


**ID:** 715054
**Sample Name:** Locus Map 4 Outdoor Navigation_v4.12.0_apkpure.com.xapk
**Cookbook:** defaultandroidfilecookbook.jbs
**Time:** 15:43:17
**Date:** 03/10/2022
**Version:** 36.0.0 Rainbow Opal

# Table of Contents


Table of Contents 2
Android Analysis Report Locus Map 4 Outdoor Navigation_v4.12.0_apkpure.com.xapk 3
- Overview 3
  - General Information 3
  - Detection 3
  - Signatures 3
  - Classification 3
- Yara Signatures 3
- Snort Signatures 3
- Joe Sandbox Signatures 3
- Mitre Att&ck Matrix 3
- Antivirus, Machine Learning and Genetic Malware Detection 4
  - Initial Sample 4
  - Dropped Files 4
  - Domains 4
  - URLs 4
- Domains and IPs 4
  - Contacted Domains 4
  - World Map of Contacted IPs 4
- General Information 4
  - Errors 4
  - Warnings 5
- Joe Sandbox View / Context 5
  - IPs 5
  - Domains 5
  - ASNs 5
  - JA3 Fingerprints 5
  - Dropped Files 5
- Created / dropped Files 5
- Static File Info 5
  - General 5
- Static APK Info 5
  - General 6
  - Receivers 6
  - Permission Requested 6
  - Certificate 6
  - Resources 6
- Network Behavior 6
  - TCP Packets 6
- APK Behavior 6
- Disassembly 6
  - 0 Executed Methods 6
  - 0 Non-Executed Methods 6

# Android Analysis Report

## Locus Map 4 Outdoor Navigation_v4.12.0_apkpure.com.xapk

## Overview

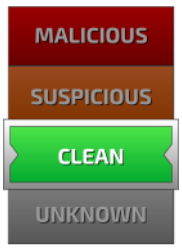
### General Information

| | |
|---|---|
| Sample Name: | Locus Map 4 Outdoor Navigation_v4.12.0_apkpure.com.xapk |
| Analysis ID: | 715054 |
| MD5: | 7d1e9e34c72e9a.. |
| SHA1: | 3c9658cd706ced.. |
| SHA256: | 36e896d31814d4.. |
| Infos: | |

**Errors**

Setup command "_JBInstrumentAPK" failed: Invalid APK

### Detection

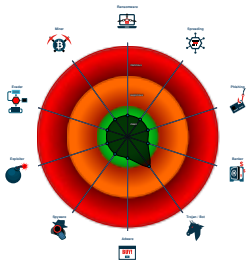



| | |
|---|---|
| Score: | 0 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 80% |

### Signatures

Tries to connect to HTTP servers, b…

### Classification



## Yara Signatures

No yara matches

## Snort Signatures

No Snort rule has matched

## Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Path Interception | Direct Volume Access | OS Credential Dumping | System Service Discovery | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | 1 Encrypted Channel | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Rootkit | LSASS Memory | Application Window Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | 1 Application Layer Protocol | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |

## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

No Antivirus matches

### Dropped Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

No Antivirus matches

## Domains and IPs

### Contacted Domains

No contacted domains info

### World Map of Contacted IPs

No contacted IP infos

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 36.0.0 Rainbow Opal |
| Analysis ID: | 715054 |
| Start date and time: | 2022-10-03 15:43:17 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 1m 26s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | Locus Map 4 Outdoor Navigation_v4.12.0_apkpure.com.xapk |
| Cookbook file name: | defaultandroidfilecookbook.jbs |
| Analysis system description: | Android 9 (Pie) |
| Run name: | No or little behavior, retry without instrumentation |
| Analysis Mode: | default |
| APK Instrumentation enabled: | true |
| Detection: | CLEAN |
| Classification: | clean0.andXAPK@0/0@0/0 |

### Errors

- Setup command "_JBInstrumentAPK" failed: Invalid APK

### Warnings

- No dynamic data available
- Static analyzation failed: null
- VT rate limit hit for: Locus Map 4 Outdoor Navigation_v4.12.0_apkpure.com.xapk

## Joe Sandbox View / Context

### IPs

No context

### Domains

No context

### ASNs

No context

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

No created / dropped files found

## Static File Info

### General

| | |
|---|---|
| File type: | Zip archive data, at least v2.0 to extract, compression method=store |
| Entropy (8bit): | 7.616420158694971 |
| TrID: | • Android Package (27504/1) 56.11%<br>• Java Archive (13504/1) 27.55%<br>• ZIP compressed archive (8000/1) 16.32%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01% |
| File name: | Locus Map 4 Outdoor Navigation_v4.12.0_apkpure.com.xapk |
| File size: | 42912763 |
| MD5: | 7d1e9e34c72e9a2dd619ce04f59b6f1a |
| SHA1: | 3c9658cd706ced7e53d89b408cfe1eac4e532780 |
| SHA256: | 36e896d31814d4a7a26144c0064d9ed072070b88b9a9f2a8ba42f04f27a5e572 |
| SHA512: | 6a931c2772fc39718557fa1031fed34db3f28be9fb6c695fc1d1782b0f4847a9a86257e3977ef51c7704c995679f866a45c3420077e47927a230d7a81432088c |
| SSDEEP: | 786432:epdKdgSbNonBCqB4ewVSjAoYIBXiUC9Jf48/Q7XcKLOa8am4h:EKdgOmCqeewVkAvR9hggaz |
| TLSH: | 6F97F207FE0C582AD5BB647D4BCA8221F0225E416E41CBD37065B21E76B7AE4CB663F1 |
| File Content Preview: | PK.....menion.android.locus.apkPK.....!.!..A)^.B...*.....AndroidManifest.xml....Ue.....2 .....#3.83,....s..8.....;".....?<br>3#.BC2333333323#3....\|....g.3..L.._...s...>.~....h.=-h.....>F.....B..!.8h"4.:....A..".. |

## Static APK Info

| General | |
|---|---|
| Label: | |
| Version Code: | |
| Version Name: | |
| Package Name: | |
| Is Activity: | |
| Is Receiver: | |
| Is Service: | |
| Requests System Level Permissions: | |
| Play Store Compatible: | |

| Receivers |
|---|
| **Permission Requested** |
| **Certificate** |

| | |
|---|---|
| Name: | |
| Issuer: | |
| Subject: | |

| Resources | | |
|---|---|---|
| **Name** | **Type** | **Size** |

# Network Behavior

## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Oct 3, 2022 15:43:36.543329954 CEST | 50458 | 443 | 192.168.2.30 | 216.58.212.170 |
| Oct 3, 2022 15:43:36.671384096 CEST | 39602 | 443 | 192.168.2.30 | 142.250.186.163 |

# APK Behavior

# Disassembly

### 0 Executed Methods

### 0 Non-Executed Methods