous 1 Next</td></tr>
</table>

Showing 1 to 1 of 1 entries

Previous 1 Next

QUARK ANALYSIS

Search:

POTENTIAL MALICIOUS BEHAVIOUR	EVIDENCE
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

ABUSED PERMISSIONS

Top Malware Permissions	**11**/24	Other Common Permissions	
android.permission.SYSTEM_ALERT_WINDOW, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.SET_WALLPAPER, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_CONTACTS, android.permission.READ_SMS, android.permission.ACCESS_FINE_LOCATION, android.permission.WAKE_LOCK, android.permission.INTERNET, android.permission.CAMERA			

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

SERVER LOCATIONS

DOMAIN MALWARE CHECK

URLS

FIREBASE DATABASE

EMAILS

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

POSSIBLE HARDCODED SECRETS

"password" : "..."

A STRINGS

From APK Resource

"text1" : " Pay 1000/Rs to Get UnlocK Key on that number +923044466333 "
"text" : "You are Hacked By Anonymous Group"
"password" : "..."
"app_name" : "Free Followers"
"hello" : "Hello World!"

From Code

com.XPhantom.id.MyService
com.adrt.CONNECT
android.intent.action.BOOT_COMPLETED
LogCat
com.adrt.BREAKPOINT_HIT
com.adrt.FIELDS
Abdullah@
variableValues
variableKinds
path
logcat -v threadtime
variables
fields
window
stackLocations
Ваш текст
package

fieldKinds

fieldValues

stackLocationKinds

com.adrt.STOP

com.aide.ui

lines

com.adrt.LOGCAT_ENTRIES

stackMethods

layout_inflater

From Shared Objects

ACTIVITIES

com.XPhantom.id.MainActivity

SERVICES

com.XPhantom.id.MyService

RECEIVERS

com.XPhantom.id.BootReceiver

PROVIDERS

LIBRARIES

FILES

resources.arsc

classes.dex

AndroidManifest.xml

res/drawable-xhdpi-v4/ic_launcher.png

res/drawable-xhdpi-v4/ic_launcher_background.png

res/drawable-xhdpi-v4/ic_launcher_round.png

res/drawable-hdpi-v4/ic_launcher.png

res/drawable-hdpi-v4/ic_launcher_background.png

res/drawable-hdpi-v4/ic_launcher_round.png

res/drawable-xxhdpi-v4/ic_launcher.png

res/drawable-xxhdpi-v4/ic_launcher_background.png

res/drawable-xxhdpi-v4/ic_launcher_round.png

res/layout/main.xml

res/drawable-mdpi-v4/ic_launcher.png

res/drawable-mdpi-v4/ic_launcher_round.png res/drawable-mdpi-v4/ic_launcher_bacground.png

META-INF/DEBUGGIN.SF

META-INF/DEBUGGIN.RSA

META-INF/MANIFEST.MF

Version v3.9.4 Beta