CEF VARIOT

VULNERABILITY AND ATTACK REPOSITORY FOR IOT

Authors

Gregory Blanc
IMT/Télécom SudParis
Institut Polytechnique de Paris

Marek Janiszewski
NASK - PIB

Piotr Kijewski
Shadowserver

Partners

NASK

SHADOWSERVER

CIRCL
Computer Incident Response Center Luxembourg

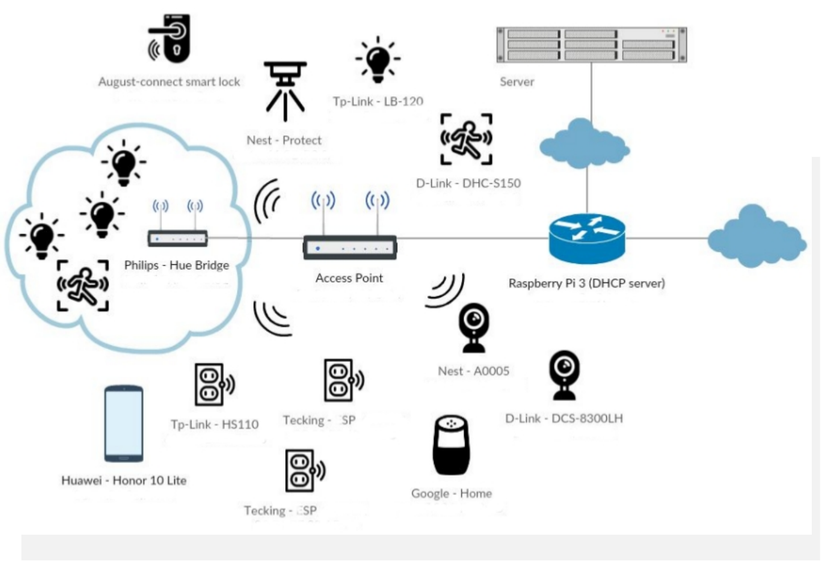
Mondragon Unibertsitatea

Data Sheet

CEF Telecom – Public Open Data
CEF-TC-2018-5
Started: July 1st, 2019
End: June 30th, 2022

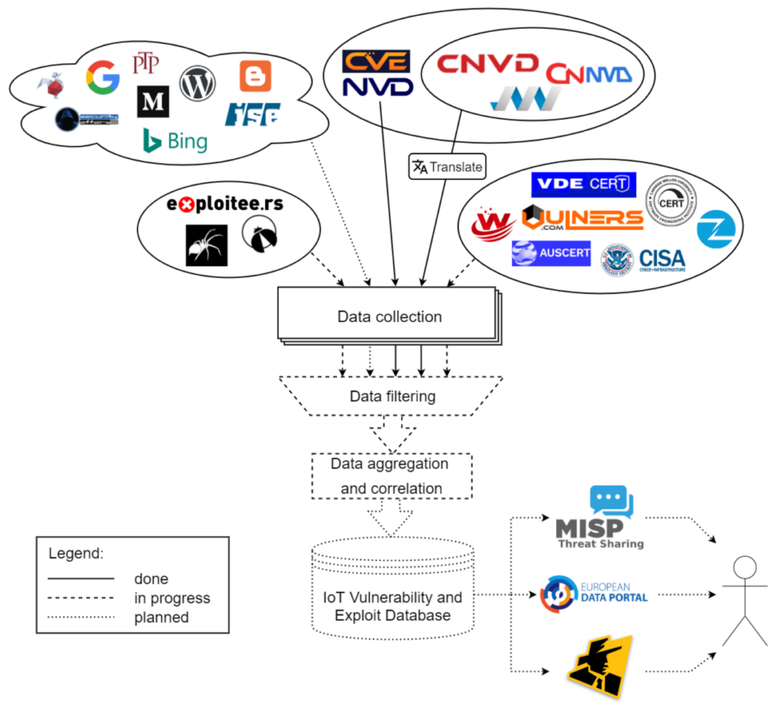
TRAFFIC GENERATION & MODELLING

- Network traffic analysis for IoT device identification: deep-learning-based solution for each device type, enabling anomaly detection
- IoT network traffic generation: setting up a testbed to generate real-life traffic daily
- Generate behavioural models for generalised anomaly detection: leverage previous results to transfer models learned in controlled environments to edge or user premises
- IoT malware analysis: understand compromised IoT behaviour, and generate malicious IoT traffic



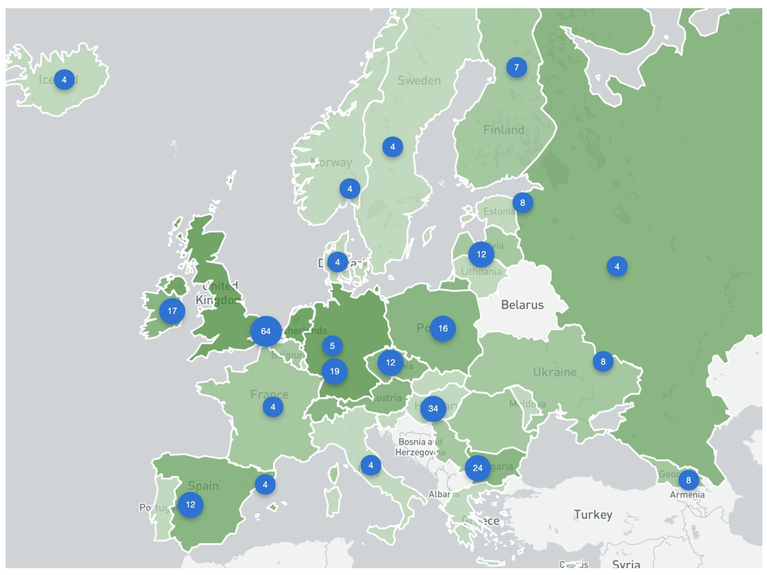
INTERNET-WIDE SCAN OF IOT PROTOCOLS

- Campaigns of Internet-wide (IPv4) scans for IoT-specific protocols: CoAP, MQTT, IPP
- Results shared daily with 114 national CSIRTs and 6000+ network owners worldwide
- Tagging scan results to enable IoT device identification (40M x509 certificates collected each day)
- Rule language developed for tagging: hunders of rules currently being tested
- IoT-oriented honeypot network: 400 honeypots in 49 countries, 68 uniques ASNs, and 202 /24 networks
- Future works include 1) scanning of IPv6 and new protocols; 2) development of a new honypot type suited to observing IoT related exploits and malware



VULNERABILITIES & EXPLOIT DB

- Identification of data sources: vulnerability databases, security advisories, exploits databases, blogs, etc.
- Collection of data from the selected sources: parsing, and eventually translating sources' contents
- Filtering the data concerning IoT: requires device cataloguing to refine collected data
- Data aggregation, correlation and enhancement: creation of a common format to unify all sources; correlation of data for a single entry from different sources
- Publication of the data: European Data Portal, MISP Threat Sharing Platform, Shadowserver's free daily remediation feeds



6ème Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information
décembre 2020

Contact info@variot.eu

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

www.variot.eu