Summary of MVT Tool Output

Overview

The Mobile Verification Toolkit (MVT) analyzed an iTunes backup of an iPhone using various indicators from multiple sources, including Predator, Kingspawn, Helios, RCS, and Pegasus. The following is a summary of the key findings and outputs from the MVT analysis.

Device Information

Device Name: User's iPhone

Build Version: 21F90

Product Type: iPhone 15 Pro (iPhone16,1)

Product Version: 17.5.1

Serial Number: AB1CD2EF3GH

IMEI: 123456789012345

Phone Number: +12 3456 789012

Last Backup Date: 2024-07-25 20:29:02

Indicators and Detections

Total Unique Indicators Loaded: 9898

The MVT tool parsed several STIX2 indicators files from different sources including:

- Intellexa Predator
- Quadream Kingspawn
- Wintego Helios
- RCS Lab
- Stalkerware
- Wyrmspy Dragonegg
- Amnesty Tech's Pegasus

- Operation Triangulation
- Android Malware Campaign

Installed Applications

Communication and social apps: WhatsApp, Signal, Telegram, Messenger, Facebook, Instagram, LinkedIr

Finance and trading apps: Binance, KuCoin, Coinbase, MetaMask, TradingView.

Utilities and productivity apps: Google Drive, Microsoft Office, Adobe Reader, Notion, Zoom.

Miscellaneous apps: Uber, Deliveroo, Netflix, Spotify, Strava.

Configuration Profiles

One configuration profile was extracted with no detections:

- Vodafone UK profile installation and removal events were logged.

Backup Analysis

Manifest: Extracted 181,647 file metadata items with no detections.

Profile Events: Two profile events were logged with no detections.

Calls: 2,129 calls were extracted with no detections.

Contacts: 914 contacts were extracted with no detections.

Other Modules

Chrome and Firefox Favicon & History: No data to extract.

ID Status Cache: Extracted with no detections.

InteractionC: 3,281 events were extracted with no detections.

Conclusions

The MVT analysis did not produce any detections for malicious indicators within the analyzed backup. However, given the extensive list of loaded indicators and the comprehensive data extraction, it's advisable for the user to stay vigilant and ensure all applications and system software are up to date.

For any potential detections or suspicious activity found in the future, immediate steps should include securing the device, consulting cybersecurity experts, and taking preventive measures to avoid future compromises.