The VARIoT project - a source of open data regarding IoT security

Vulnerability and Attack Repository for IoT

CIRCL
Computer Incident
Response Center
Luxembourg

Gérard Wagener

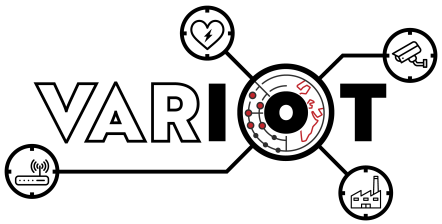
TLP:WHITE

info@circl.lu

2021-11-17 -Luxembourg
Internet Days 2021

Co-financed by the European Union
Connecting Europe Facility

Consortium



- CEF Telecom - Public Open Data
- CEF-TC-2018-5
- Project launch: 01.07.2019
- Project end: 30.06.2022

Co-financed by the European Union
Connecting Europe Facility

Project objectives in detail 1/2

- Create a database covering vulnerabilities and exploits related to IoT devices
- Improve IoT-related data collection through large-scale systematic mapping of IoT devices on the Internet
- Create a database of aggregated, correlated and enhanced information of various types relating to IoT
  - Vulnerabilities
  - Exploits
  - Indicators of Compromise (IoC)
  - Events
  - Incidents
  - Malware samples
  - etc

Project objectives in detail 2/2

- Create datasets of IoT traffic, of both legitimate and malicious natures, including models learnt to characterize these traffics, and their associated features, as well as raw packet captures
- Create mechanisms of active monitoring and harvesting of information of IoT devices and information about new types of threats
- Create interfaces to share selected data
  - The publication of the data on the EDP such as regularly updated information on
    - the number of infected or vulnerable devices in Member States,
    - the number of device types by Member States
    - their integration with the Malware Information Sharing Platform (MISP)
    - reporting via Shadowserver's free daily remediation feeds to National CSIRTs and verified network owners

Create datasets of IoT traffic 1/2

Network traffic under normal /compromised conditions

Samsung UE55ES6100
TP-Link HS110
Google Chromecast Ultra
Netatmo Smart Rain Gauge
Mobvoi TicWatch Sensor Set
Xiaomi Mi Air Purifier 3H
Smarter Coffee 2nd Generation
Raspberry Pi 4 Model B
Honeywell C2 Wi-Fi Home Security Camera
Leotec Android TvBox GCX2
Xiaomi Mi Home Security Basic Camera 1080
Google Nest Hub
Netatmo Smart Alarm
TP-Link HS110
Netatmo Smarter Home Weather Station
Leotec Android TvBox GCX2 432

BeagleBoard BeagleBone AI
Smarter Fridge Cam
MikroTik RB951Ui2HnD
Smarter iKettle
Xiaomi Mi Sensor Set
Xiaomi Mi LED Ceiling Light
Amazon Echo Show
Netatmo Smart Alarm System with Camera
Amazon Echo Dot 3rd Gen
TP-Link Tapo C200 IP Camera
Honeywell W1 Water Leak and Freeze Detector
Google Home Mini
Xiaomi Mi Smarter Plug (Wifi)
Xiaomi Mi LED Smart Bulb
TP-Link Smart Bulb Tapo L510E
...

Datasets available on `https://data.europa.eu/data/datasets`

Create datasets of IoT traffic 2/2

Example

- Wondering why your Xiaomi-MiHomeSecurityBasicCamera1080p is sending UDP packets to port 10001?
- Check dataset Xiaomi MiHomeSecurityBasic Camera1080p normal / compromised conditions dataset

```
IP 172.18.1.10.34317 > 47.91.78.150.10001: UDP, length 24
```

https://data.europa.eu/data/datasets/https-datos-gob-es-catalogo-pudat0001-seguridad-iot-trafico?locale=en

The number of infected or vulnerable devices

Open data available for IPs world wide

- Data is available since 2021-05-03 to today
- It is daily updated with a day of delay

Example (Infected devices (Luxembourg) on 2021-10-29)

```
infection,geo,country,count
mirai,LU,Luxembourg,198
android.hummer,LU,Luxembourg,18
android.bakdoor.prizmes,LU,Luxembourg,14
android.teleplus,LU,Luxembourg,13
flubot,LU,Luxembourg,7
android.rootnik,LU,Luxembourg,2
...
```

`https://cra.circl.lu/opendata/variot/iot-exposed-infected-device-stats/`

Co-financed by the European Union
Connecting Europe Facility

Shadowserver remediation feeds 1/2

Processing

- CIRCL automatically dispatches identified vulnerable / infected systems to network owners
- Automation software is open-source `https://github.com/rommelfs/ticket-tools`
- Contact addresses are used from **whois**
- To ensure efficient processing records in **whois** should be correct, maintained and processed.

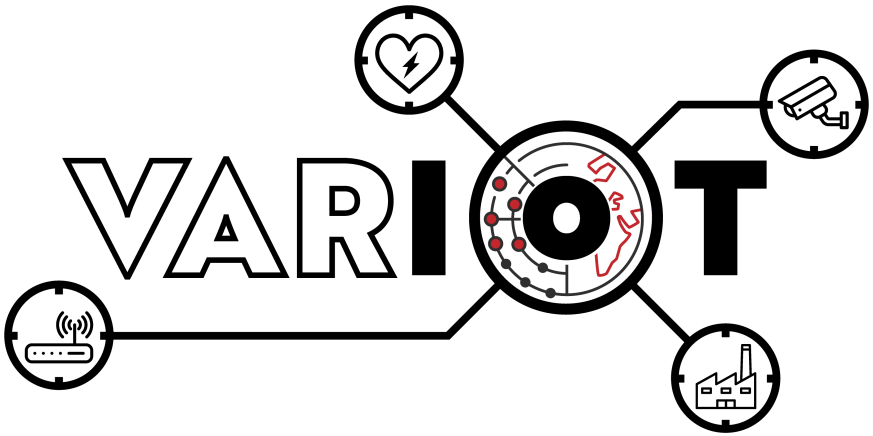
Shadowserver remediation feeds 2/2

Example

```
Dear Abuse teams,

CIRCL is the CERT/CSIRT for the private sector...

... the following list of client(s) appears to be compromised

asn, ip, timestamp, malware, src_port, dst_ip, dst_port,
    ↪ dst_host, proto
xx,xx,2021-10-28 02:52:09,flubot,4454,xx,80,xx,tcp

Please disinfect or even better re-install the concerned
    ↪ machines. Should they be belonging to a client, please
    ↪  inform them accordingly.
...
```

Questions?

Vulnerability and Attack Repository for IoT



- Gérard Wagener (CIRCL)
- gerard.wagener@circl.lu
- www.variot.eu
- www.twitter.com/VARIoT_project

Co-financed by the European Union
Connecting Europe Facility