FORENSIPIE ANALYSIS REPORT

Timestamp: 2025-05-04 16:29:09
Tool Version: 1.0.0

DEVICE IS CLASSIFIED AS MALICIOUS

Reasons:

- Missing or Suspicious Certificates
- Suspicious API Calls Detected
- YARA Match Found: Hidden Payloads
- YARA Match Found: Obfuscation

APK OVERVIEW

- File Name: E:\ExtractedAPKs\PM KISAN NEW RAGISTRATION UPDATE 2024.apk
- File Path: E:\ExtractedAPKs\PM KISAN NEW RAGISTRATION UPDATE 2024.apk
- Package Name: com.example.smsreafna
- Minimum SDK: 24
- Target SDK: 34

APK UNPACK AND DECOMPILATION

- **Total Classes Decompiled:** 8031
- **Total Methods Decompiled:** 56559

MANIFEST ANALYSIS

- Minimum SDK: 24
- Target SDK: 34
- Permissions:
* com.example.smsreafna.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION
* android.permission.RECEIVE_SMS
* android.permission.ACCESS_NETWORK_STATE
* android.permission.SEND_SMS
* android.permission.INTERNET
- Broadcast Receivers:
* com.example.smsreafna.ReceiveSms
* androidx.profileinstaller.ProfileInstallReceiver
- Content Providers:
* androidx.startup.InitializationProvider
* com.google.firebase.provider.FirebaseInitProvider

- Activities:
* com.example.smsreafna.MainActivity
* com.google.android.gms.common.api.GoogleApiActivity
- Certificates:
* SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81

DATABASE ENCRYPTION STATE

- Status: Not Available

SUSPICIOUS API CALLS

- Method: getSearchManagerSuggestions
Description: Potential database query operation.
- Method: query
Description: Potential database query operation.
- Method: unwrapCryptoObject
Description: Potential cryptographic operation.
- Method: unwrapCryptoObject
Description: Potential cryptographic operation.
- Method: unwrapCryptoObject
Description: Potential cryptographic operation.
- Method: wrapCryptoObject
Description: Potential cryptographic operation.
- Method: wrapCryptoObject
Description: Potential cryptographic operation.
- Method: wrapCryptoObject
Description: Potential cryptographic operation.
- Method: query
Description: Potential database query operation.
- Method: exists
Description: Potential database query operation.
- Method: queryForLong
Description: Potential database query operation.
- Method: queryForString
Description: Potential database query operation.
- Method: listFiles
Description: Potential database query operation.
- Method: onCreate
Description: Potential SMS sending activity.
- Method: onReceive
Description: Potential SMS sending activity.
- Method: zzb
Description: Potential database query operation.

SIGNATURE BASED ANALYSIS

- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled__xif8r1p\classes.dex matched rule: hidden_payloads
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled__xif8r1p\resources.arsc matched rule: hidden_payloads
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled__xif8r1p\META-INF\ANDROID.SF matched rule: hidden_payloads
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled__xif8r1p\META-INF\MANIFEST.MF matched rule: hidden_payloads
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled__xif8r1p\res\-6.webp matched rule: hidden_payloads
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled__xif8r1p\res\iE.webp matched rule: hidden_payloads
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled__xif8r1p\classes.dex matched rule: obfuscation
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled__xif8r1p\classes2.dex matched rule: obfuscation
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled__xif8r1p\DebugProbesKt.bin matched rule: obfuscation
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled__xif8r1p\resources.arsc matched rule: obfuscation
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled__xif8r1p\kotlin\coroutines\coroutines.kotlin_builtins matched rule: obfuscation
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled__xif8r1p\META-INF\ANDROID.SF matched rule: obfuscation
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled__xif8r1p\META-INF\MANIFEST.MF matched rule: obfuscation