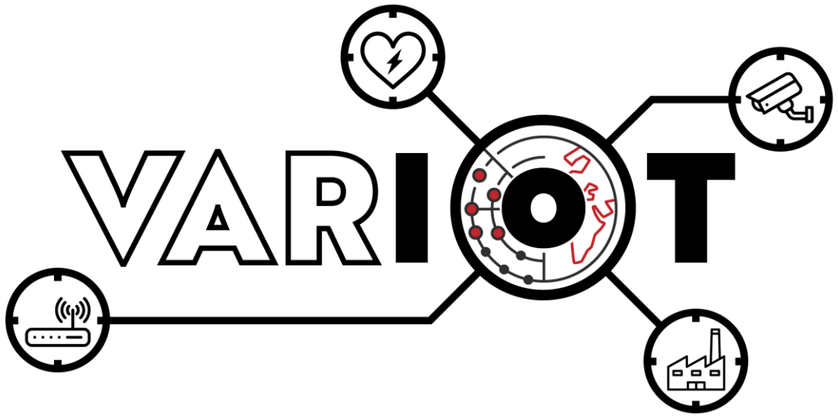
Vulnerability and Attack Repository for IoT

Contact: info@variot.eu

Co-financed by the Connecting Europe Facility of the European Union

Globecom 2021

Vulnerability and Attack Repository for IoT



CEF Telecom - Public Open Data

CEF-TC-2018-5

Project launch: 01.07.2019

Project end: 30.06.2022

Co-financed by the Connecting Europe Facility of the European Union

Consortium

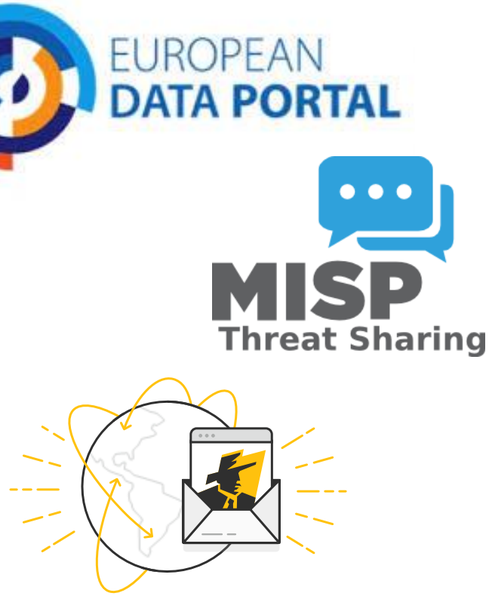
Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	NASK-PIB	Poland *(Coordinator)*
Stichting the Shadowserver Foundation Europe	Shadowserver	Netherlands
Security Made In Letzebuerg G.I.E.	SMILE	Luxembourg
Institut Mines-Télécom - Télécom SudParis	IMT-TSP	France
Mondragon Goi Eskola Politeknikoa Jose Maria Arizmendiarrieta S COOP	MGEP	Spain

Project objectives

Provide actionable information regarding IoT devices which can be processed manually or automatically to ensure cybersecurity of these devices.

Relevant data will be made available through

- European Data Portal (EDP)
- Malware Information Sharing Platform (MISP)
- Shadowserver’s free daily remediation feeds



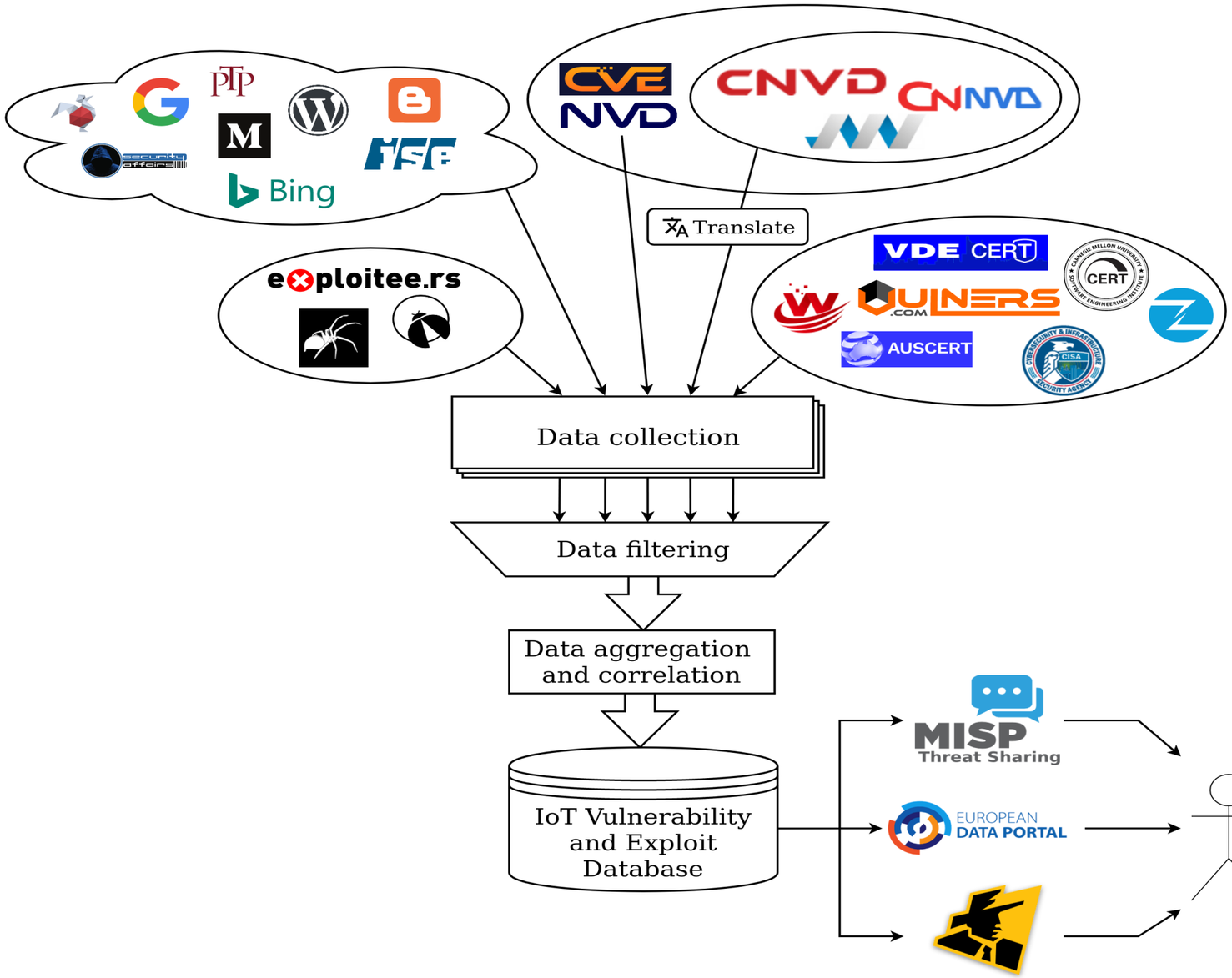
Co-financed by the Connecting Europe Facility of the European Union

Main outcomes

- database of information on vulnerabilities and exploits of IoT devices
- mechanisms of correlation of various types of information
- vulnerability information search engine
- catalogue of IoT device types
- catalogue of IoT related malware
- scanning the Internet to identify vulnerable, publicly available IoT devices
- system for Network Anomaly Detection of IoT Devices
- Internet Draft documents describing the open data with its implementation in MISP
- aggregated and anonymised statistics on infected and vulnerable IoT devices

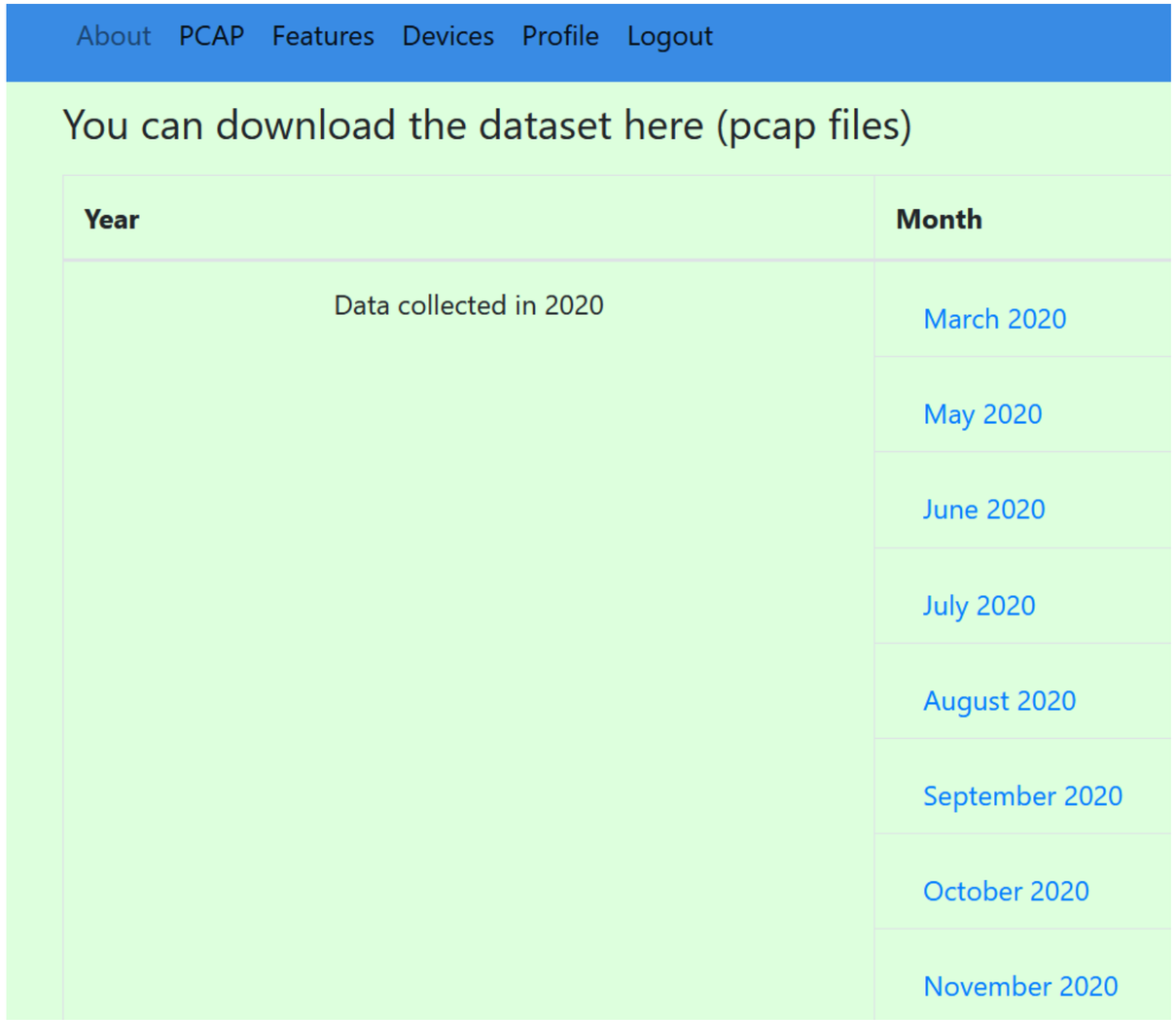
Co-financed by the Connecting Europe Facility of the European Union

Vulnerability database



Testbed to generate IoT network traffic

https://variot.telecom-sudparis.eu/



Co-financed by the Connecting Europe Facility of the European Union

84 datasets found

Keywords: VARIoT ×

Infected and Exposed IoT device statistics

This is a dataset containing a county level breakdown of infected and Exposed IoT devices detected through sinkholes, honeypots and darknets operated by The Shadowserver Foundation and its partners. The data is GROUPED by IoT related threats. In some cases a vulnerability id is provided as a threat name — this is for cases where an IP was seen…

CSV

Created: 09.06.2021 16:42

La plateforme de données luxembourgeoise

IoT security - network traffic under normal conditions - Samsung UE55ES6100

Dataset created under the Connecting Europe Facility of the European Union programme, VARIOT project TENtec n. 28263632. Developed by the Intelligent Systems for Industrial Systems group supported by the Department of Education, Language policy and Culture of the Basque Government. This dataset comprises Samsung UE55ES6100 Iot device network…

GNU zip

Updated: 31.03.2021 09:09 **Created:** 31.03.2021 09:09

datos.gob.es

Shadowserver's honeypots

Look here

VARIoT project database: https://variotdbs.pl/

Polish Open Data: https://dane.gov.pl/

European Data Portal: https://data.europa.eu/

Co-financed by the Connecting Europe Facility of the European Union

Vulnerability and Attack Repository for IoT

Contact: info@variot.eu

www.variot.eu

@VARIoT_project

Co-financed by the Connecting Europe Facility of the European Union

Globecom 2021