About Tails-MVT

Tails-MVT is a customised version of Tails that has the Mobile Verification Toolkit preinstalled and working out of the box. Tails-MVT is meant for non-advanced users. If you have a technical background, you may want to setup MVT yourself and follow the official MVT Documentation.

For more information on Tails-MVT, visit actionaiddk.github.io.

IMPORTANT Not finding any indications of compromise does **NOT** mean your device is not infected. It just means that the public indicators of compromise was not matched with data extracted from your phone. The indicators are derived from forensic work and they are publicly available. This means the the spyware authors have access to them as well, and can rule them out of future spyware and infections.

Table of Contents

1. Analysing Android devices

1.1 Preparing the Android device To analyse an Android device, the **developer options** and **USB debugging** need to be enabled. On the device, head to the **Settings** -> **About phone** and press the build number several times. Once the developer options are enabled, enable USB Debugging from within **Settings** -> **System** -> **Developer options** and toggle **USB debugging**.

1.2 Perform analysis To analyse your device, connect it to the laptop with a compatible cable. A cable of good quality is advised. Make the phone is turned on and unlocked Press the Windows or Super button on the keyboard and search for terminal or select it from the menu in the upper left corner: **Applications** -> **Utilities** -> **Terminal**. Once the terminal is open, type `mvt-android check-adb` and hit enter.

A prompt will appear on the Android device asking whether to trust this PC. Toggle **Always allow from this computer** and press **Allow**.

Next, a prompt will show asking whether to allow a full backup. Press **Back up my data**. The analysis will now run and analyse the data with the indicators of compromised provided by Mobile Verification Toolkit.

1.3 Error handling You may run into an error stating **Device is busy, maybe run `adb kill-server` and try again**. Type `killall adb` and try again. If the problem persists. Try unplugging the phone and redoing the steps again. You may also try the command `adb kill-server`, however we found that `killall adb` works in the majority of cases.

2. Analysing iOS devices

2.1 Preparing folders To analyse an iOS device, create a folder structure according to the one listed below. It can be done through the File Explorer found under **Applications** -> **Accessories** -> **Files** or by opening a terminal and typing `mkdir -p ios/backup ios/backup-decrypted ios/result`.

To open a terminal, press the Windows or Super button on the keyboard and search for terminal or select it from **Applications** -> **Utilities** -> **Terminal**

```
--ios/
   |--backup/
   |--backup-decrypted/
   |--result
```

2.2 Create backup Now connect your iOS device with a compatible cable and make sure it is unlocked. A prompt on the iOS device will show asking whether to trust this computer. Press **Trust**.

In the terminal type `idevicebackup2 -i encryption on`. You will be asked to enter a new backup password. Enter a password of your selection and make sure to remember it. If the password has previously been set, make sure you have the password ready. If the password is set but you don't know it, you may try to reset it by following the following steps described in the MVT documentation.

To create a backup, enter the following command in the terminal:

```
idevicebackup2 backup --full ios/backup
```

2.3 Decrypt backup To decrypt the backup, type the following command and replace with the decryption password for you device backup. The `<long string of numbers>` will vary. You may press **Tab** to autocomplete after typing the first characters of the string.

```
mvt-ios decrypt-backup -p <password> -d ios/backup-decrypted ios-analysis/backup/<long
string of numbers>
```

2.4 Perform analysis To check the backup, run the following command

```
mvt-ios check-backup --output ios/results ios/backup-decrypted
```

The analysis will now run and analyse the data with the indicators of compromised provided by Mobile Verification Toolkit.

2.5 Error handling You may run into where the backup of the iOS device takes up more space than available in the file system. To circumvent this issue, you must flash the Tails-MVT image to a larger media or plug in an external drive after booting, to store the backup. The external will mount itself under `/media/amnesia/<device name>`. Before running the commands in step 2.1, 2.2, 2.3 and 2.4, write the following command to change your working directory to the external drive.

```
cd /media/amnesia/<device name>
```

Make sure to delete the backup properly from the external drive after analysis (including the Trash folder).

3. Update indicators of compromise

To update the indicators of compromise, make sure the laptop is online through either WiFi or cabled connection. Once connected, a window with the title **Tor Connection** will appear. Toggle **Connect to Tor automatically** and press **Connect to Tor**. Once the connection is established, open a terminal and type `torify mvt-android download-iocs`and `torify mvt-ios download-iocs`.

Note that the indicators of compromise are reset for every reboot and will need updating again. We try to release a new image when new indicators are published to support offline complete offline analysis.