Forensic Analysis of Xiaomi IoT Ecosystem

By:
Evangelos Dragonas

From the proceedings of
The Digital Forensic Research Conference
DFRWS USA 2021
July 12-15, 2021

Forensic Analysis of Xiaomi IoT Ecosystem

Evangelos Dragonas
University of Piraeus (UNIPI), Greece
DFRWS USA
12nd JULY 2021

Whoami

- Live in Greece
- Work as a Digital Forensics Examiner
- PhD candindate in the area of IoT Forensics (UNIPI)
- Created/Maintain the DFIR research blog atropos4n6.com
- Nominee for the award of the “DFIR Article of the Year” category at the 2021 Forensic 4:cast Awards (Post your votes at http://f4c.me/v21)

Contents

Xiaomi

- One of the world's biggest manufacturers (smartphones and IoT)
- Xiaomi's IoT devices are becoming more and more likely to appear in smart home investigations
- Is popular in Europe and is coming to the US as well

Bloomberg

Technology

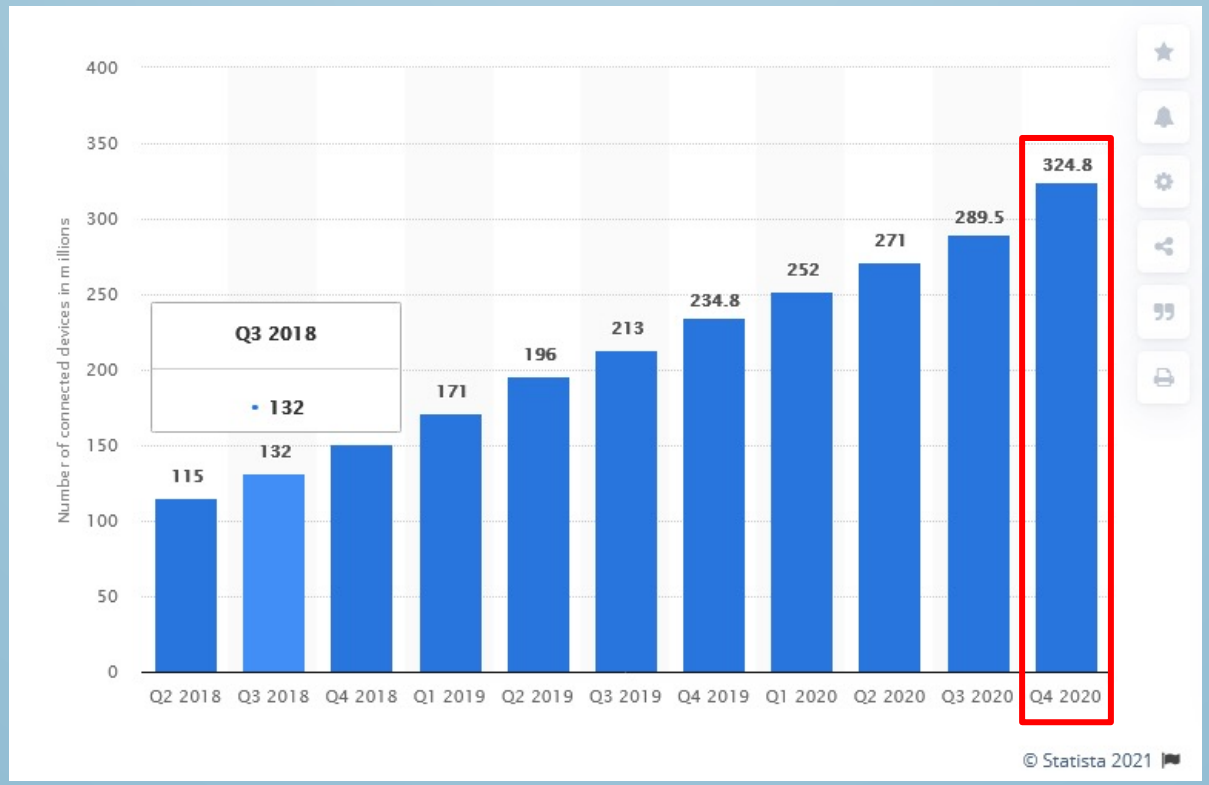
U.S. Agrees to Remove Xiaomi From Blacklist After Lawsuit

Bloomberg News
May 12, 2021, 8:31 AM GMT+3 *Updated on May 12, 2021, 7:53 PM GMT+3*

Source: https://www.bloomberg.com/news/articles/2021-05-12/xiaomi-u-s-government-agree-to-drop-firm-from-blacklist

Xiaomi IoT Statistics

Number of Xiaomi IoT connected devices worldwide from 2018-2020 (in millions)*



Source: https://www.statista.com/statistics/967485/worldwide-xiaomi-number-of-connected-devices/

Xiaomi IoT Ecosystem

- Xiaomi and third-party partners offer a diversity of IoT solutions:

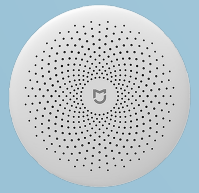
Sensors	Power Sockets & Switches	Smart Lighting	Cleaning Gear	Household Appliances
Health Care	Cameras	Air Treatment	Personal Transport	Other

Contents

Subset of this Research

Mi Motion Sensors

Mi Door and Window Sensors



Mi Control Hub

Mi Wireless Switch

Mi Temperature and Humidity Sensors

Mi LED Smart Bulbs

Mi Smart Power Plugs

Mi Home Security Camera 360 1080p

Mi WiFi Smart Speaker

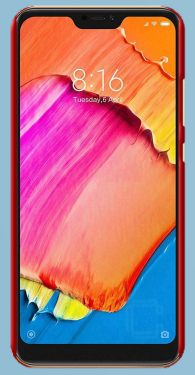
Mi Smart Electric Toothbrush T500

Mi Electric Scooter

Mi Robot Vacuum Mop P

*Products' pictures retrieved from official Xiaomi websites: https://www.mi.com, https://www.mistore-greece.gr

Equipment and Setup 1/2



- Redmi Note 6 Pro
- Android 9
- MIUI 12.0.1.0
- Rooted with Magisk v22

- Mi Account

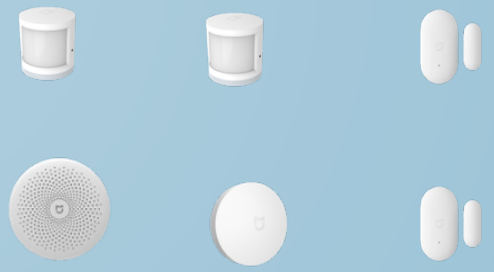
WiFi

ZigBee

- Mi Home app
- com.xiaomi.smarthome
- version 6.6.701

Equipment and Setup 2/2

Source: https://floorplanner.com



- Devices were assigned to the smart home
- They were managed using the smartphone
- They were used for ~2 months
- Different settings were chosen from time to time

Contents

Sources of Evidence Identification

- Smartphone Application
- Cloud
- Device
- Local API (Applies only to the Xiaomi Mi Smart Speaker)
- Network Traffic

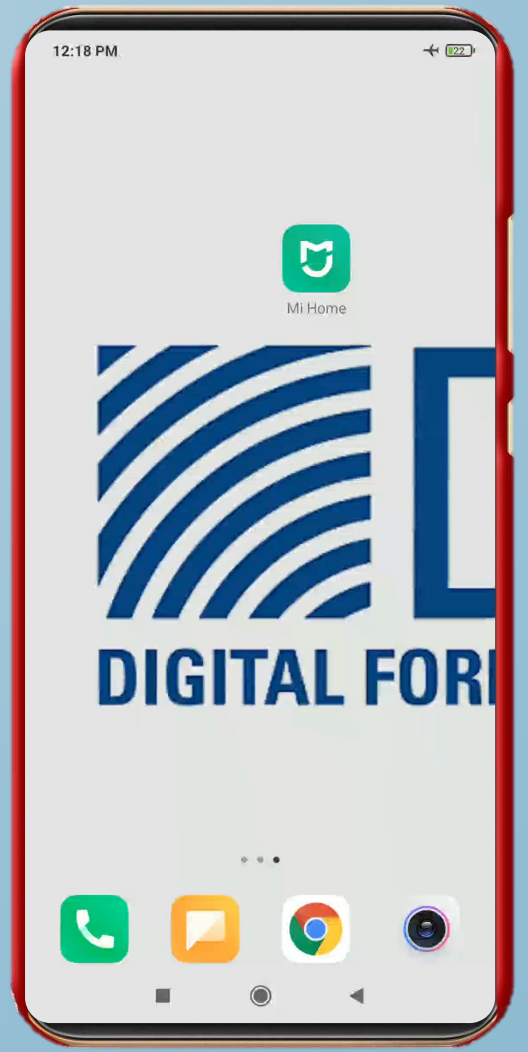
Evidence Extraction Method

- Smartphone Application
  - Airplane Mode ON
  - Application cache was not cleared
  - ADB commands to retrieve the data

Contents

Smartphone Application-Mi Home

- Smart home Overview
  - Current status of IoT devices (Online-Offline and/or ON-OFF)
  - Devices assigned to each Room
  - Rooms used
  - Logs of SPECIFIC devices (Requires Internet Connection-only few records are stored locally)
- Automation Information
  - List of current Scenes (automatically/user created)
  - Current status of each Scene (Enabled/Disabled)
  - Configuration of each Scene (Room and/or Device specific)
  - Logs of each Scene (Requires Internet Connection)
- Profile Information
  - Personal Info (Account ID, Name, etc.) (Requires Internet Connection)
  - Application Settings



Mi Home – Account artifacts

/com.xiaomi.smarthome/databases/miio.db

Table: shareuserrecord — Filter in any column

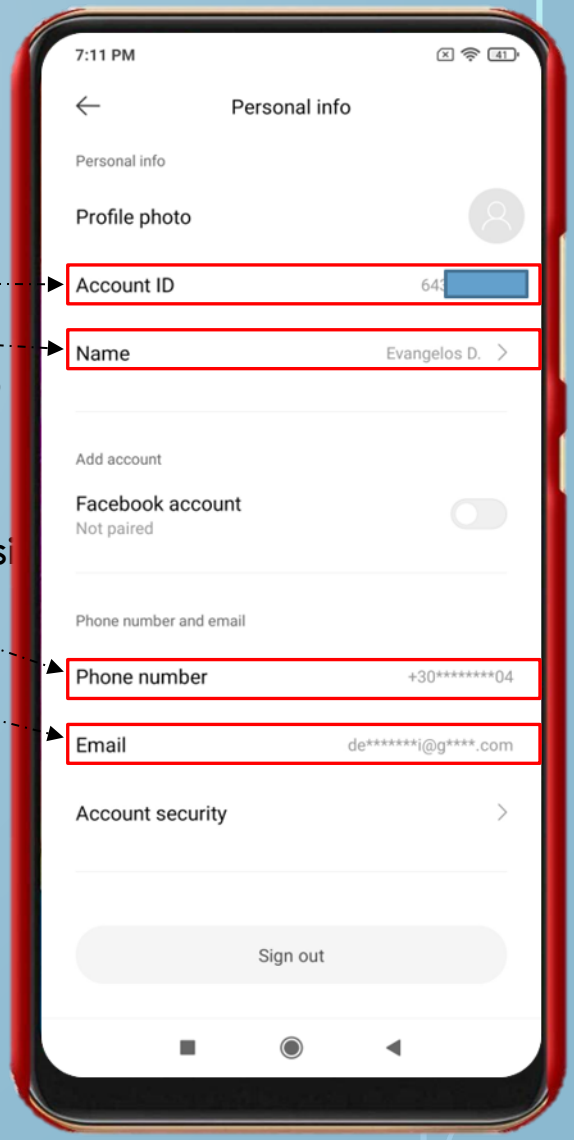
	birth	email	id	localPath	nickName	phone	sex	shareTime	url	userId
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	NULL	[redacted]@gmail.com	199	NULL	Evangelos D.	+30[redacted]	Not set	1617564251	NULL	643[redacted]

- Email
- Nickname
- Phone
- Share timestamp
- User ID

/com.xiaomi.smarthome/shared_prefs/shared_user_info_list_UID.xml (NOT populated in the latest versi

```
<string name="content">{"list":[{
"userId":643[redacted],
"userName":"c5[redacted]",
"nickname":"Evangelos D.",
"create_time":1617448410000,
"infoupdate_time":1617448410000,"
```

- User ID
- Username
- Nickname
- Account creation timestamp
- Account info last update timestamp

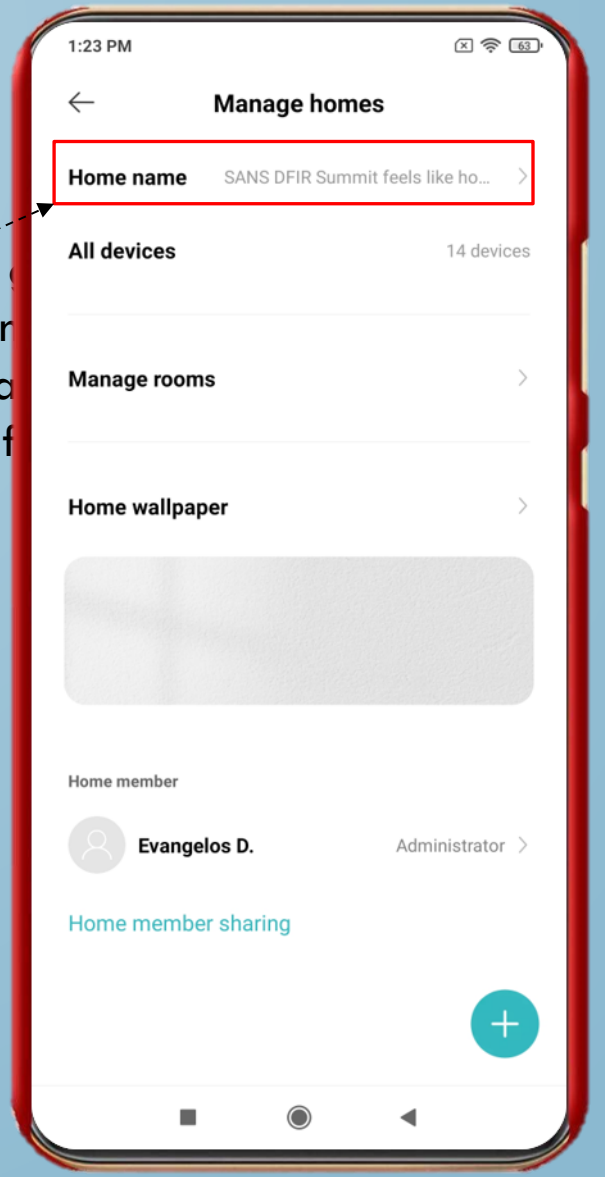


Mi Home – Smart Home artifacts

- /com.xiaomi.smarthome/shared_prefs/home_roomv_manager_sp_.xml


```
<string name="home_room_content">{"homelist":[{
"background":"style_1",
"bssid":"",
"city_id":"0",
"desc":"",
"icon":"style 1 favorites",
"id":"9130[redacted]",
"latitude":"0",
"longitude":"0",
"address":"",]
"name":"SANS DFIR Summit feels like home",
"shareflag":0,
"uid":643[redacted],
"dids":["lumi.158d000[redacted]"],"status":"1",
"roomlist":[
    {"bssid":"","id":"9130[redacted]","name":"Balcony","pa
    {"bssid":"","id":"9130[redacted]","name":"Living room"
    {"bssid":"","id":"9130[redacted]","name":"Workshop","p
    {"bssid":"","id":"9130[redacted]","name":"Back yard","
    {"bssid":"","id":"9130[redacted]","name":"Bathroom","p
    {"bssid":"","id":"9130[redacted]","name":"Bedroom","pa
```

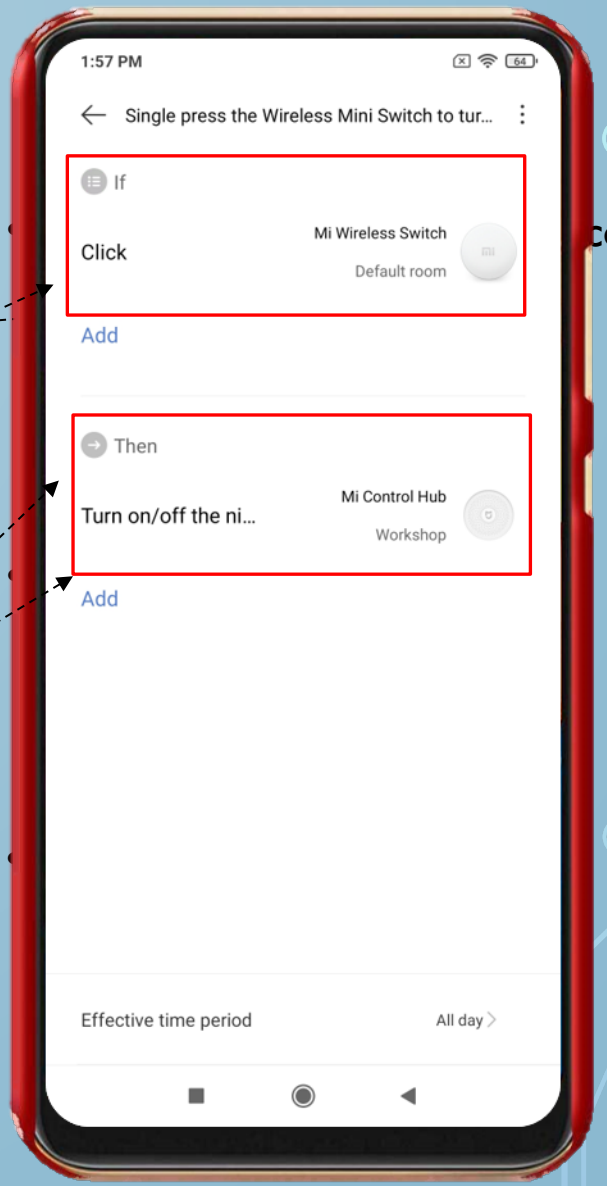

- Smart Home ID
- Smart Home name &
  (location authorizatio
- Smart Home share sta
- Smart Home rooms inf
  - Room Name
  - Room ID
  - Creation time
  - Devices assigned
  - Share status



Mi Home – Smart Home's automation artifacts

- /com.xiaomi.smarthome/shared_prefs/MD5(UserID)scene_list_cache.xml

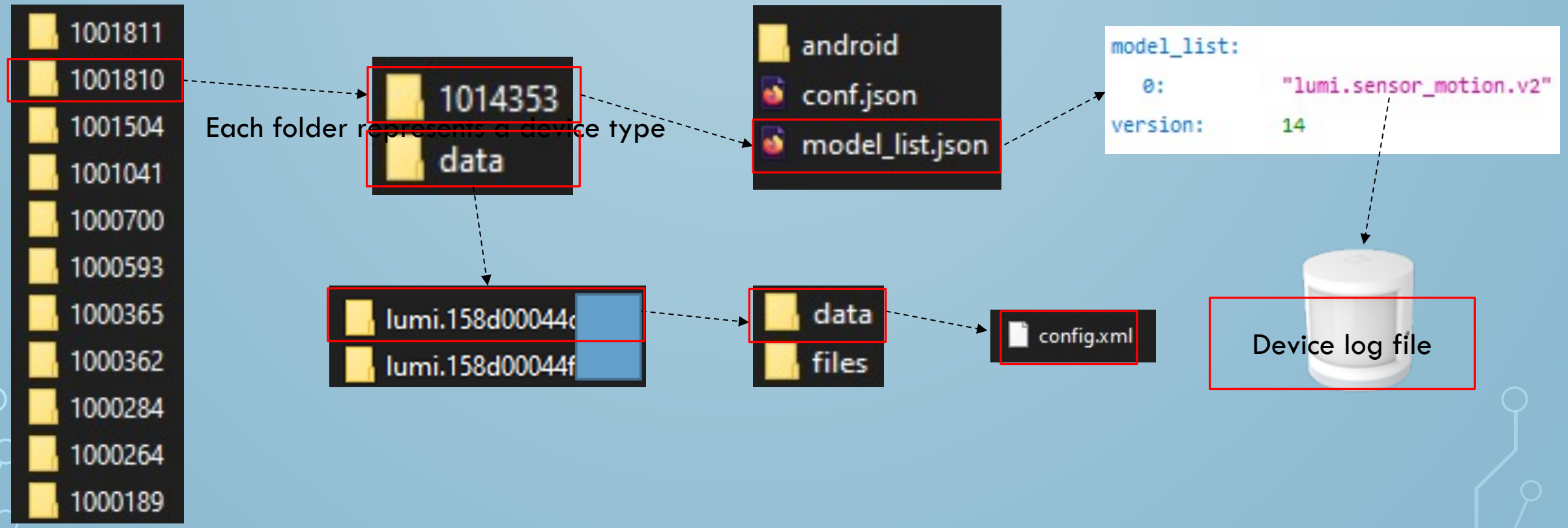
```
<string name="scene_list">
{
"0":
    {"us_id":273[redacted],
    "type":1,
    "status":0,
    "uid":643[redacted],
    "name":"Single press the Wireless Mini Switch to turn on\/off the night light",
    "st_id":15,
    "sr_id":0,
    "identify":"",
    "local_dev":"332[redacted]",
    "create_time":1617904461,
    "setting":
        {"action_list":
        [
            {"id":1,"keyName":"Turn on\/off the night light","model":"lumi.gateway.mieu01","name":"Mi Control Hub"
            ,"payload":{"command":"lumi.gateway.mieu01.toggle_light","delay_time":0,"did":"332[redacted]","extra":"[1,19,7,111,[40,2],0,0]"
            ,"total_length":0,"value":"toggle"},"sa_id":0,"tr_id":0,"type":0}],
        "enable":"0",
        "enable_push":"0",
        "launch":
            {"attr":[{"device_name":"Mi Wireless Switch",
            "did":"lumi.158d000485[redacted]",
            "enable":true,
            "extra":"[1,6,1,0,[0,0],0,0]",
            "key":"event.lumi.sensor_switch.v2.click",
            "name":"Click",
            "src":"device",
            "tempId":-1,
            "tr_id":101,
            "value":""}],"express":1}},
        "authed":["3326[redacted]","lumi.158d00048[redacted]],
        "real_st_id":15
    },
"1":{"us_id":273[redacted],"type":1,"status":0,"uid":643[redacted],"name":"Double press the Wireless Mini Switch to turn the security mode
```



cenes:

Mi Home – IoT device artifacts

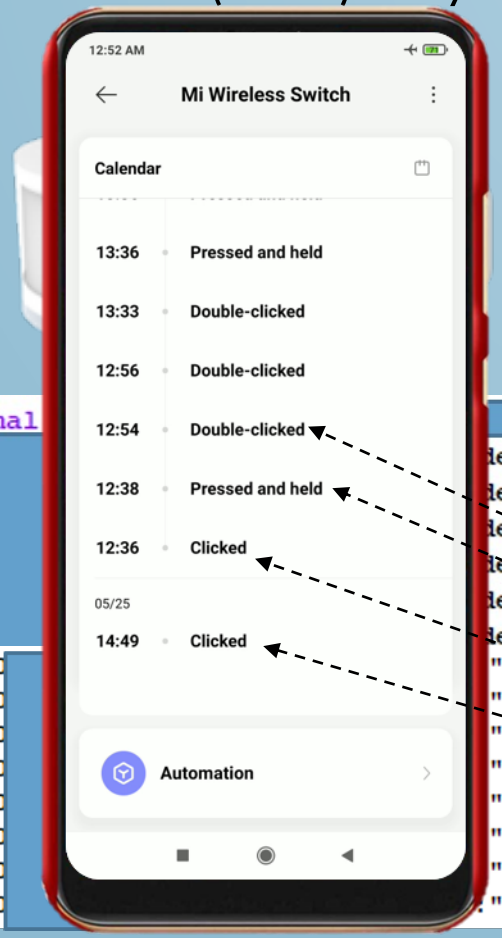
- /com.xiaomi.smarthome/files/plugin/install/rn/1001810/1014353/model_list.json



- /com.xiaomi.smarthome/files/data/lumi.XXXXXXX/data/config.xml

Mi Home – Mi Motion, Door and Window Sensors and Wireless Switch artifacts

- For these devices, the config.xml files:
  - Are fixed in size (~3KB). They will only store the 20 latest events recorded by each device



Occurrence Timestamp

Event Type

Storage Timestamp

<string name="Log_Normal

{"did":"lumi.158d000

{"did":"lumi.158d000

{"did":"lumi.158d000

{"did":"lumi.158d000

{"did":"lumi.158d000

{"d {"did":"lumi.158d00

{"did":"lumi.158d00

{"did":"lumi.158d00

{"did":"lumi.158d00

{"did":"lumi.158d00

{"did":"lumi.158d00

{"did":"lumi.158d00

">{"value":[

device_log","value":"[\"[1623178462,[\\\"event.close\\\",[]]]\"]","time":1623178464},

device_log","value":"[\"[1623177618,[\\\"event.open\\\",[]]]\"]","time":1623177620},

device_log","value":"[\"[1623177436,[\\\"event.close\\\",[]]]\"]","time":1623177437},

device_log","value":"[\"[1623149624,[\\\"event.open\\\",[]]]\"]","time":1623149625},

device_log","value":"[\"[1623149141,[\\\"event.close\\\",[]]]\"]","time":1623149142},

device_log","value":"[\"[1623144586,[\\\"event.open\\\",[]]]\"]","time":1623144587},

"device_log","value":"[\"[1622111795,[\\\"event.long_click_press\\\",[]]]\"]","time":1622111797},

"device_log","value":"[\"[1622111792,[\\\"event.long_click_press\\\",[]]]\"]","time":1622111793},

"device_log","value":"[\"[1622111613,[\\\"event.double_click\\\",[]]]\"]","time":1622111615},

"device_log","value":"[\"[1622109408,[\\\"event.double_click\\\",[]]]\"]","time":1622109409},

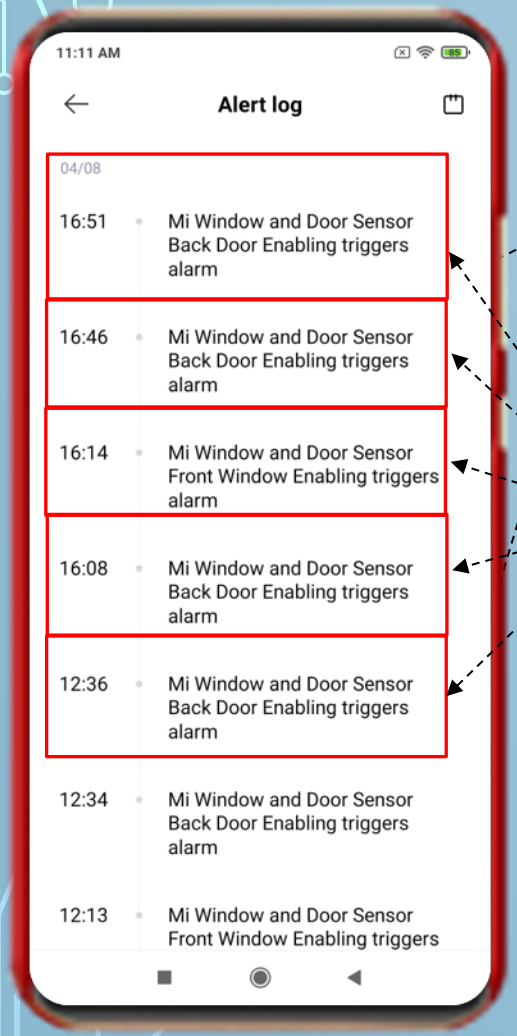
"device_log","value":"[\"[1622109266,[\\\"event.double_click\\\",[]]]\"]","time":1622109267},

"device_log","value":"[\"[1622108325,[\\\"event.long_click_press\\\",[]]]\"]","time":1622108327},

"device_log","value":"[\"[1622108168,[\\\"event.click\\\",[]]]\"]","time":1622108170},

"device_log","value":"[\"[1621943380,[\\\"event.click\\\",[]]]\"]","time":1621943381}],

Mi Home – Mi Control Hub artifacts



- The config.xml file stores specific information about this device, including:


```
<string name="332[redacted]_main_page_64[redacted]">{"value":
{"guardStatus":"off",
"lightRgb":0,
"rgbValue":1191117312,
"corridorLightValue":"on",
"cacheLog":"04/08 16:51 Mi Window and Door Sensor Back Door Enabling triggers alarm"},
"expire":8640000000,"time":1624190121033}</string>
<string name="Log_Normal_device_log_33[redacted]">{"value":[
{"did":"33[redacted]","type":"prop","key":"device_log","value":"[\"[1617889913,[\\\"event.arming_magnet_open\\\",
{"did":"33[redacted]","type":"prop","key":"device_log","value":"[\"[1617889584,[\\\"event.arming_magnet_open\\\",
{"did":"33[redacted]","type":"prop","key":"device_log","value":"[\"[1617887666,[\\\"event.arming_magnet_open\\\",
{"did":"33[redacted]","type":"prop","key":"device_log","value":"[\"[1617887304,[\\\"event.arming_magnet_open\\\",
{"did":"33[redacted]","type":"prop","key":"device_log","value":"[\"[1617874572,[\\\"event.arming_magnet_open\\\",
{"did":"33[redacted]","type":"prop","key":"device_log","value":"[\"[1617874440,[\\\"event.arming_magnet_open\\\",
{"did":"33[redacted]","type":"prop","key":"device_log","value":"[\"[1617873234,[\\\"event.arming_magnet_open\\\",
{"did":"33[redacted]","type":"prop","key":"device_log","value":"[\"[1617872749,[\\\"event.arming_magnet_open\\\",
{"did":"33[redacted]","type":"prop","key":"device_log","value":"[\"[1617561065,[\\\"event.arming_magnet_open\\\",
{"did":"33[redacted]","type":"prop","key":"device_log","value":"[\"[1617476259,[\\\"event.arming_magnet_open\\\",
{"did":"33[redacted]","type":"prop","key":"device_log","value":"[\"[1617454983,[\\\"event.arming_magnet_open\\\",
```

Contents

Findings

- Xiaomi IoT Ecosystem is an under-researched field of IoT Forensics, which can be valuable in current/future smarthome investigations
- The forensic analysis of Mi Home application can provide information about:
  - Smarthome's structure (Rooms, IoT devices present, etc.)
  - Smarthome's Automation system (Scenes' configuration, logs, etc.)
  - Smarthome's devices' logs or/and settings
  - Owner's personal information

Points of Consideration

- Config.xml file's content depends on the device type. This means:
  - For some devices, it may not exist
  - For some devices, it may only store settings or other information about the device
  - For some devices, it may store logs of the device
- Most logs (scene/device) will reside in the Cloud. This means:
  - If you pull data from the Cloud using the application, typically this data will remain available until you exit the application.
  - Consider taking pictures of the smartphone screen (as some data will not be available if Internet connection is lost).
  - If BLE devices are present, make sure to connect to them, pull their data and take pictures of that.

Contents

References

- **Smart Home IoT Forensics, Birhanu Addisu Afework, 2019.**

  [Link: https://lifs.hallym.ac.kr/pubs/2019-Thesis-MSc-Addisu-Smart_Home_IoT_Forensics.pdf]

- **Having fun with IoT: Reverse Engineering and Hacking of Xiaomi IoT Devices, Giese Dennis, 2018.**

  [Link: https://www.researchgate.net/publication/328743723_Having_fun_with_IoT_Reverse_Engineering_and_Hacking_of_Xiaomi_IoT_Devices]

- **Github theAtropos4n6**

  [Link: https://www.github.com/theAtropos4n6]

Acknowledgments

- Prof. Costas Lambrinoudakis (UNIPI)

Q&A

Evangelos Dragonas

PhD Candidate, UNIPI, Greece

Contact info:

@theAtropos4n6

theatropos4n6@gmail.com

theAtropos4n6#4634

https://www.atropos4n6.com

Atropos4n6

2021 Forensic 4:cast Awards
(Post your votes at: *http://f4c.me/v21*)