OVERVIEW OF FORENSIC METODOLOGHY FOR APPROACHING FORENSICS

tes
texto.texto@proton.me

July 2024

AGENDA | 3 SESSIONS

Pre-assessment:

1. Core key questions
2. Contextual assessment, Vetting & Consent collection
3. Documentation
4. Preparation (lab, tools)

Assessment:

1. Data Acquisition
2. Forensics Analysis

Post-assessment:

1. Follow-up
2. Outcome
3. Lessons learned

+ REFERENCES

Built on top of other organizations/individuals efforts:

Trainings:

- Digital Forensics Fellowship from Amnesty International (this session is based on this material)
- Digital Defenders workshop on Forensics (Jacobo Najera & Marla)

Online resources:

- Guide to forensics Security Without borders | Garnieri & Etienne (https://github.com/securitywithoutborders)

Tools development:

- MVT project (https://github.com/mvt-project)

& personal perspective of field work

SESSION 2

Data acquisition

- The process of extracting data from a device for analysis
- Focus on Logical extraction, extract data from OS filesystem

Sources of data

a. Android:

- Bugreport
- Via an adb connection
- Backup
- Via androidQF

b. iOS:

- Backup
- Sysdiagnose

ANALYSIS

The main objective is to **detect any irregularity, suspicious behavior, or known malicious indicator**. We have some hypothesis and we need to see if evidence supports or refuses it.

Guided by:

- **Context** & **Core questions**
- **Timeline** of events

Allows scoping and prioritizing time & efforts.

How to detect a potential compromise?

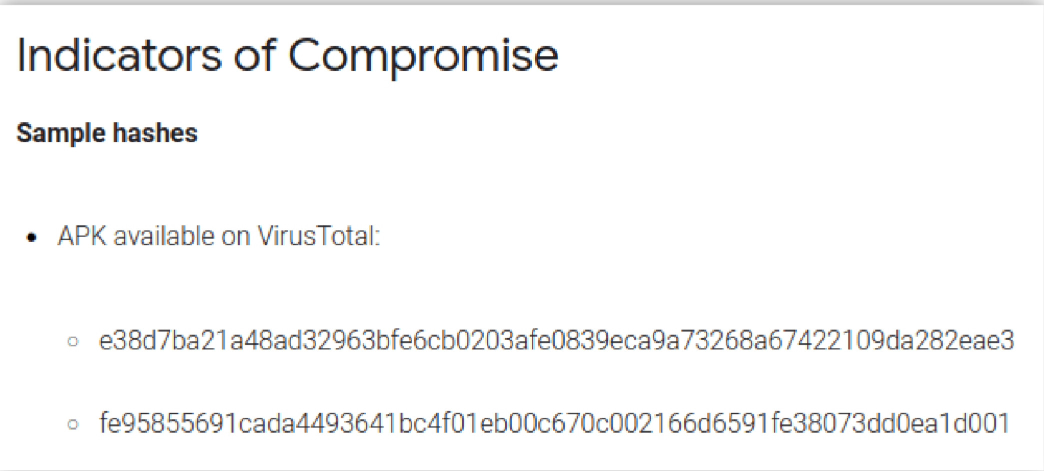
- **Indicator of Compromise** based detection

ANALYSIS

INDICATORS OF COMPROMISE

IoCs are specific artifacts or pieces of information known to be malicious.

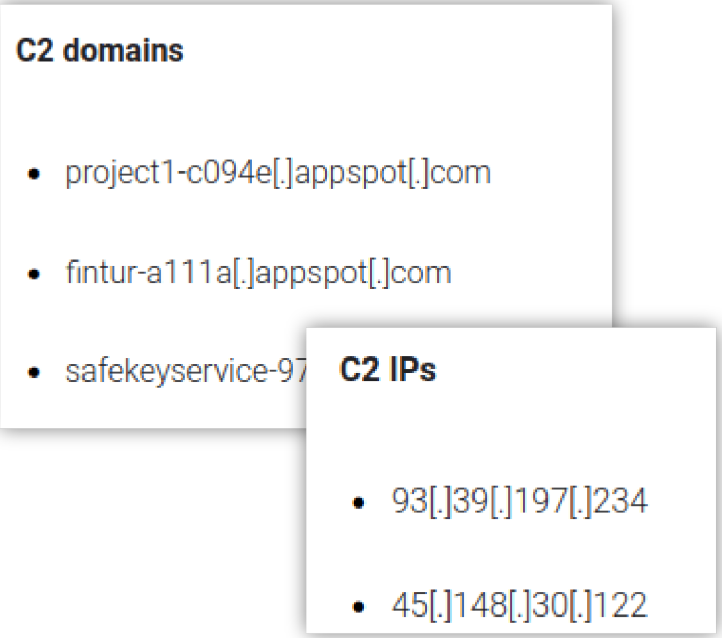
For example: file hashes, IP addresses, domain names, and email addresses associated with malicious activities.



Indicators of Compromise

Sample hashes

- APK available on VirusTotal:
  - e38d7ba21a48ad32963bfe6cb0203afe0839eca9a73268a67422109da282eae3
  - fe95855691cada4493641bc4f01eb00c670c002166d6591fe38073dd0ea1d001



C2 domains

- project1-c094e[.]appspot[.]com
- fintur-a111a[.]appspot[.]com
- safekeyservice-97

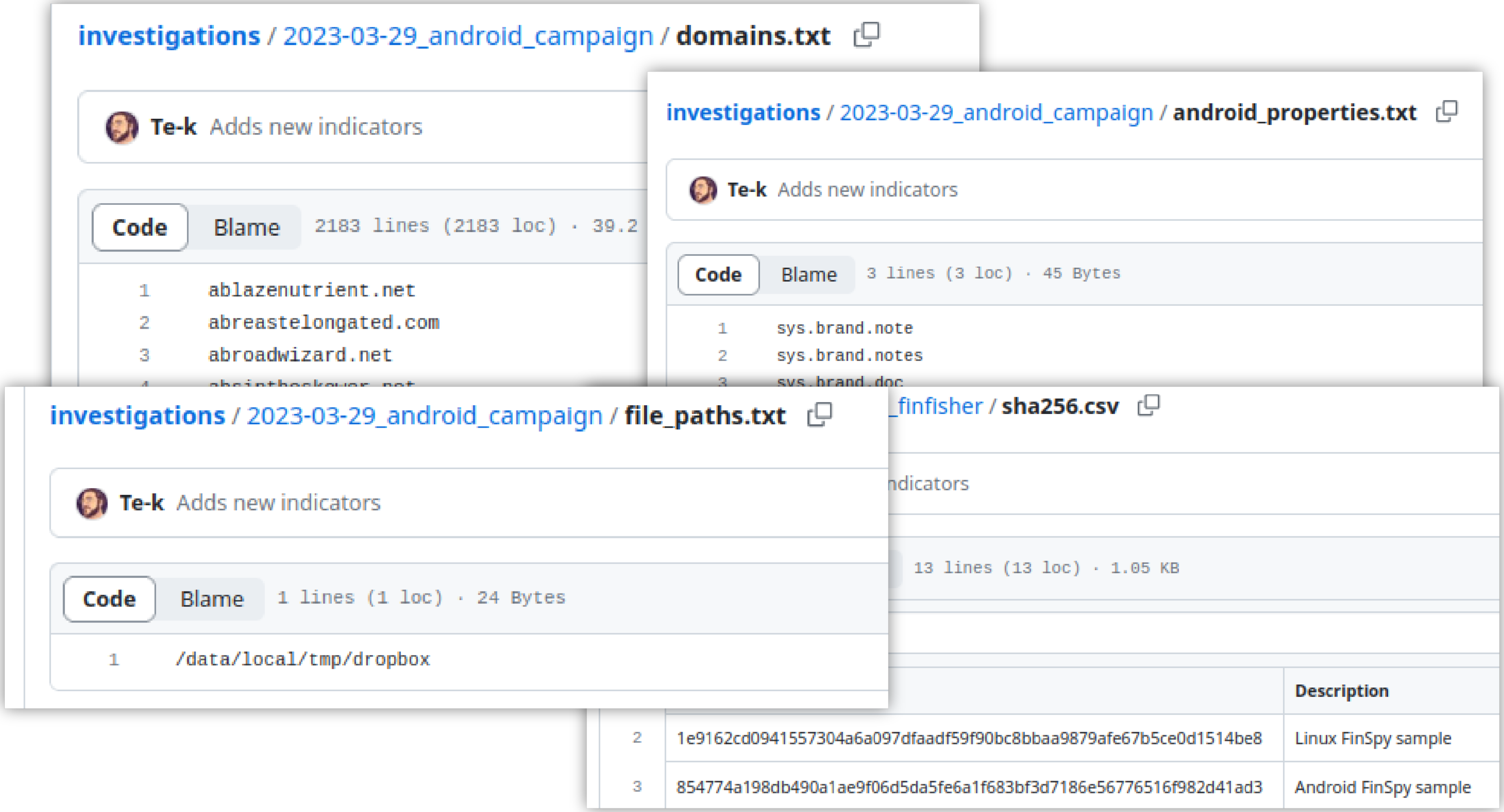
C2 IPs

- 93[.]39[.]197[.]234
- 45[.]148[.]30[.]122

https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/

ANALYSIS

INDICATORS OF COMPROMISE



investigations / 2023-03-29_android_campaign / domains.txt

Te-k Adds new indicators

Code Blame 2183 lines (2183 loc) · 39.2

```
ablazenutrient.net
abreastelongated.com
abroadwizard.net
```

investigations / 2023-03-29_android_campaign / android_properties.txt

Te-k Adds new indicators

Code Blame 3 lines (3 loc) · 45 Bytes

```
sys.brand.note
sys.brand.notes
sys.brand.doc
```

investigations / 2023-03-29_android_campaign / file_paths.txt

Te-k Adds new indicators

Code Blame 1 lines (1 loc) · 24 Bytes

```
/data/local/tmp/dropbox
```

_finfisher / sha256.csv

ndicators

13 lines (13 loc) · 1.05 KB

	Description
1e9162cd0941557304a6a097dfaadf59f90bc8bbaa9879afe67b5ce0d1514be8	Linux FinSpy sample
854774a198db490a1ae9f06d5da5fe6a1f683bf3d7186e56776516f982d41ad3	Android FinSpy sample

https://github.com/AmnestyTech/investigations/tree/master/2023-03-29_android_campaign

+ ANALYSIS

Caveats:

1. Using known indicators vs detecting unknown malicious traces
2. Matching known IOCs (similar to signature matching in AV world) vs heuristic approach
3. IOCs available from threat intelligence feeds, previous incidents, or security research & public community repositories. Sharing challenges.
4. Conducting an automated analysis vs manual analysis
5. The technology impose limits. Information needed may not be present in our acquisition sample.

ANALYSIS

2 approaches:

a. Automated analysis

b. Manual analysis

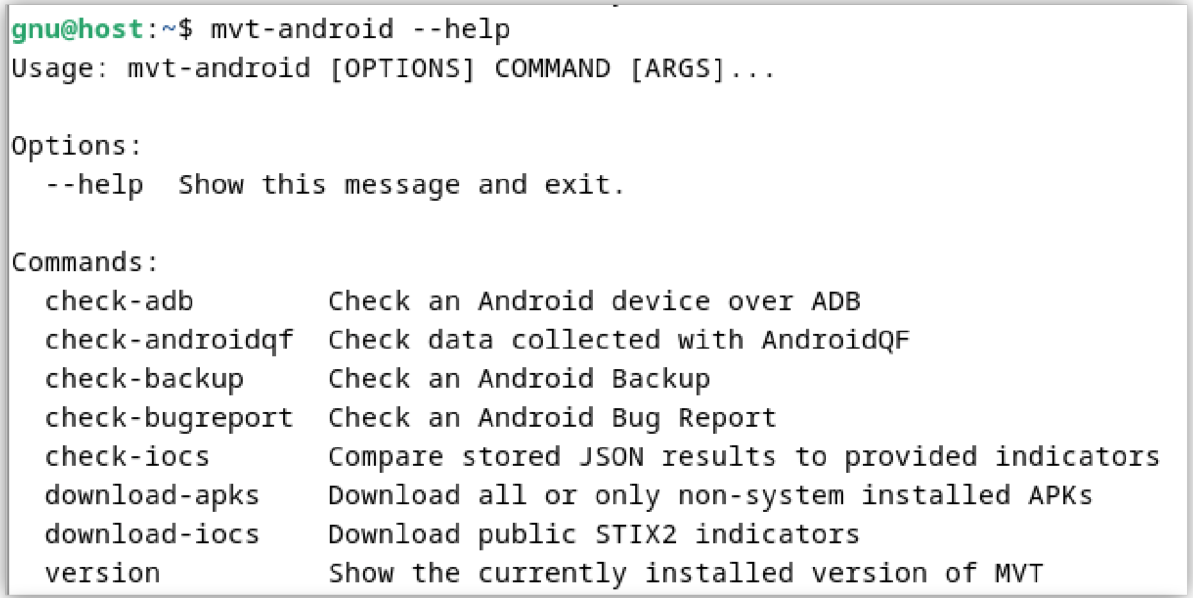
ANALYSIS

AUTOMATED ANALYSIS

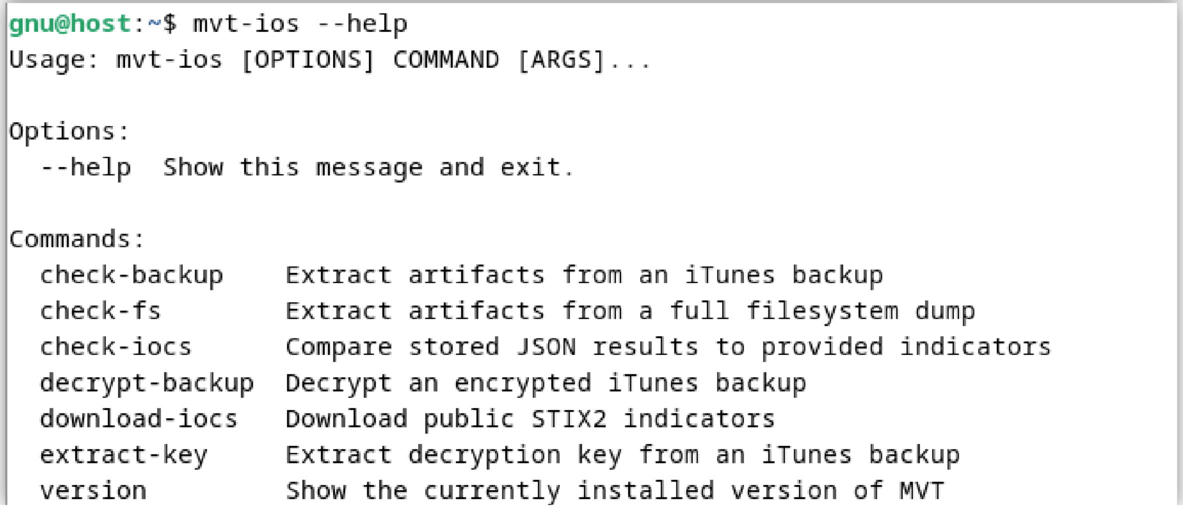
MVT (Mobile Verification Toolkit)

https://github.com/mvt-project/mvt

A collection of utilities to simplify and automate the process of **gathering** forensic traces helpful to **identify a potential compromise** of Android and iOS devices.



```
gnu@host:~$ mvt-android --help
Usage: mvt-android [OPTIONS] COMMAND [ARGS]...

Options:
  --help  Show this message and exit.

Commands:
  check-adb         Check an Android device over ADB
  check-androidqf   Check data collected with AndroidQF
  check-backup      Check an Android Backup
  check-bugreport   Check an Android Bug Report
  check-iocs        Compare stored JSON results to provided indicators
  download-apks     Download all or only non-system installed APKs
  download-iocs     Download public STIX2 indicators
  version           Show the currently installed version of MVT
```

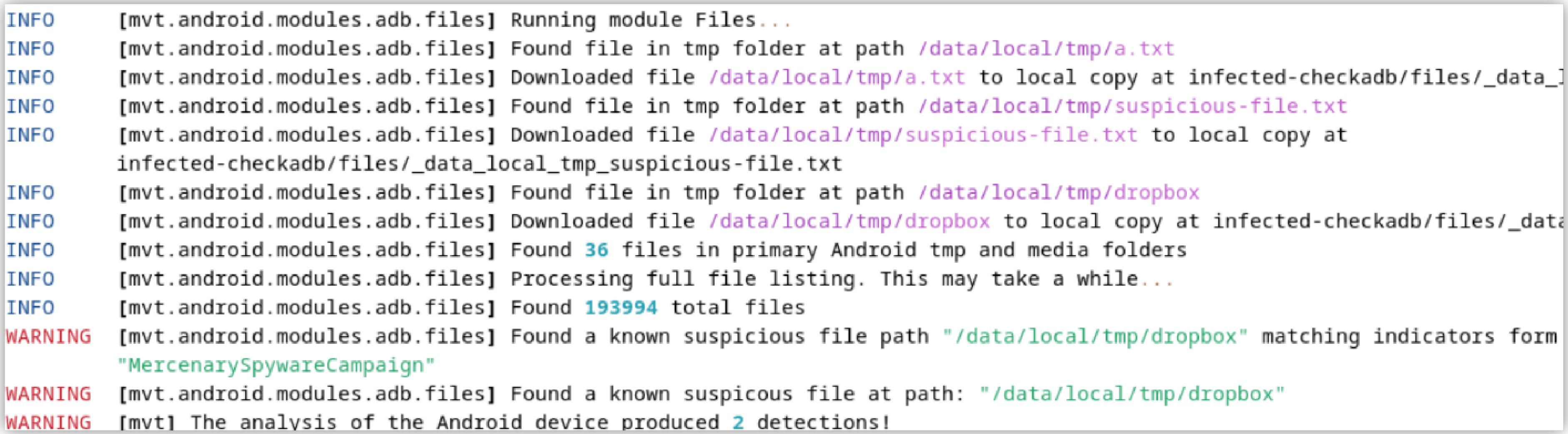


```
gnu@host:~$ mvt-ios --help
Usage: mvt-ios [OPTIONS] COMMAND [ARGS]...

Options:
  --help  Show this message and exit.

Commands:
  check-backup    Extract artifacts from an iTunes backup
  check-fs        Extract artifacts from a full filesystem dump
  check-iocs      Compare stored JSON results to provided indicators
  decrypt-backup  Decrypt an encrypted iTunes backup
  download-iocs   Download public STIX2 indicators
  extract-key     Extract decryption key from an iTunes backup
  version         Show the currently installed version of MVT
```

ANALYSIS

AUTOMATED ANALYSIS

MVT CHECK-ADB: Check an Android device over ADB.
$ mvt-android check-adb



```
INFO      [mvt.android.modules.adb.files] Running module Files...
INFO      [mvt.android.modules.adb.files] Found file in tmp folder at path /data/local/tmp/a.txt
INFO      [mvt.android.modules.adb.files] Downloaded file /data/local/tmp/a.txt to local copy at infected-checkadb/files/_data_
INFO      [mvt.android.modules.adb.files] Found file in tmp folder at path /data/local/tmp/suspicious-file.txt
INFO      [mvt.android.modules.adb.files] Downloaded file /data/local/tmp/suspicious-file.txt to local copy at
          infected-checkadb/files/_data_local_tmp_suspicious-file.txt
INFO      [mvt.android.modules.adb.files] Found file in tmp folder at path /data/local/tmp/dropbox
INFO      [mvt.android.modules.adb.files] Downloaded file /data/local/tmp/dropbox to local copy at infected-checkadb/files/_data
INFO      [mvt.android.modules.adb.files] Found 36 files in primary Android tmp and media folders
INFO      [mvt.android.modules.adb.files] Processing full file listing. This may take a while...
INFO      [mvt.android.modules.adb.files] Found 193994 total files
WARNING   [mvt.android.modules.adb.files] Found a known suspicious file path "/data/local/tmp/dropbox" matching indicators form
          "MercenarySpywareCampaign"
WARNING   [mvt.android.modules.adb.files] Found a known suspicous file at path: "/data/local/tmp/dropbox"
WARNING   [mvt] The analysis of the Android device produced 2 detections!
```

It is the most complete check.

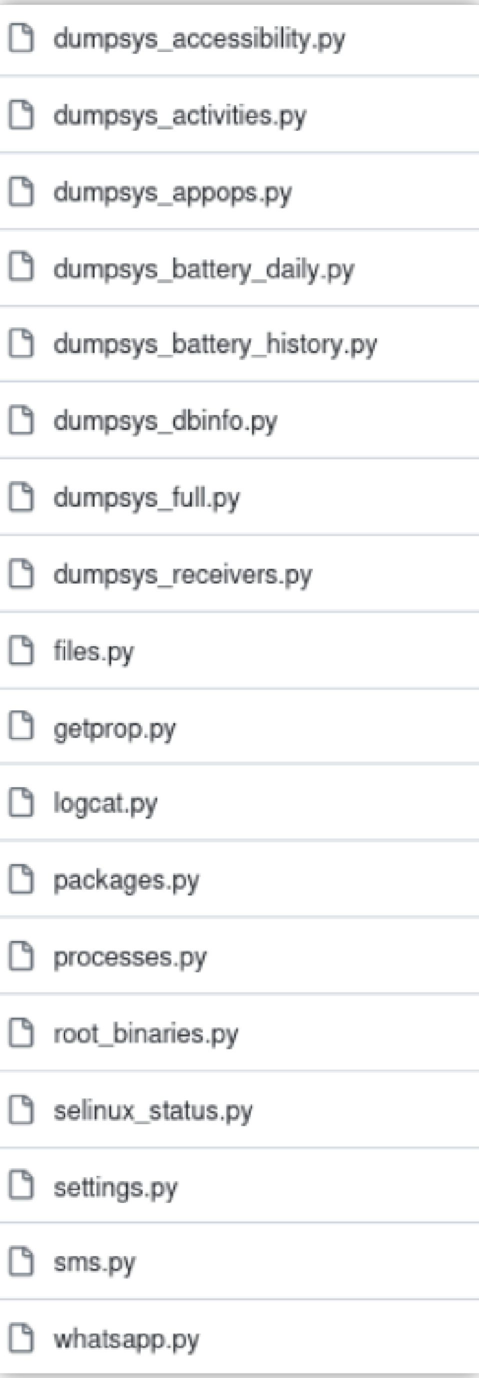
ANALYSIS

AUTOMATED ANALYSIS

MVT CHECK-ADB:

Modules being checked for rooted and non-rooted devices

https://github.com/mvt-project/mvt/tree/main/mvt/android/modules/adb



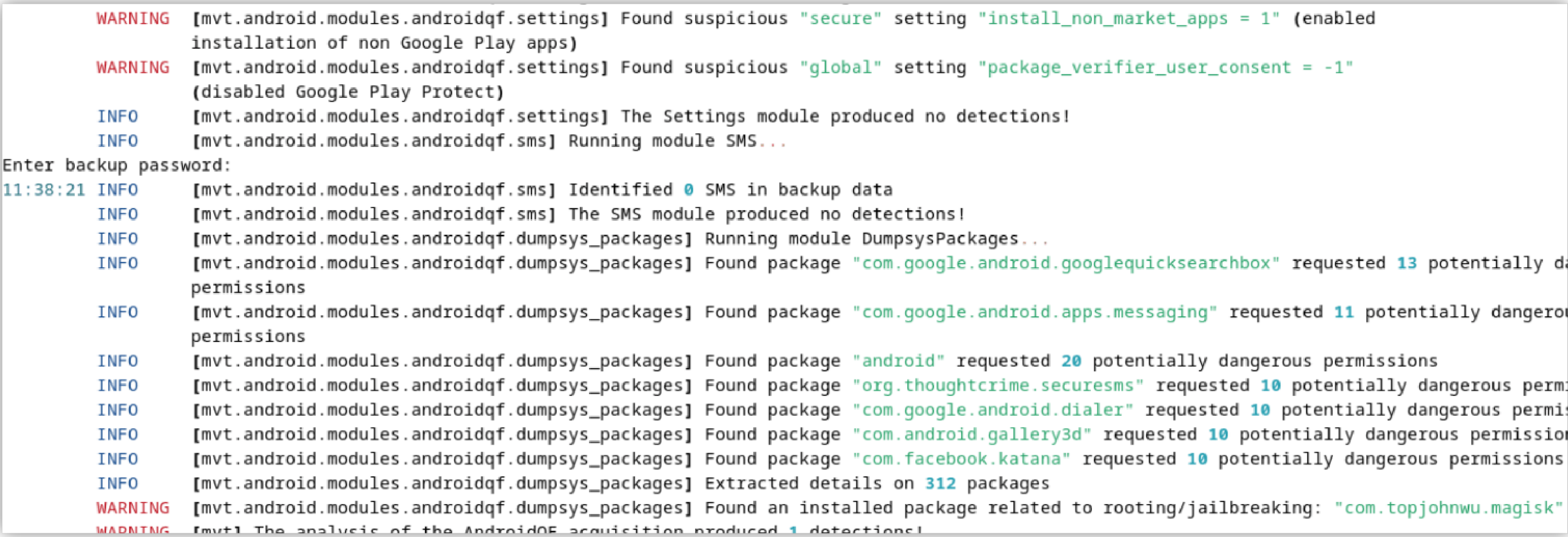
- dumpsys_accessibility.py
- dumpsys_activities.py
- dumpsys_appops.py
- dumpsys_battery_daily.py
- dumpsys_battery_history.py
- dumpsys_dbinfo.py
- dumpsys_full.py
- dumpsys_receivers.py
- files.py
- getprop.py
- logcat.py
- packages.py
- processes.py
- root_binaries.py
- selinux_status.py
- settings.py
- sms.py
- whatsapp.py

ANALYSIS

AUTOMATED ANALYSIS

MVT CHECK-ANDROIDQF: Check data collected with AndroidQF

```
$ mvt-android check-androidqf ./androidqf-output -o out
```



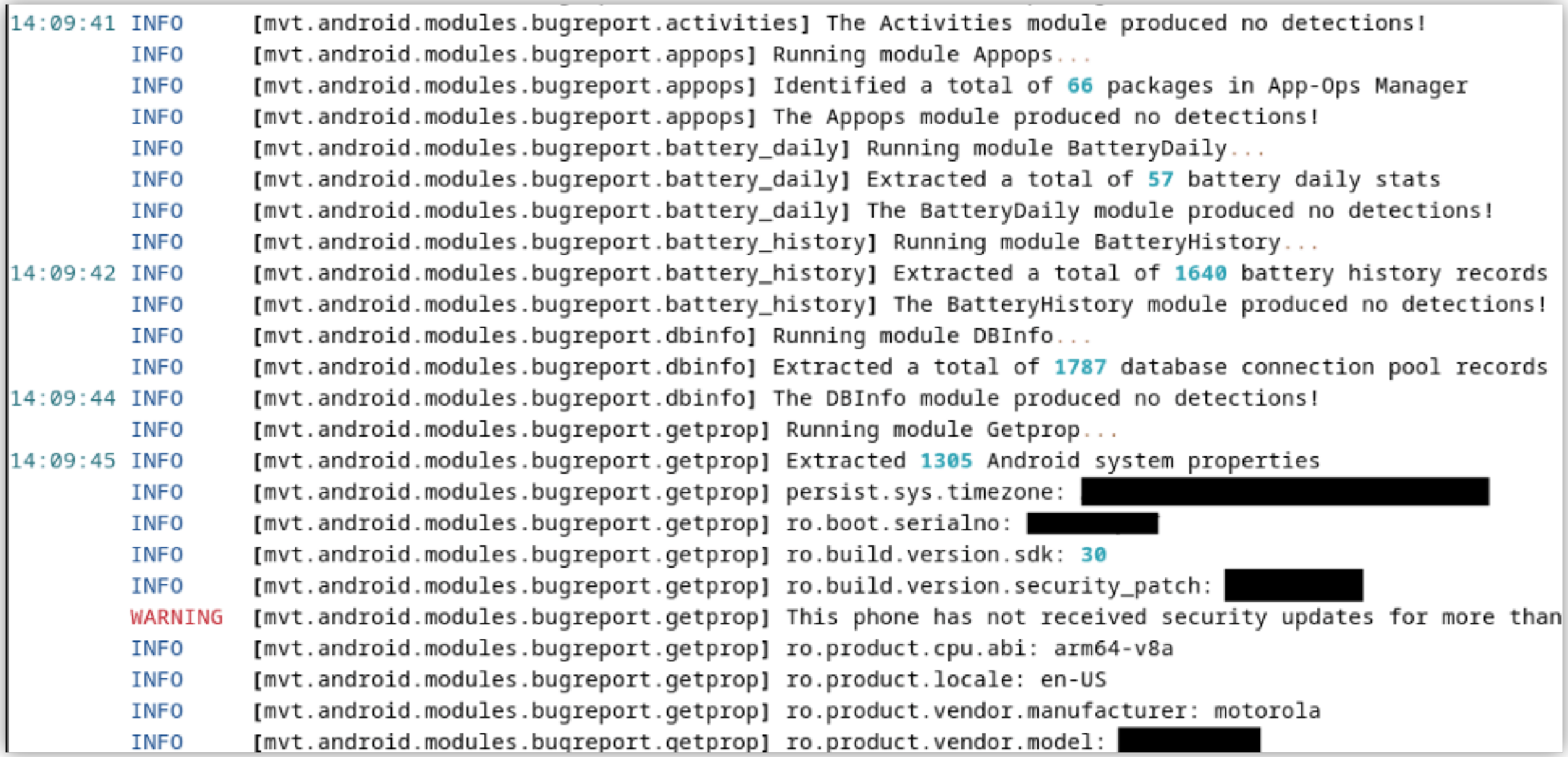
```
         WARNING  [mvt.android.modules.androidqf.settings] Found suspicious "secure" setting "install_non_market_apps = 1" (enabled
                  installation of non Google Play apps)
         WARNING  [mvt.android.modules.androidqf.settings] Found suspicious "global" setting "package_verifier_user_consent = -1"
                  (disabled Google Play Protect)
         INFO     [mvt.android.modules.androidqf.settings] The Settings module produced no detections!
         INFO     [mvt.android.modules.androidqf.sms] Running module SMS...
Enter backup password:
11:38:21 INFO     [mvt.android.modules.androidqf.sms] Identified 0 SMS in backup data
         INFO     [mvt.android.modules.androidqf.sms] The SMS module produced no detections!
         INFO     [mvt.android.modules.androidqf.dumpsys_packages] Running module DumpsysPackages...
         INFO     [mvt.android.modules.androidqf.dumpsys_packages] Found package "com.google.android.googlequicksearchbox" requested 13 potentially da
                  permissions
         INFO     [mvt.android.modules.androidqf.dumpsys_packages] Found package "com.google.android.apps.messaging" requested 11 potentially dangerou
                  permissions
         INFO     [mvt.android.modules.androidqf.dumpsys_packages] Found package "android" requested 20 potentially dangerous permissions
         INFO     [mvt.android.modules.androidqf.dumpsys_packages] Found package "org.thoughtcrime.securesms" requested 10 potentially dangerous permi
         INFO     [mvt.android.modules.androidqf.dumpsys_packages] Found package "com.google.android.dialer" requested 10 potentially dangerous permis
         INFO     [mvt.android.modules.androidqf.dumpsys_packages] Found package "com.android.gallery3d" requested 10 potentially dangerous permissio
         INFO     [mvt.android.modules.androidqf.dumpsys_packages] Found package "com.facebook.katana" requested 10 potentially dangerous permissions
         INFO     [mvt.android.modules.androidqf.dumpsys_packages] Extracted details on 312 packages
         WARNING  [mvt.android.modules.androidqf.dumpsys_packages] Found an installed package related to rooting/jailbreaking: "com.topjohnwu.magisk"
         WARNING  [mvt] The analysis of the AndroidQF acquisition produced 1 detections!
```

ANALYSIS

AUTOMATED ANALYSIS

MVT CHECK-BUGREPORT: Check an Android Bug Report

$ mvt-android check-bugreport ./bugreport-<BUILD-ID> -o out



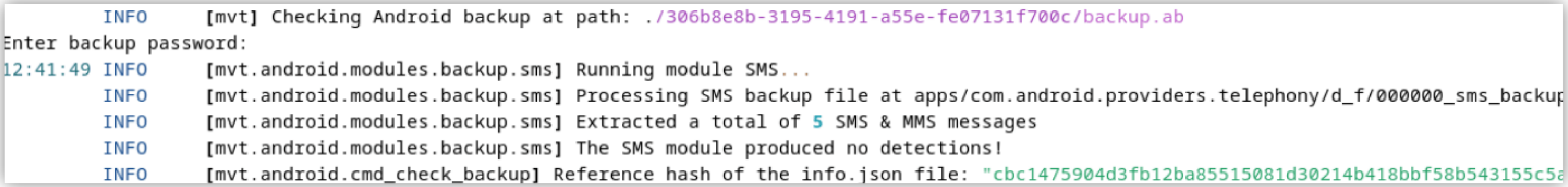
```
14:09:41 INFO     [mvt.android.modules.bugreport.activities] The Activities module produced no detections!
         INFO     [mvt.android.modules.bugreport.appops] Running module Appops...
         INFO     [mvt.android.modules.bugreport.appops] Identified a total of 66 packages in App-Ops Manager
         INFO     [mvt.android.modules.bugreport.appops] The Appops module produced no detections!
         INFO     [mvt.android.modules.bugreport.battery_daily] Running module BatteryDaily...
         INFO     [mvt.android.modules.bugreport.battery_daily] Extracted a total of 57 battery daily stats
         INFO     [mvt.android.modules.bugreport.battery_daily] The BatteryDaily module produced no detections!
         INFO     [mvt.android.modules.bugreport.battery_history] Running module BatteryHistory...
14:09:42 INFO     [mvt.android.modules.bugreport.battery_history] Extracted a total of 1640 battery history records
         INFO     [mvt.android.modules.bugreport.battery_history] The BatteryHistory module produced no detections!
         INFO     [mvt.android.modules.bugreport.dbinfo] Running module DBInfo...
         INFO     [mvt.android.modules.bugreport.dbinfo] Extracted a total of 1787 database connection pool records
14:09:44 INFO     [mvt.android.modules.bugreport.dbinfo] The DBInfo module produced no detections!
         INFO     [mvt.android.modules.bugreport.getprop] Running module Getprop...
14:09:45 INFO     [mvt.android.modules.bugreport.getprop] Extracted 1305 Android system properties
         INFO     [mvt.android.modules.bugreport.getprop] persist.sys.timezone: [redacted]
         INFO     [mvt.android.modules.bugreport.getprop] ro.boot.serialno: [redacted]
         INFO     [mvt.android.modules.bugreport.getprop] ro.build.version.sdk: 30
         INFO     [mvt.android.modules.bugreport.getprop] ro.build.version.security_patch: [redacted]
         WARNING  [mvt.android.modules.bugreport.getprop] This phone has not received security updates for more than
         INFO     [mvt.android.modules.bugreport.getprop] ro.product.cpu.abi: arm64-v8a
         INFO     [mvt.android.modules.bugreport.getprop] ro.product.locale: en-US
         INFO     [mvt.android.modules.bugreport.getprop] ro.product.vendor.manufacturer: motorola
         INFO     [mvt.android.modules.bugreport.getprop] ro.product.vendor.model: [redacted]
```

ANALYSIS

AUTOMATED ANALYSIS

MVT CHECK-BACKUP: Check a Android Backup

```
$ mvt-android check-backup ./backup.ab -o out
```



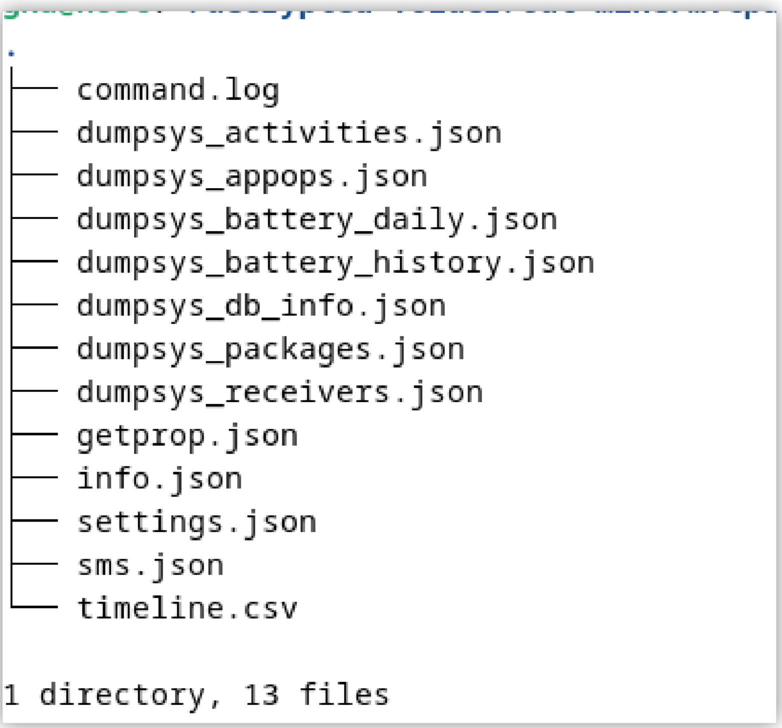
```
         INFO      [mvt] Checking Android backup at path: ./306b8e8b-3195-4191-a55e-fe07131f700c/backup.ab
Enter backup password:
12:41:49 INFO      [mvt.android.modules.backup.sms] Running module SMS...
         INFO      [mvt.android.modules.backup.sms] Processing SMS backup file at apps/com.android.providers.telephony/d_f/000000_sms_backup
         INFO      [mvt.android.modules.backup.sms] Extracted a total of 5 SMS & MMS messages
         INFO      [mvt.android.modules.backup.sms] The SMS module produced no detections!
         INFO      [mvt.android.cmd_check_backup] Reference hash of the info.json file: "cbc1475904d3fb12ba85515081d30214b418bbf58b543155c5a
```

ANALYSIS

AUTOMATED ANALYSIS

MVT output are a series of json and csv files, and when a detection is identified a "_detected" will be appended on those files.

Ej. timeline.csv & timeline_detected.csv



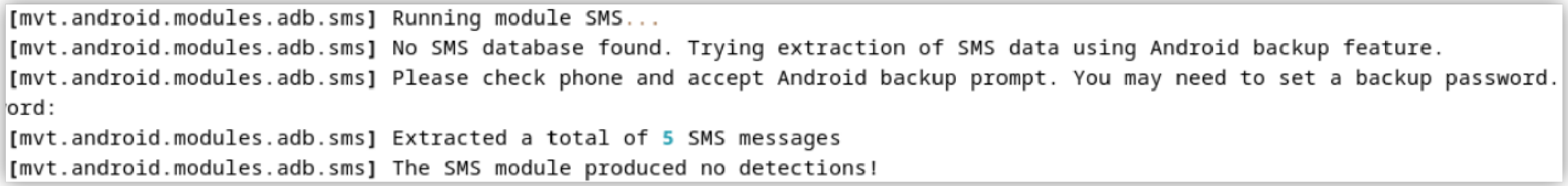
```
.
├── command.log
├── dumpsys_activities.json
├── dumpsys_appops.json
├── dumpsys_battery_daily.json
├── dumpsys_battery_history.json
├── dumpsys_db_info.json
├── dumpsys_packages.json
├── dumpsys_receivers.json
├── getprop.json
├── info.json
├── settings.json
├── sms.json
└── timeline.csv

1 directory, 13 files
```

ANALYSIS

SMS

Acquired via backup.ab & in androidqf output also.

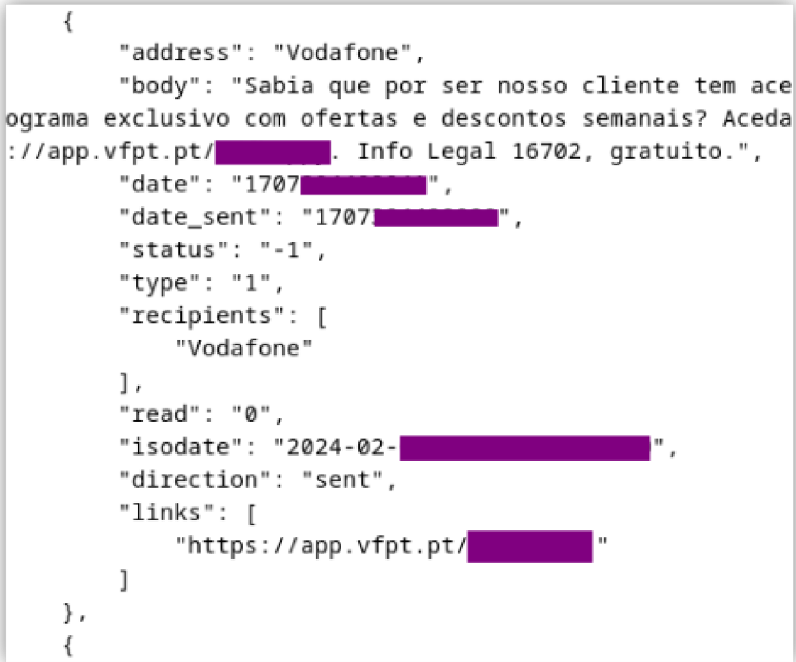
MVT will check links in SMS against known IOCs.



```
[mvt.android.modules.adb.sms] Running module SMS...
[mvt.android.modules.adb.sms] No SMS database found. Trying extraction of SMS data using Android backup feature.
[mvt.android.modules.adb.sms] Please check phone and accept Android backup prompt. You may need to set a backup password.
ord:
[mvt.android.modules.adb.sms] Extracted a total of 5 SMS messages
[mvt.android.modules.adb.sms] The SMS module produced no detections!
```

Manual analysis.

Parsed info of SMS can be found in sms.js files from the output of check-androidqf and check-adb



```
    {
        "address": "Vodafone",
        "body": "Sabia que por ser nosso cliente tem ace
ograma exclusivo com ofertas e descontos semanais? Aceda
://app.vfpt.pt/[redacted]. Info Legal 16702, gratuito.",
        "date": "1707[redacted]",
        "date_sent": "1707[redacted]",
        "status": "-1",
        "type": "1",
        "recipients": [
            "Vodafone"
        ],
        "read": "0",
        "isodate": "2024-02-[redacted]",
        "direction": "sent",
        "links": [
            "https://app.vfpt.pt/[redacted]"
        ]
    },
    {
```

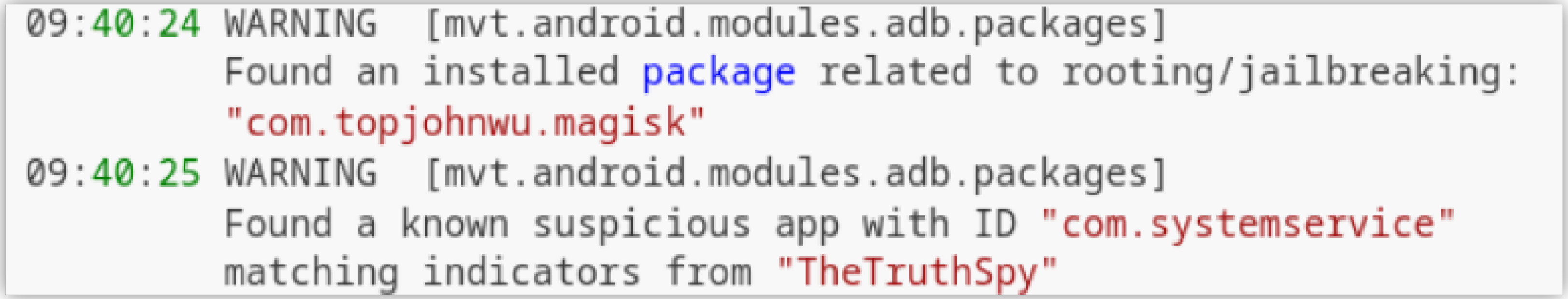
ANALYSIS

APPS

Aim check if apps are legitimate, have abusive capabilities.

We acquire both information about apps & the apps themselves (apk files), available in the output of androidqf, via adb, MVT directly.

MVT will check their names against known IOCs from malicious apps & rooting capable apps.

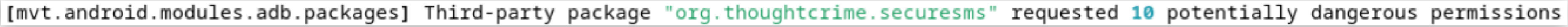


```
09:40:24 WARNING  [mvt.android.modules.adb.packages]
         Found an installed package related to rooting/jailbreaking:
         "com.topjohnwu.magisk"
09:40:25 WARNING  [mvt.android.modules.adb.packages]
         Found a known suspicious app with ID "com.systemservice"
         matching indicators from "TheTruthSpy"
```

ANALYSIS

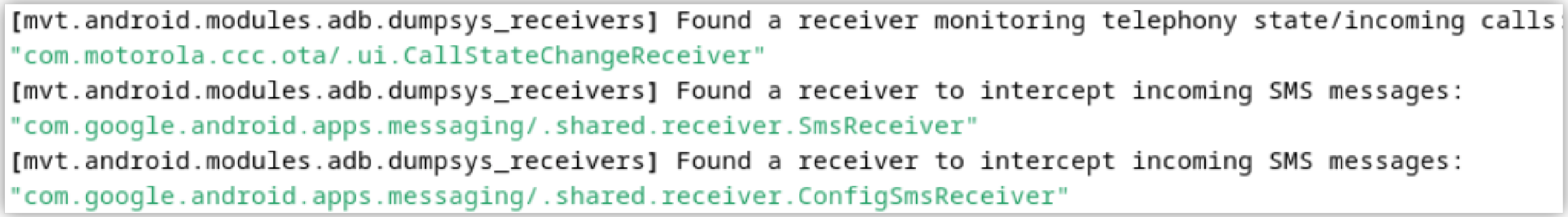
APPS

MVT will also flag apps with abusive permissions.



```
[mvt.android.modules.adb.packages] Third-party package "org.thoughtcrime.securesms" requested 10 potentially dangerous permissions
```

And it will flag specific components able to access sensitive functionalities from the device. In the example what apps are registered for listening to incoming SMS / CALLS.



```
[mvt.android.modules.adb.dumpsys_receivers] Found a receiver monitoring telephony state/incoming calls
"com.motorola.ccc.ota/.ui.CallStateChangeReceiver"
[mvt.android.modules.adb.dumpsys_receivers] Found a receiver to intercept incoming SMS messages:
"com.google.android.apps.messaging/.shared.receiver.SmsReceiver"
[mvt.android.modules.adb.dumpsys_receivers] Found a receiver to intercept incoming SMS messages:
"com.google.android.apps.messaging/.shared.receiver.ConfigSmsReceiver"
```

ANALYSIS

APPs

MVT also provides a summary of information of applications installed in dumpsys_packages.json (check-androidqf) and packages.json (check-adb)

-package_name. -file_name

-installer:

a. Google Play install:

com.android.vending

b. Chrome installation:

com.google...packageinstaller

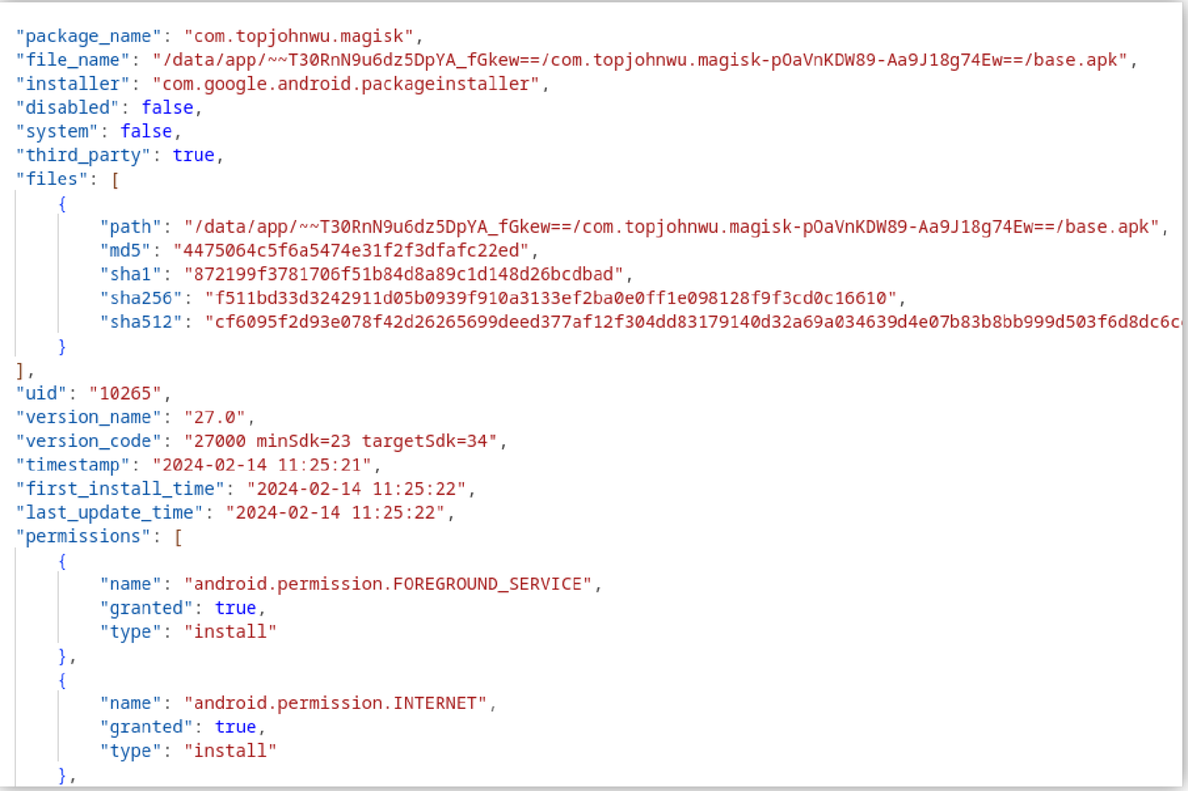
c. adb installation:

null/None

-system | third_party

-path | local_path

-permissions



```
"package_name": "com.topjohnwu.magisk",
"file_name": "/data/app/~~T30RnN9u6dz5DpYA_fGkew==/com.topjohnwu.magisk-pOaVnKDW89-Aa9J18g74Ew==/base.apk",
"installer": "com.google.android.packageinstaller",
"disabled": false,
"system": false,
"third_party": true,
"files": [
    {
        "path": "/data/app/~~T30RnN9u6dz5DpYA_fGkew==/com.topjohnwu.magisk-pOaVnKDW89-Aa9J18g74Ew==/base.apk",
        "md5": "4475064c5f6a5474e31f2f3dfafc22ed",
        "sha1": "872199f3781706f51b84d8a89c1d148d26bcdbad",
        "sha256": "f511bd33d3242911d05b0939f910a3133ef2ba0e0ff1e098128f9f3cd0c16610",
        "sha512": "cf6095f2d93e078f42d26265699deed377af12f304dd83179140d32a69a034639d4e07b83b8bb999d503f6d8dc6c
    }
],
"uid": "10265",
"version_name": "27.0",
"version_code": "27000 minSdk=23 targetSdk=34",
"timestamp": "2024-02-14 11:25:21",
"first_install_time": "2024-02-14 11:25:22",
"last_update_time": "2024-02-14 11:25:22",
"permissions": [
    {
        "name": "android.permission.FOREGROUND_SERVICE",
        "granted": true,
        "type": "install"
    },
    {
        "name": "android.permission.INTERNET",
        "granted": true,
        "type": "install"
    },
```

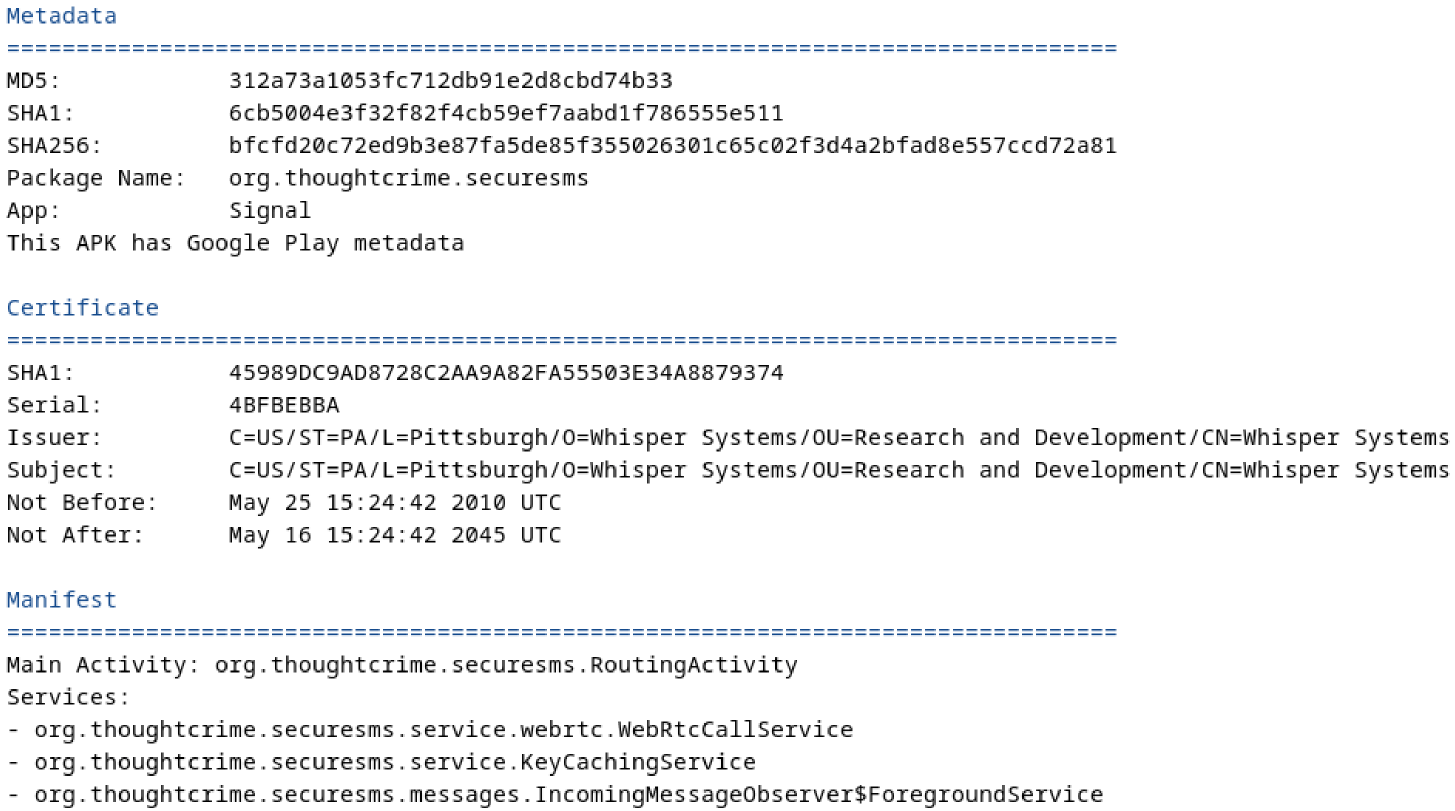
ANALYSIS

APPs

Look at permissions, components & certificate.

APKcli: https://github.com/Te-k/apkcli

$ apkcli info com.app-file.apk



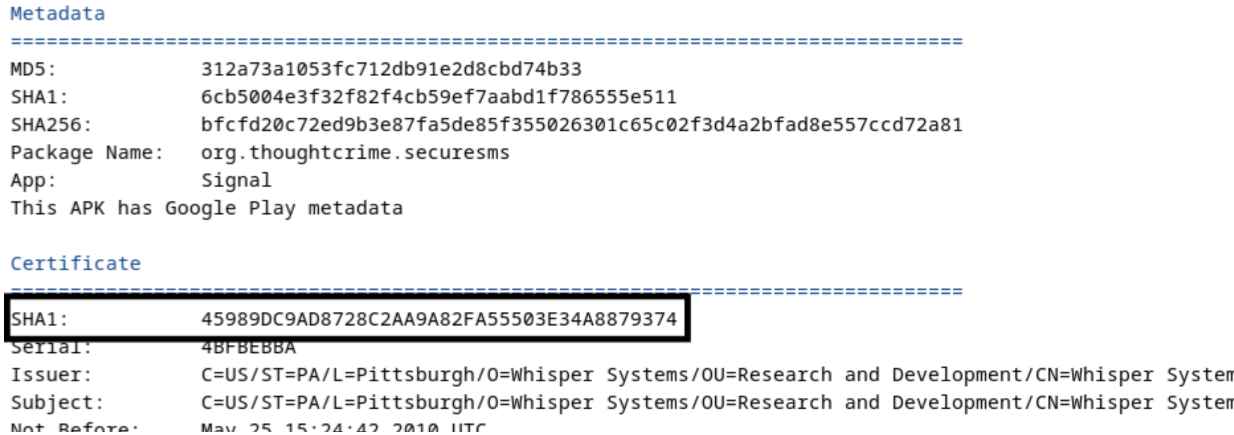
```
Metadata
================================================================================
MD5:            312a73a1053fc712db91e2d8cbd74b33
SHA1:           6cb5004e3f32f82f4cb59ef7aabd1f786555e511
SHA256:         bfcfd20c72ed9b3e87fa5de85f355026301c65c02f3d4a2bfad8e557ccd72a81
Package Name:   org.thoughtcrime.securesms
App:            Signal
This APK has Google Play metadata

Certificate
================================================================================
SHA1:           45989DC9AD8728C2AA9A82FA55503E34A8879374
Serial:         4BFBEBBA
Issuer:         C=US/ST=PA/L=Pittsburgh/O=Whisper Systems/OU=Research and Development/CN=Whisper Systems
Subject:        C=US/ST=PA/L=Pittsburgh/O=Whisper Systems/OU=Research and Development/CN=Whisper Systems
Not Before:     May 25 15:24:42 2010 UTC
Not After:      May 16 15:24:42 2045 UTC

Manifest
================================================================================
Main Activity: org.thoughtcrime.securesms.RoutingActivity
Services:
- org.thoughtcrime.securesms.service.webrtc.WebRtcCallService
- org.thoughtcrime.securesms.service.KeyCachingService
- org.thoughtcrime.securesms.messages.IncomingMessageObserver$ForegroundService
```

ANALYSIS

APPs

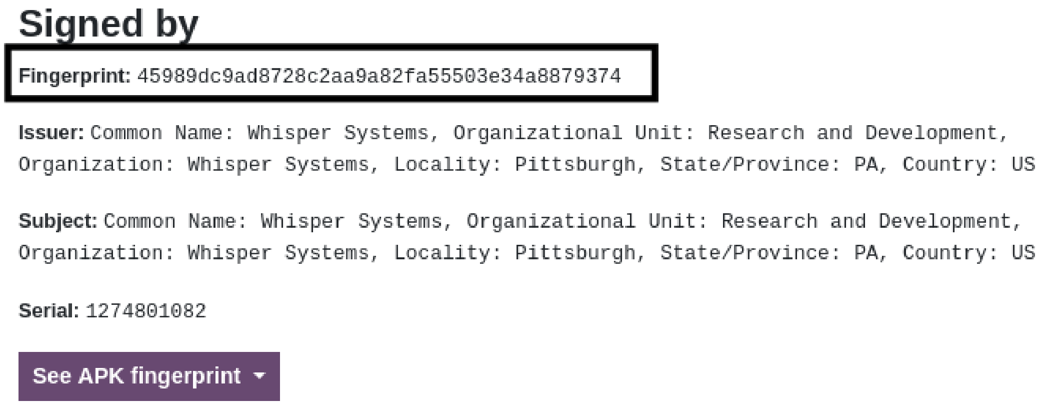
Signing certificate.

APKcli:



```
Metadata
================================================================================
MD5:            312a73a1053fc712db91e2d8cbd74b33
SHA1:           6cb5004e3f32f82f4cb59ef7aabd1f786555e511
SHA256:         bfcfd20c72ed9b3e87fa5de85f355026301c65c02f3d4a2bfad8e557ccd72a81
Package Name:   org.thoughtcrime.securesms
App:            Signal
This APK has Google Play metadata

Certificate
================================================================================
SHA1:           45989DC9AD8728C2AA9A82FA55503E34A8879374
Serial:         4BFBEBBA
Issuer:         C=US/ST=PA/L=Pittsburgh/O=Whisper Systems/OU=Research and Development/CN=Whisper System
Subject:        C=US/ST=PA/L=Pittsburgh/O=Whisper Systems/OU=Research and Development/CN=Whisper System
Not Before:     May 25 15:24:42 2010 UTC
```

Exodus Privacy:



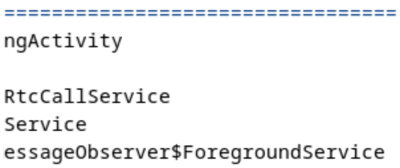
Signed by

Fingerprint: 45989dc9ad8728c2aa9a82fa55503e34a8879374

Issuer: Common Name: Whisper Systems, Organizational Unit: Research and Development, Organization: Whisper Systems, Locality: Pittsburgh, State/Province: PA, Country: US

Subject: Common Name: Whisper Systems, Organizational Unit: Research and Development, Organization: Whisper Systems, Locality: Pittsburgh, State/Province: PA, Country: US

Serial: 1274801082



```
=================================
ngActivity

RtcCallService
Service
essageObserver$ForegroundService
```

https://reports.exodus-privacy.eu.org/en/reports/org.thoughtcrime.securesms/latest/

ANALYSIS

APPs

Static analysis:

Look at permissions, components & certificate.

Tools: jadx, jeb, mobFS

Dynamic analysis:

Tools: Frida.

Emulator:

Tools: avd, genymotion

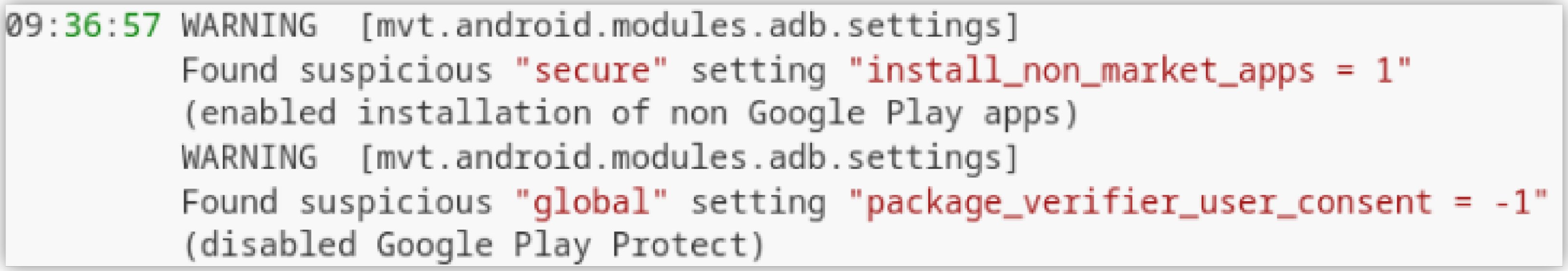
ANALYSIS

GLOBAL SETTINGS

Available in settings.json file (from MVT check-androidqf & check-adb)

MVT will flag some of these (related to malware & security)

1. Disable Google Play Protect (global)
   - verifier_verify_adb_installs
   - package_verifier_enable
   - package_verifier_user_consent
2. Disable crash / log reporting
   - send_security_reports (system)
   - send_action_app_error (global)



```
09:36:57 WARNING  [mvt.android.modules.adb.settings]
         Found suspicious "secure" setting "install_non_market_apps = 1"
         (enabled installation of non Google Play apps)
         WARNING  [mvt.android.modules.adb.settings]
         Found suspicious "global" setting "package_verifier_user_consent = -1"
         (disabled Google Play Protect)
```

ANALYSIS

SIGNS OF ROOTING

Rooting a phone leave signs:

1. Root binaries installed

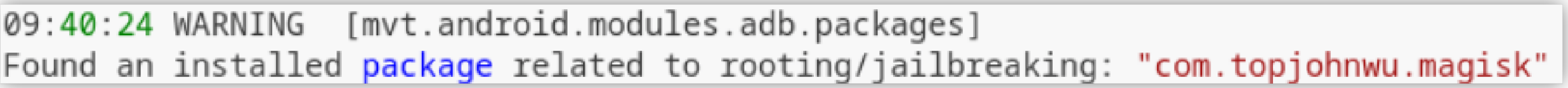
Ex. su, busybox, etc

Available in root_binaries.json file (from MVT check-androidqf)

2. Apps installed

Ex. com.topjohnwu.magisk

Available in packages_detected.json file (from MVT check-adb)



```
09:40:24 WARNING  [mvt.android.modules.adb.packages]
Found an installed package related to rooting/jailbreaking: "com.topjohnwu.magisk"
```

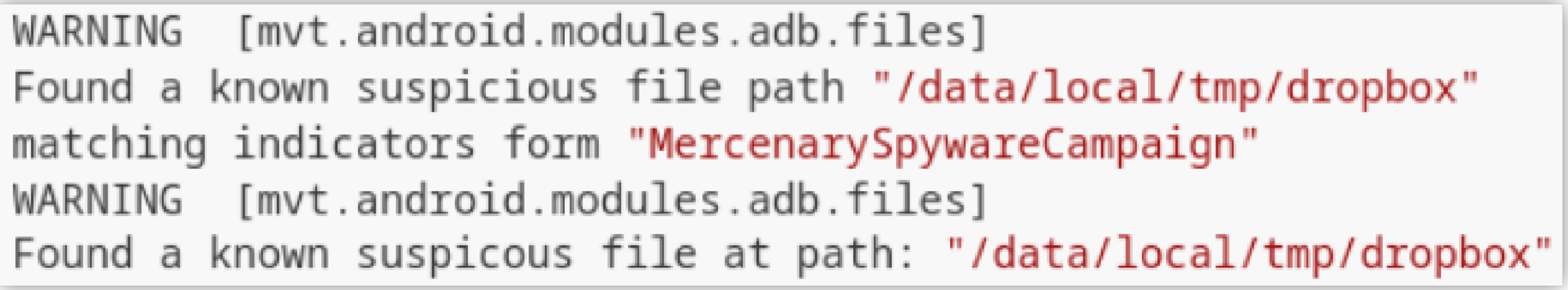
ANALYSIS

FILES

Listing of files creation & modification on the device

MVT matches with known malicious paths.

Manual analysis: suspicious paths & file manipulations during a timeframe.



```
WARNING  [mvt.android.modules.adb.files]
Found a known suspicious file path "/data/local/tmp/dropbox"
matching indicators form "MercenarySpywareCampaign"
WARNING  [mvt.android.modules.adb.files]
Found a known suspicous file at path: "/data/local/tmp/dropbox"
```

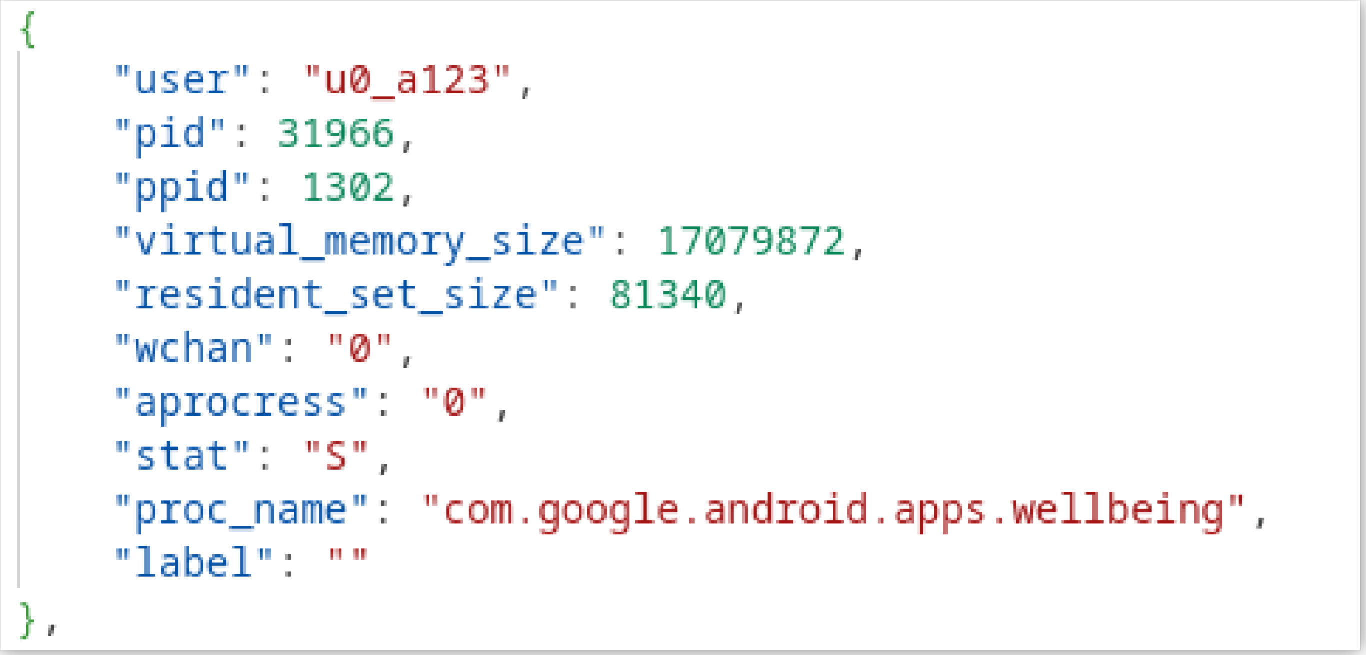
ANALYSIS

PROCESSES RUNNING

Listing of process running on the phone while the acquisition is in place

Information is available in processes.json (check-adb)

MVT checks against IOCs of malicious process names running



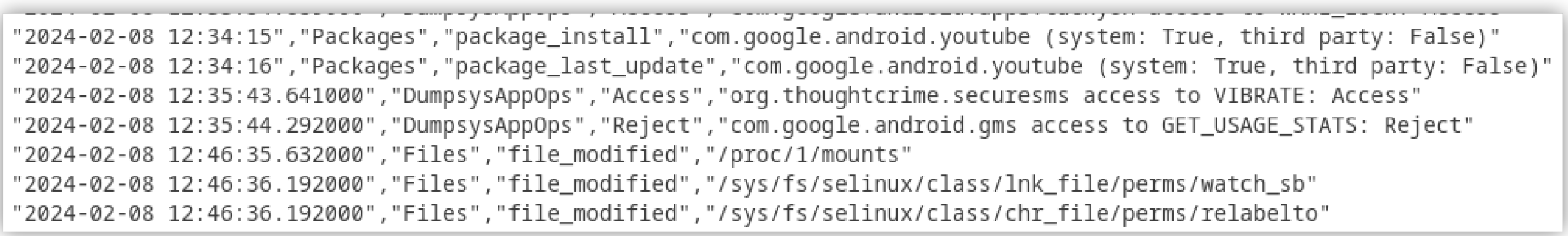
```
{
        "user": "u0_a123",
        "pid": 31966,
        "ppid": 1302,
        "virtual_memory_size": 17079872,
        "resident_set_size": 81340,
        "wchan": "0",
        "aprocress": "0",
        "stat": "S",
        "proc_name": "com.google.android.apps.wellbeing",
        "label": ""
},
```

ANALYSIS

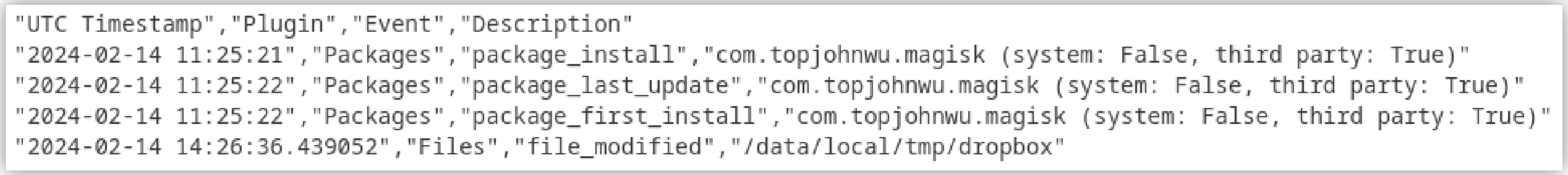
TIME FRAMED EVENTS

Narrow down the time scope based on a threat exposure on a limited time. Leverage the timestamps of the timeline to reconstruct events chronologically.

MVT creates a timeline.csv and a timeline_detected.csv (check-androidqf & check-adb)



```
"2024-02-08 12:34:15","Packages","package_install","com.google.android.youtube (system: True, third party: False)"
"2024-02-08 12:34:16","Packages","package_last_update","com.google.android.youtube (system: True, third party: False)"
"2024-02-08 12:35:43.641000","DumpsysAppOps","Access","org.thoughtcrime.securesms access to VIBRATE: Access"
"2024-02-08 12:35:44.292000","DumpsysAppOps","Reject","com.google.android.gms access to GET_USAGE_STATS: Reject"
"2024-02-08 12:46:35.632000","Files","file_modified","/proc/1/mounts"
"2024-02-08 12:46:36.192000","Files","file_modified","/sys/fs/selinux/class/lnk_file/perms/watch_sb"
"2024-02-08 12:46:36.192000","Files","file_modified","/sys/fs/selinux/class/chr_file/perms/relabelto"
```



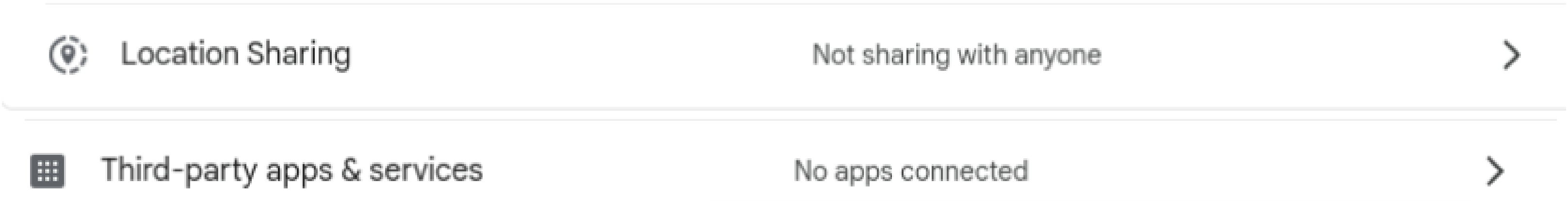
```
"UTC Timestamp","Plugin","Event","Description"
"2024-02-14 11:25:21","Packages","package_install","com.topjohnwu.magisk (system: False, third party: True)"
"2024-02-14 11:25:22","Packages","package_last_update","com.topjohnwu.magisk (system: False, third party: True)"
"2024-02-14 11:25:22","Packages","package_first_install","com.topjohnwu.magisk (system: False, third party: True)"
"2024-02-14 14:26:36.439052","Files","file_modified","/data/local/tmp/dropbox"
```

ANALYSIS

ACCOUNT SECURITY CONFIGS

Google Data & Privacy: https://myaccount.google.com/data-and-privacy?hl=en

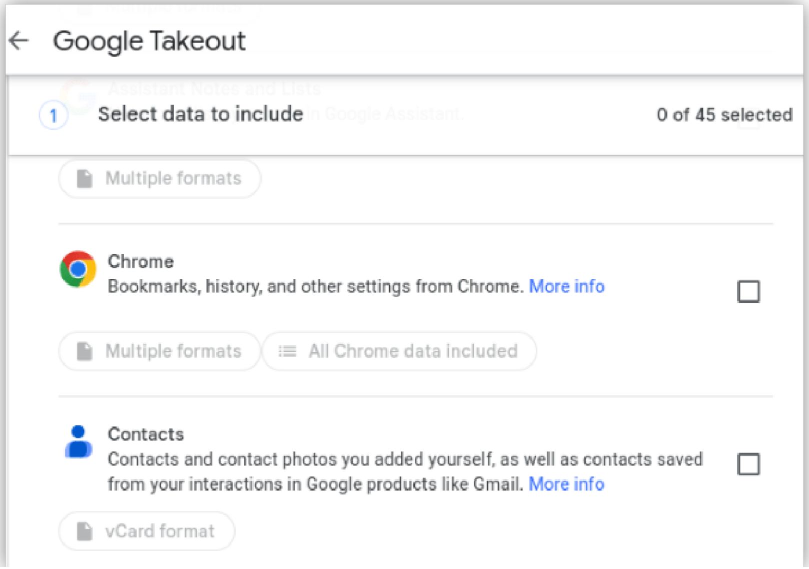
- 3erd party apps & services connected
- Location sharing. - Trusted devices



Location Sharing — Not sharing with anyone

Third-party apps & services — No apps connected

Google Takeout
https://takeout.google.com



Google Takeout

1 Select data to include — 0 of 45 selected

Multiple formats

Chrome
Bookmarks, history, and other settings from Chrome. More info □

Multiple formats — All Chrome data included

Contacts
Contacts and contact photos you added yourself, as well as contacts saved from your interactions in Google products like Gmail. More info □

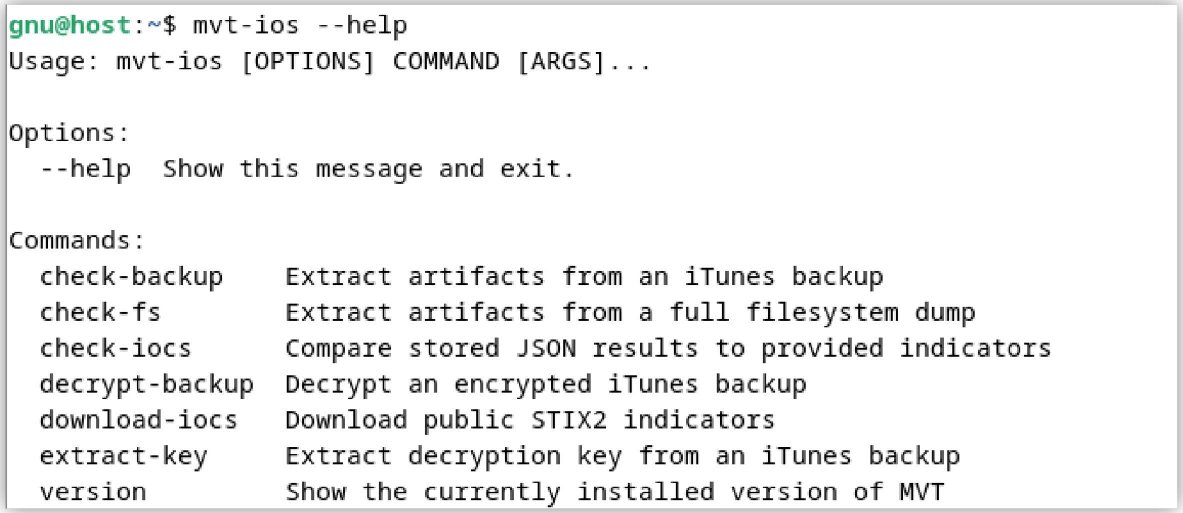
vCard format

ANALYSIS

iOS

- MVT automated analysis:

$ mvt-ios check-backup ./backup-ios --output out



```
gnu@host:~$ mvt-ios --help
Usage: mvt-ios [OPTIONS] COMMAND [ARGS]...

Options:
  --help  Show this message and exit.

Commands:
  check-backup    Extract artifacts from an iTunes backup
  check-fs        Extract artifacts from a full filesystem dump
  check-iocs      Compare stored JSON results to provided indicators
  decrypt-backup  Decrypt an encrypted iTunes backup
  download-iocs   Download public STIX2 indicators
  extract-key     Extract decryption key from an iTunes backup
  version         Show the currently installed version of MVT
```

- Triangle Check (Kaspersky):
  https://github.com/KasperskyLab/triangle_check
  Scan iTunes backups for traces of compromise by Operation Triangulation.
  More info: https://securelist.com/operation-triangulation/109842/

ANALYSIS

iOS

MVT: summary of modules:

- applications.py: installed applications on the device
- calendar.py: calendar events
- calls.py: call logs
- chrome_history.py: chrome browsing history
- contacts.py: contacts database
- firefox_history.py: Firefox browsing history
- global_preferences.py: global preference settings
- sms.py: SMS messages
- sms_attachments.py: analyzes attachments sent or received via SMS
- whatsapp.py: analyzes WhatsApp messages and metadata

https://github.com/mvt-project/mvt/tree/main/mvt/ios/modules/mixed

https://github.com/mvt-project/mvt/tree/main/mvt/ios/modules/backup

POST-ASSESSMENT

1. Follow-up
    - Communication
    - Recommended actions
    - Long term support

2. Outcome
    - Report
    - Research
    - Accountability

3. Lessons learned
    - Methodology & Documentation

QUESTIONS

Questions?