Vulnerability and Attack Repository for IoT

Anna Felkner (NASK-PIB)

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

Warsaw, 10 October 2019

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

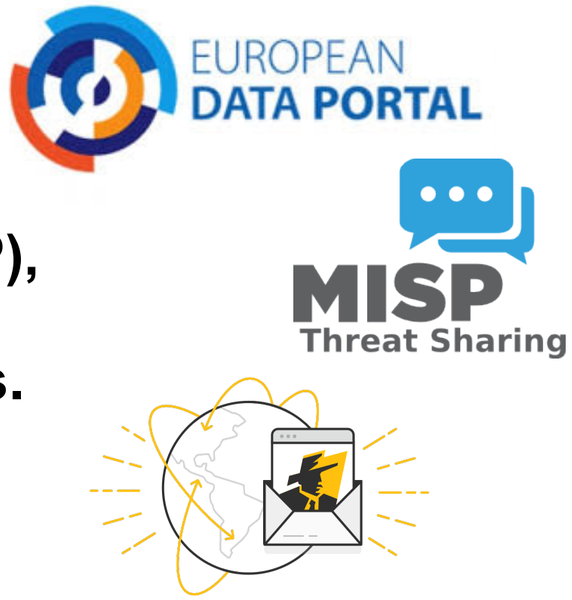
Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	NASK-PIB	Poland *(Coordinator)*
Stichting the Shadowserver Foundation Europe	Shadowserver	Netherlands
Security Made In Letzebuerg G.I.E.	SMILE	Luxembourg
Institut Mines-Télécom - Télécom SudParis	IMT-TSP	France
Mondragon Goi Eskola Politeknikoa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

Project objectives

Creating a service providing actionable information regarding IoT devices which can be processed manually or automatically and that can be used to ensure their cybersecurity.

Relevant data will be made available through

- **the 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

Project objectives in detail

- 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.

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

Project objectives in detail

- 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,
    - 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.

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

Vulnerability and Attack Repository for IoT

Anna Felkner (NASK-PIB)
anna.felkner@nask.pl

www.variot.eu
www.twitter.com/VARIoT_project

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