VARIOT

Vulnerability and Attack Repository for IoT

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

and by the program of the Minister of Science and Higher Education entitled "PMW" in the years 2020-2022

CEF Telecom – Public Open Data

CEF-TC-2018-5

Project launch: 01.07.2019

Project end: 30.06.2022

Consortium

NASK

SHADOWSERVER

CIRCL
Computer Incident Response Center Luxembourg

Mondragon Unibertsitatea

TELECOM SudParis

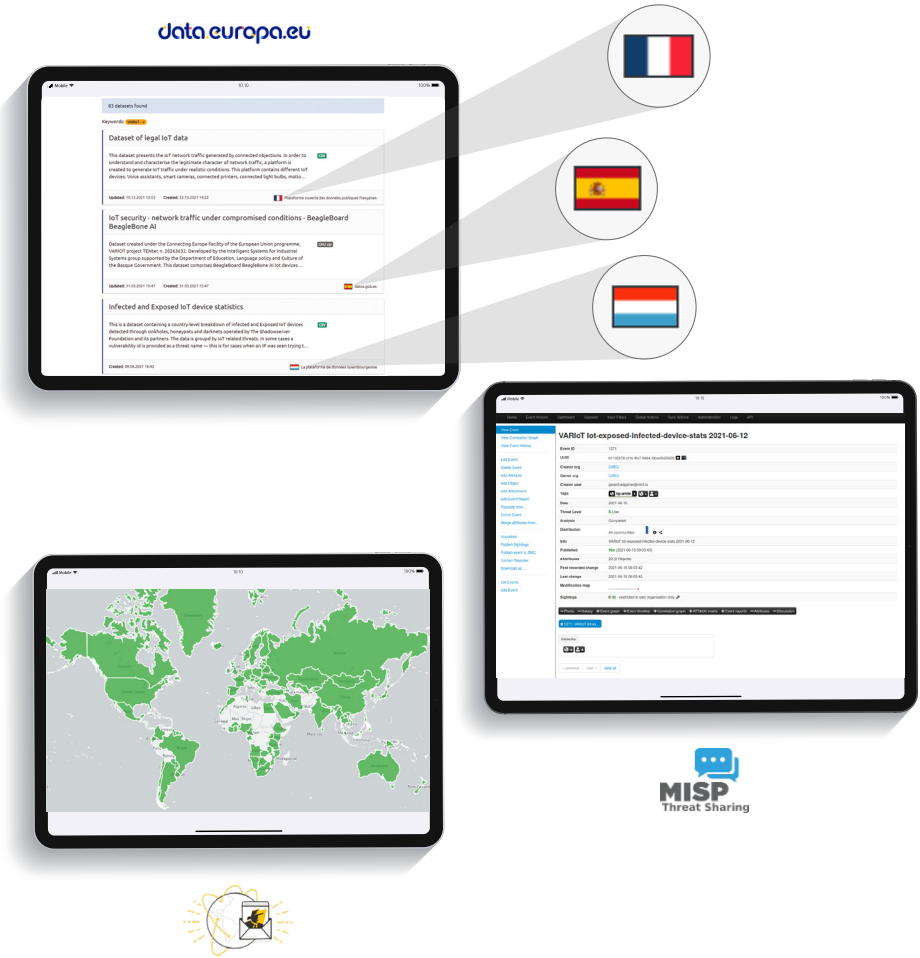
IP PARIS

Project objectives

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

Relevant data is made available through:

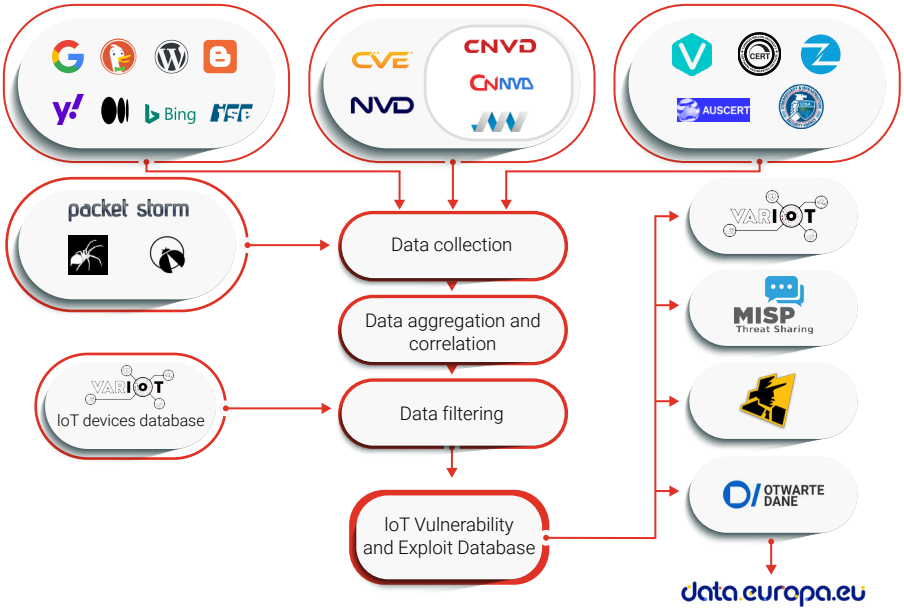
- data.europa.eu
- Malware Information Sharing Platform (MISP)
- Shadowserver's free daily remediation feeds



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 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

Vulnerability database



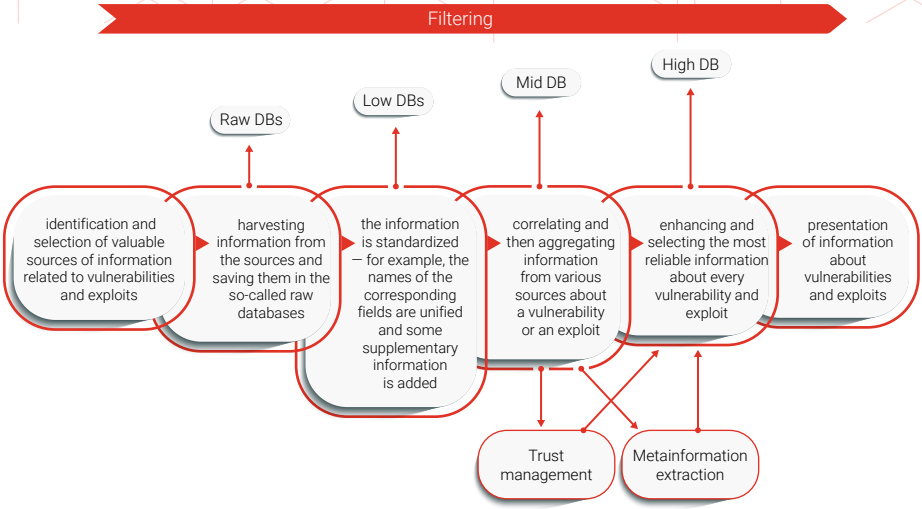
Data is collected from various sources:

- Vulnerability databases (e.g. NVD)
- Advisories from PSIRTs, bug bounty programs or research labs
- Exploit databases (e.g. exploit-db.com)
- Recent posts and articles found over the Internet.

Information from different sources is aggregated into one meta-entry for every specific vulnerability or exploit.

Entries are judged for their relevancy in the IoT field, based on the metadata from the original sources, supplemented with IoT devices database created for this project.

https://www.variot.eu/project-outcomes/sharing-data-with-the-world/



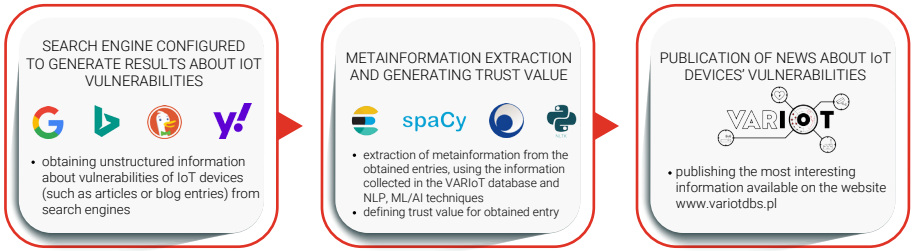
Trust evaluation:

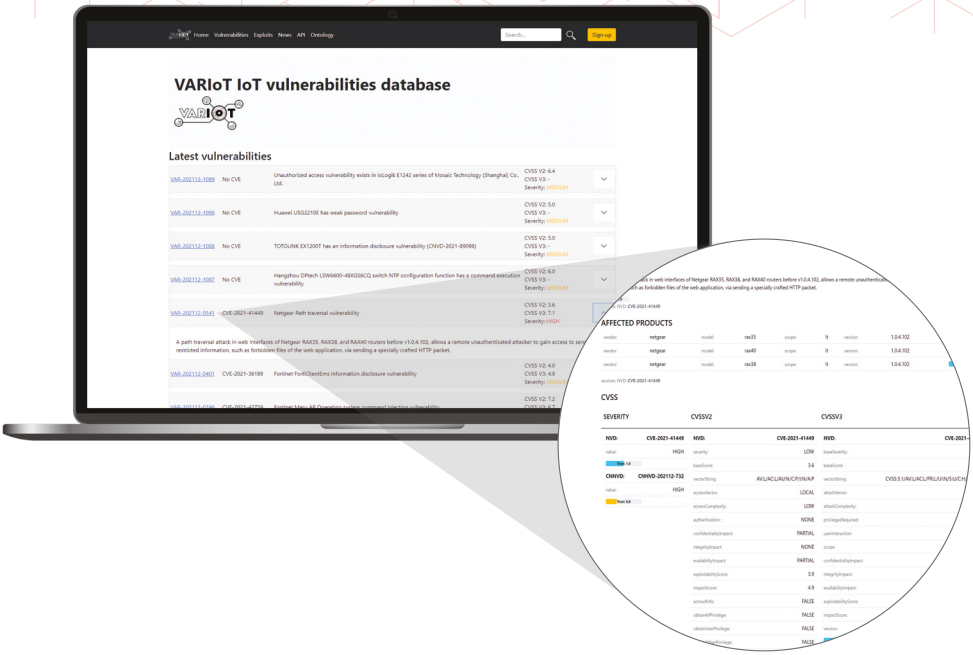
- to select the most reliable and informative piece of information
- to evaluate information reliability
- to identify vulnerabilities and exploits related to IoT

Evaluation based on:

- reputation of source
- convergence of information from various sources
- method of aggregation and classification performed
- additional searches

IoT vulnerability search engine





vulnerabilities – information about IoT vulnerabilities aggregated from many sources

exploits – exploits targeting IoT devices

API – easy access to data in JSON and JSON-LD format

news – news about IoT security crawled using our custom search engine

well structured data

information sources and trust level

www.variotdbs.pl

In VARIoT, active attacks against IoT devices are also observed using fake (emulated) devices – honeypots.

VARIoT primary honeypot network runs 260 nodes with dedicated IP addresses for a total of 821 honeypots operating at once. The nodes are located in 88 countries, 331 unique /24's and 134 unique ASNs. As part of the project Shadowserver developed a new Web/IoT honeypot. In total 8 types of honeypots are run, both proprietary and open source.

New Device ID scan introduced:

- we identify over 22M devices daily
- we use over 1000 signatures
- we detect 119 vendors

(sample results in chart above).

Additionally:

- 5 new IoT-specific Scans and Report types introduced: MQTT, MQTT/TLS, CoAP, IPP, AMQP
- IPv6 scanning based on hitlists: HTTPS (443), HTTP (80), SMTP (25) TELNET (23), SSH (25)
- New SSL scanning ports added
- Automated Malware downloader system developed
- Honeypot Scanner Events Report type was enhanced with IoT specific and exploit information
- New Malware_URL report introduced containing malicious URLs primarily involved in IoT exploitation
- All the above shared daily with 132 National CSIRTs covering 173 countries and territories as well as 6000+ organizations worldwide

For more information:

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

Testbed to generate IoT network traffic: https://variot.telecom-sudparis.eu/

A description of the testbed and data collection method: https://variot.telecom-sudparis.eu/about.php

MISP

Want to use MISP to export a subset to a national open data portal?

https://www.misp-project.org/2020/07/30/publishing-open-data-using-MISP.html

Want to use MISP to share details of IoT firmware or Indicators of Compromise on IoT?

https://www.misp-project.org/objects.html#_iot_firmware

https://www.misp-project.org/objects.html#_iot_device

Want to make your open data sets usable by the infosec community?

https://github.com/CIRCL/open-data-security

And more: SECURITYMADEIN.LU/CIRCL: https://circl.lu/

Open Data Portals: https://www.variot.eu/project-outcomes/open-data/

variot.eu

https://twitter.com/variot_project