FORENSIPIE ANALYSIS REPORT

Timestamp: 2025-09-01 14:18:46
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\Axis_bank.apk
- File Path: E:\ExtractedAPKs\Axis_bank.apk
- Package Name: com.atrc.tr44
- Minimum SDK: 24
- Target SDK: 34

MANIFEST ANALYSIS

- Minimum SDK: 24
- Target SDK: 34
- Permissions:

* com.atrc.tr44.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION
* android.permission.INTERNET
* android.permission.FOREGROUND_SERVICE
* android.permission.READ_SMS
* android.permission.POST_NOTIFICATIONS
* android.permission.SEND_SMS
* android.permission.RECEIVE_SMS
* android.permission.FOREGROUND_SERVICE_DATA_SYNC

- Broadcast Receivers:

* androidx.profileinstaller.ProfileInstallReceiver

- Content Providers:

* androidx.startup.InitializationProvider

- Activities:

* com.example.card
* com.example.MainActivity
* com.example.customer

* com.example.splash
- Certificates:
* SHA1: e6b9d4c2f52365fe8b2f26554a54dbea2a370f1f

DATABASE ENCRYPTION STATE

- Status: Not Available

SUSPICIOUS API CALLS

- 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: exists
Description: Potential database query operation.
- Method: queryForLong
Description: Potential database query operation.
- Method: queryForString
Description: Potential database query operation.
- Method: run
Description: Potential database query operation.
- Method: listFiles
Description: Potential database query operation.
- Method: getSearchManagerSuggestions
Description: Potential database query operation.

SIGNATURE BASED ANALYSIS

- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled_7wnz4f16\classes.dex matched rule: hidden_payloads
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled_7wnz4f16\resources.arsc matched rule: hidden_payloads

```
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled_7wnz4f16\res\sm.jpg matched rule: hidden_payloads
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled_7wnz4f16\res\uY.jpg matched rule: hidden_payloads
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled_7wnz4f16\res\Z4.jpg matched rule: hidden_payloads
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled_7wnz4f16\classes.dex matched rule: obfuscation
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled_7wnz4f16\DebugProbesKt.bin matched rule: obfuscation
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled_7wnz4f16\resources.arsc matched rule: obfuscation
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled_7wnz4f16\kotlin\coroutines\coroutines.kotlin_builtins matched rule: obfuscation
- File: C:\Users\03ata\AppData\Local\Temp\apk_decompiled_7wnz4f16\res\pu.png matched rule: obfuscation
```