

Update on the SISSDEN project

Paweł Pawliński
pawel.pawlinski@cert.pl



55th TF-CSIRT Meeting

Vilnius, 2018-09-27

Secure Information Sharing Sensor Delivery Event Network



Horizon 2020 Innovation Action (call: H2020-DS-2015-1)

sisssden.eu

@sisssden

Project details

Consortium:

PL NASK (coordinator)
UK CyberDefcon
DE Deutsche Telekom
CH Eclexys
FR Montimage
IT Poste Italiane
NL Shadowserver
DE Universitaet des Saarlandes

Start: May 2016

End: April 2019

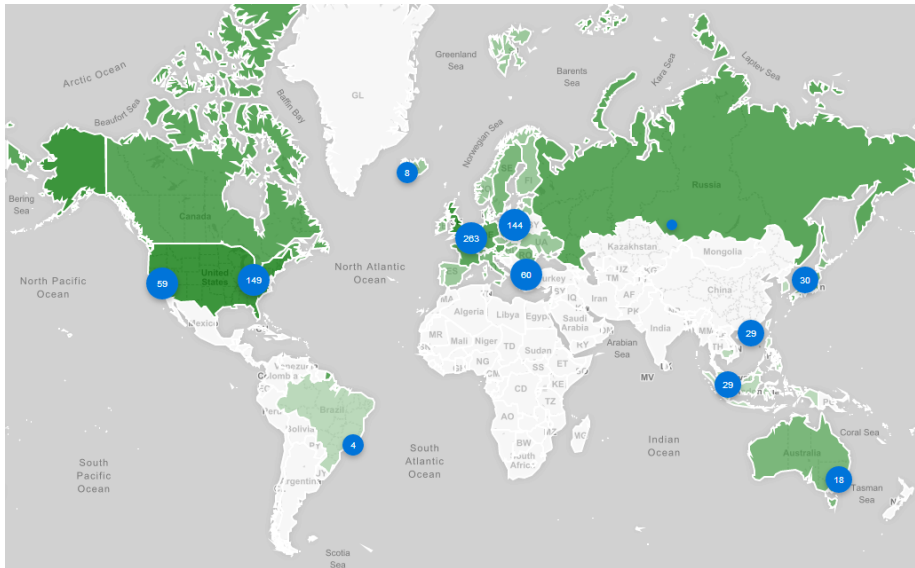
Continuation: 2019+

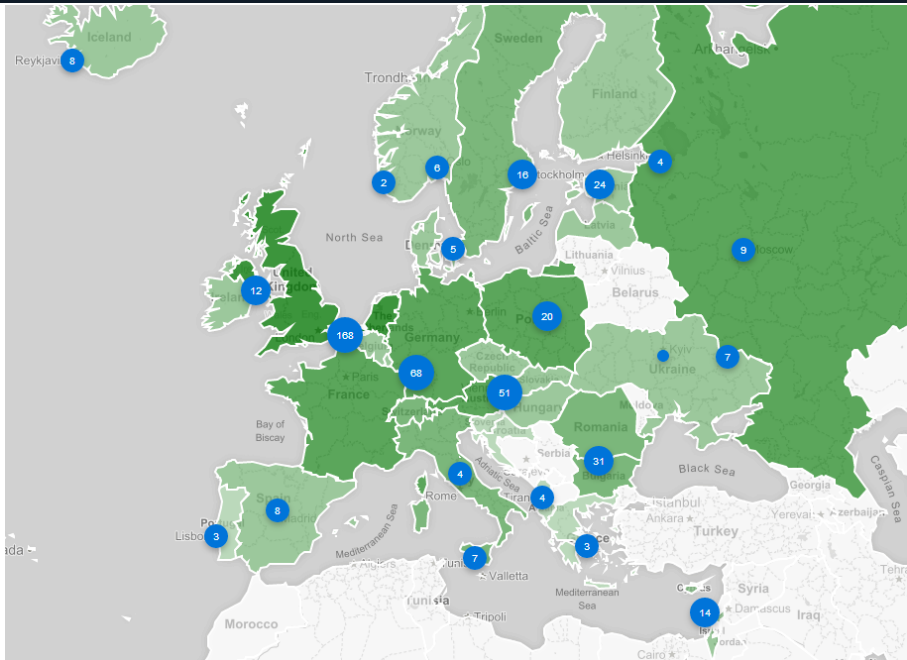
Selected objectives

- Create a **large, distributed honeypot network**
- Long-term **botnet tracking**
- **Free data feeds** for national CERTs, network owners, etc.
- Provide objective situational awareness (threats, remediation, . . .) through **metrics**
- Support for **LEA**
- Publish a large scale **curated data set** for researchers

Honeypot sensor network

- 215 sensors deployed, aiming for over 300
 - EU & worldwide
 - Looking for VPS contributors (contact us)
- Honeypot development
 - 6 types of low-interaction honeypots deployed
 - aiming for 25
 - enhancements sent to upstream projects
- Remediation feeds (notifications)
 - **Brute force attacks:** <https://www.shadowserver.org/wiki/pmwiki.php/Services/Drone-BruteForce>
 - **HTTP-based scanning activity:** <https://www.shadowserver.org/wiki/pmwiki.php/Services/HTTP-Scanners>
 - 2 more coming this month
 - free service for all network owners (sign up!)
 - over 4000 recipients





(Near) future

- Analytical platform:
 - data: 100s TB of logs, PCAPs
 - convenient way to interact with all datasets
 - internally: analyze trends & events
 - public view: metrics dashboard
- Reference curated dataset
 - unique large datasets
 - available for vetted researchers
 - ETA: October 2018
- Interested in cooperation? **Talk to us!**

Thank you for your attention.

This research has been supported by the European Union Horizon 2020 programme under grant agreement No. 700176 (SISSDEN). The opinions expressed in this presentation are those of the authors and do not necessarily reflect the views of the European Commission.