MOBSF

ANDROID STATIC ANALYSIS REPORT

Phone Tracker (2.3.8)

File Name:	Spy Phone Labs Phone Tracker_merged.apk
Package Name:	com.phonetrackerofficial1
Scan Date:	Aug. 12, 2024, 3:31 a.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	7	1	1	1

FILE INFORMATION

File Name: Spy Phone Labs Phone Tracker_merged.apk
Size: 0.99MB
MD5: 07d3270d80397002d065d18ff7bc7dc8
SHA1: 0106d6fff8fecf40a13fe78b6e72cd6dcfb192db
SHA256: 43a200f04cc2ce5937a16638c83d0722cd8d44d9663908f948452a5439fcf664

APP INFORMATION

App Name: Phone Tracker
Package Name: com.phonetrackerofficial1
Main Activity: com.phonetrackerofficial1.MyActivity
Target SDK: 33
Min SDK: 23
Max SDK:
Android Version Name: 2.3.8
Android Version Code: 163

APP COMPONENTS

Activities: 6
Services: 9
Receivers: 8
Providers: 2
Exported Activities: 0
Exported Services: 0
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: O=PhoneParent
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-09-21 18:54:41+00:00
Valid To: 2112-08-28 18:54:41+00:00
Issuer: O=PhoneParent
Serial Number: 0x41301afc
Hash Algorithm: sha256
md5: 200b741f0dcaa0dfcb19fd634f5d2811
sha1: 5f61beb9591adbdf9da5b141a1ef35cdc0944c8c
sha256: 460e9b7800d2d23653293ab0d6242c1c291de88ce15ce40b80078cd7185e2aa0
sha512: b5989ee6aa91dffca9df83bc0aebca175e039d634c7b2b037ff4caf6fb65e05e5c61623891ae2f076aed96b30264944a20cdba3fd7d6c312800e5244dfd94b66
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 90e989176bf3c923283f9d5373143e89e05f08e83b1b6f992e320dc2489fd4a1
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

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

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **2** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Broadcast Receiver (com.phonetrackerofficial1.BootReceiver) 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.
3	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **4** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				D/k.java D0/a.java D0/j.java D0/k.java F/a.java P/AbstractC0064b.java P/C0065c.java P/d.java P/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	P/i.java P/l.java P/t.java P/u.java Q/A.java Q/i.java Q/l.java Q/m.java Q/p.java Q/w.java S/H.java T/A.java T/AbstractBinderC0085a.java T/AbstractC0087c.java T/D.java T/H.java T/T.java T/W.java T/X.java T/Y.java T/a0.java T/g0.java T/k0.java X/b.java Y/n.java b/AbstractC0157m.java b/C0156l.java b/LayoutInflater$Factory2C0149e.java b/q.java com/phonetrackerofficial1/BootReceiver.java com/phonetrackerofficial1/GPSSchedService.java com/phonetrackerofficial1/GPSService.java com/phonetrackerofficial1/MyActivity.java com/phonetrackerofficial1/PhoneLookup.java com/phonetrackerofficial1/actR

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ateApp.java com/phonetrackerofficial1/deleteAccount.java com/phonetrackerofficial1/recAcctCreated.java com/phonetrackerofficial1/recGeoFence.java com/phonetrackerofficial1/recLocUpdate.java com/phonetrackerofficial1/recStartGeoFence.java com/phonetrackerofficial1/svcCheckIn.java com/phonetrackerofficial1/svcFirebaseMessaging.java com/phonetrackerofficial1/svcStartGeoFence.java f/g.java g/MenuItemC0225c.java k0/C0273a.java l/AbstractC0289b.java l/AbstractC0292e.java l/C0287B.java l0/a.java n/AbstractC0305a.java n/b.java n/f.java n0/c.java o/d.java o/f.java o/g.java o/h.java o/l.java p0/g.java p0/n.java u/C0348b.java v/AbstractC0351B.java v/AbstractC0353D.java v/AbstractC0368n.java v/l.java v/v.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				y0/b.java y0/c.java
2	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	J/B.java J/F.java J/H.java
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	y0/b.java
4	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	y0/c.java
5	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	m/c.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/24	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_CONTACTS, android.permission.WAKE_LOCK
Other Common Permissions	6/45	android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.CHANGE_WIFI_STATE, android.permission.CHANGE_NETWORK_STATE, com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE

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

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
support.google.com	ok	**IP:** 142.251.36.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.phonetracker.com	ok	**IP:** 107.23.235.145 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
www.aboutads.info	ok	**IP:** 3.161.119.13 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
play.google.com	ok	**IP:** 142.251.36.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
phonetracker95gpsonly.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://phonetracker95gpsonly.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
u0013android@android.com u0013android@android.com0	Q/v.java
support@phonetracker.com	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://phonetracker95gpsonly.firebaseio.com"
"google_api_key" : "AIzaSyCsq_WNdDBCOF0thSFE2eYNzii0JgcSkEc"
"google_crash_reporting_api_key" : "AIzaSyCsq_WNdDBCOF0thSFE2eYNzii0JgcSkEc"

PLAYSTORE INFORMATION

Title: Spy Phone Labs Phone Tracker

Score: 4.0324674 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Tools **Play Store URL:** com.phonetrackerofficial1

Developer Details: PhoneTracker.com- Spy Phone Labs LLC, PhoneTracker.com-+Spy+Phone+Labs+LLC, 680 RT 211 East, Ste 3B #123, Middletown, NY 10941, http://phonetracker.com, support@phonetracker.com,

Release Date: Aug 20, 2014 **Privacy Policy:** Privacy link

Description:

Phone Tracker 2.2.9 New! Phone Parent ® Phone Tracker provides FREE GPS, Contacts, Apps Installed and Location Activity Tracking of Phone. Spy Phone Labs LLC is the World Leader in providing free phone tracking software that enables parents to monitor their child's activities on his or her Android® smartphone. New Panic Button added for emergency situations. Added Find Phone and Beep Phone. Added Reverse Phone Number lookup. Added Lookup of Installed Apps on Phone. Millions of users worldwide have downloaded our FREE Phone Tracking apps. Version 2.2.7 now shows FREE Contacts GPS and Location activity data. By installing Phone Tracker on a smartphone, parents can monitor important information to help keep their child safe and secure, including the location of their child's phone, with whom their child has been communicating, and the websites that their child has been visiting, all from the comfort of their home or office computer. This is a free download from Spy Phone Labs LLC that can be used to monitor activity on as many as five different smartphones from the same account. HOW IT WORKS: After installing Phone Tracker software on your child's Android® smartphone, which takes approximately 30 seconds, you can monitor the following data: (1) GPS location data on a plotted map (updated every 30 minutes). 2. Phone Contacts which will include names and phone numbers are copied off phone on completing installation and sent to your Control Panel account. All of this data is sent to our servers at phonetracker.com and available 24 hours a day, 7 days a week, from an account that can be established on our secure website at PhoneTracker.com. IMPORTANT INFORMATION ABOUT THIS SOFTWARE: PHONE TRACKER IS A PRODUCT OF SPY PHONE LABS LLC, A NEW JERSEY BASED COMPANY. PHONE TRACKER IS NOT INTENDED TO BE USED, AND MAY NOT BE USED, TO SECRETLY OR SURREPTITIOUSLY OBTAIN DATA FROM A MOBILE PHONE WITHOUT THE USER'S KNOWLEDGE OR CONSENT. DOWNLOADING PHONE TRACKER ™ ON ANY PHONE WITHOUT THE KNOWLEDGE AND CONSENT OF THE OWNER IS STRICTLY PROHIBITED AND MAY BE A VIOLATION OF FEDERAL AND/OR STATE PRIVACY LAWS. TO DETER UNLAWFUL AND/OR UNAUTHORIZED USE OR MISUSE OF PHONE TRACKER SOFTWARE, AN ICON WILL APPEAR ON ANY PHONE ON WHICH THE SOFTWARE HAS BEEN DOWNLOADED AND A NOTIFICATION WILL APPEAR ON THE PHONE AT REGULAR INTERVALS NOTIFYING THE USER OF THE MOBILE PHONE THAT DATA RELATING TO THE USER'S LOCATION AND/OR SMARTPHONE ACTIVITIES ARE BEING

REMOTELY MONITORED, RECORDED AND ARCHIVED. SPY PHONE LABS LLC IS NOT RESPONSIBLE FOR ANY UNAUTHORIZED USE OR MISUSE OF PHONE TRACKER SOFTWARE. IF YOU BELIEVE THAT DATA HAS BEEN OBTAINED FROM YOUR PHONE WITHOUT PERMISSION THROUGH THE USE OF PHONE TRACKER SOFTWARE, PLEASE CONTACT YOUR LOCAL LAW ENFORCEMENT OFFICIALS PROMPTLY. To deter unlawful and/or unauthorized use of the Phone Tracker software and/or the secret or surreptitious gathering of data without the user's permission, an icon will appear on any smartphone on which Phone Tracker has been downloaded, and notifications are sent to the smartphone to notify the user that Phone Tracker is running on the phone, and that certain data from the phone is being monitored and collected remotely. Installing this app allows you to view information and data transmitted by a phone or mobile device to Spy Phone Labs LLC (SPL) and PhoneTracker.com. By logging into our website at phonetracker.com, you, as the recipient of this information and data, consent to its receipt and acknowledge that it is not spam.

SCAN LOGS

Timestamp	Event	Error
2024-08-12 03:31:46	Generating Hashes	OK
2024-08-12 03:31:46	Extracting APK	OK
2024-08-12 03:31:46	Unzipping	OK
2024-08-12 03:31:46	Getting Hardcoded Certificates/Keystores	OK
2024-08-12 03:31:47	Parsing AndroidManifest.xml	OK
2024-08-12 03:31:47	Parsing APK with androguard	OK
2024-08-12 03:31:48	Extracting Manifest Data	OK

2024-08-12 03:31:48	Performing Static Analysis on: Phone Tracker (com.phonetrackerofficial1)	OK
2024-08-12 03:31:48	Fetching Details from Play Store: com.phonetrackerofficial1	OK
2024-08-12 03:31:48	Manifest Analysis Started	OK
2024-08-12 03:31:48	Checking for Malware Permissions	OK
2024-08-12 03:31:48	Fetching icon path	OK
2024-08-12 03:31:48	Library Binary Analysis Started	OK
2024-08-12 03:31:48	Reading Code Signing Certificate	OK
2024-08-12 03:31:48	Failed to get signature versions	CalledProcessError(1, ['/jdk-20.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/07d3270d80397002d065d18ff7bc7dc8/07d3270d80397002d065d18ff7bc7dc8.apk'])
2024-08-12 03:31:48	Running APKiD 2.1.5	OK
2024-08-12 03:31:49	Detecting Trackers	OK

2024-08-12 03:31:49	Decompiling APK to Java with jadx	OK
2024-08-12 03:31:54	Converting DEX to Smali	OK
2024-08-12 03:31:54	Code Analysis Started on - java_source	OK
2024-08-12 03:31:57	Android SAST Completed	OK
2024-08-12 03:31:57	Android API Analysis Started	OK
2024-08-12 03:32:00	Android Permission Mapping Started	OK
2024-08-12 03:32:02	Android Permission Mapping Completed	OK
2024-08-12 03:32:02	Finished Code Analysis, Email and URL Extraction	OK
2024-08-12 03:32:02	Extracting String data from APK	OK
2024-08-12 03:32:02	Extracting String data from Code	OK
2024-08-12 03:32:02	Extracting String values and entropies from Code	OK

2024-08-12 03:32:03	Performing Malware check on extracted domains	OK
2024-08-12 03:32:04	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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.