NASK

Adam Kozakiewicz

SISSDEN

Secure Information Sharing Sensor Delivery Event Network

Horizon 2020

Call H2020-DS-2015-1: „Digital Security: Cybersecurity, Privacy and Trust”

Topic DS-04-2015: „Information driven Cyber Security Management”

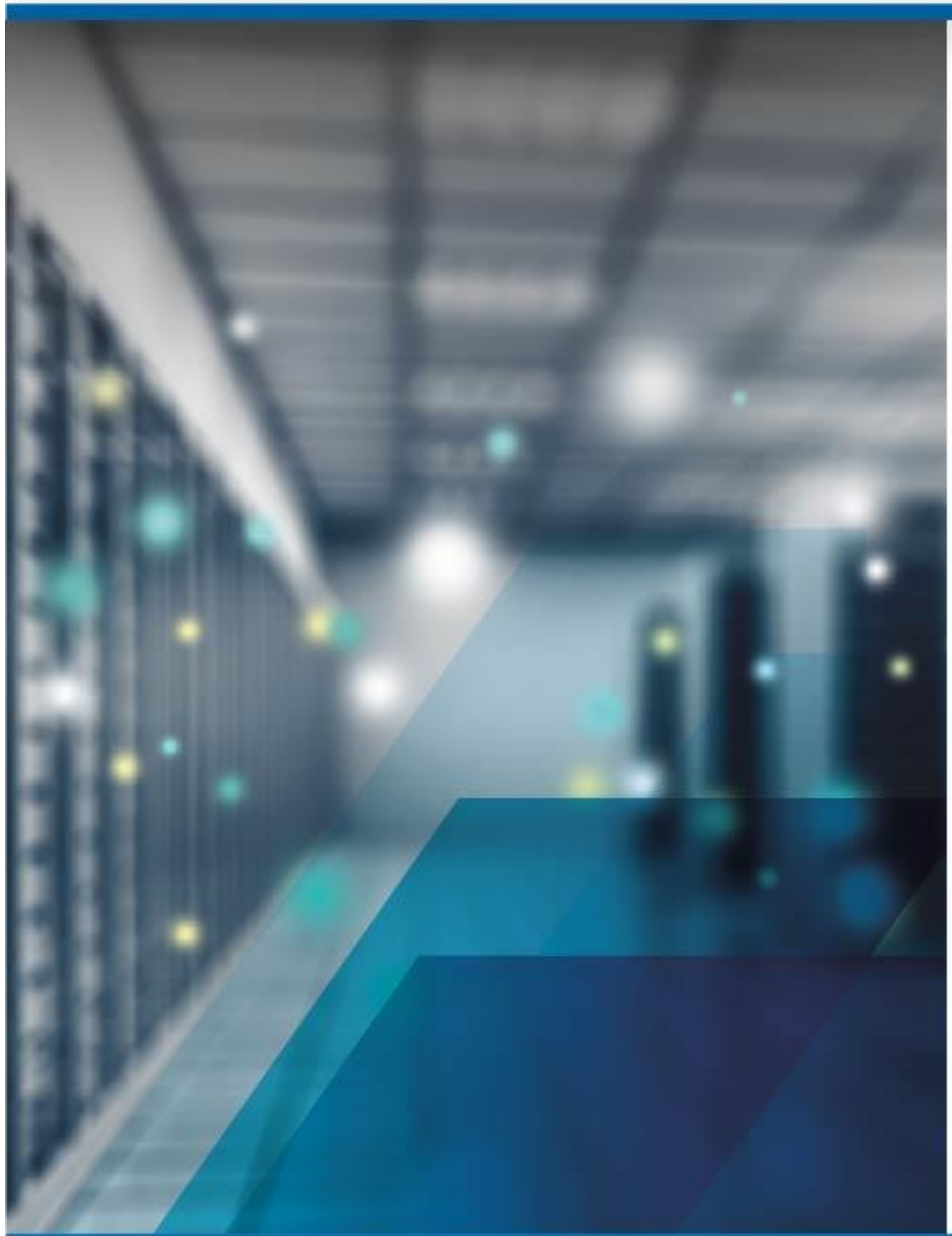
Type: Innovation Action

2016.05.01-2019.04.30

Improving the cybersecurity posture of EU entities and end users through development of situational awareness and sharing of actionable information.

European Commission

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 700176.



NASK-PIB - coordinator

MONTIMAGE EURL (FR)

CYBERDEFCON LIMITED (GB)

UNIVERSITAET DES SAARLANDES (DE)

DEUTCHE TELEKOM AG (DE)

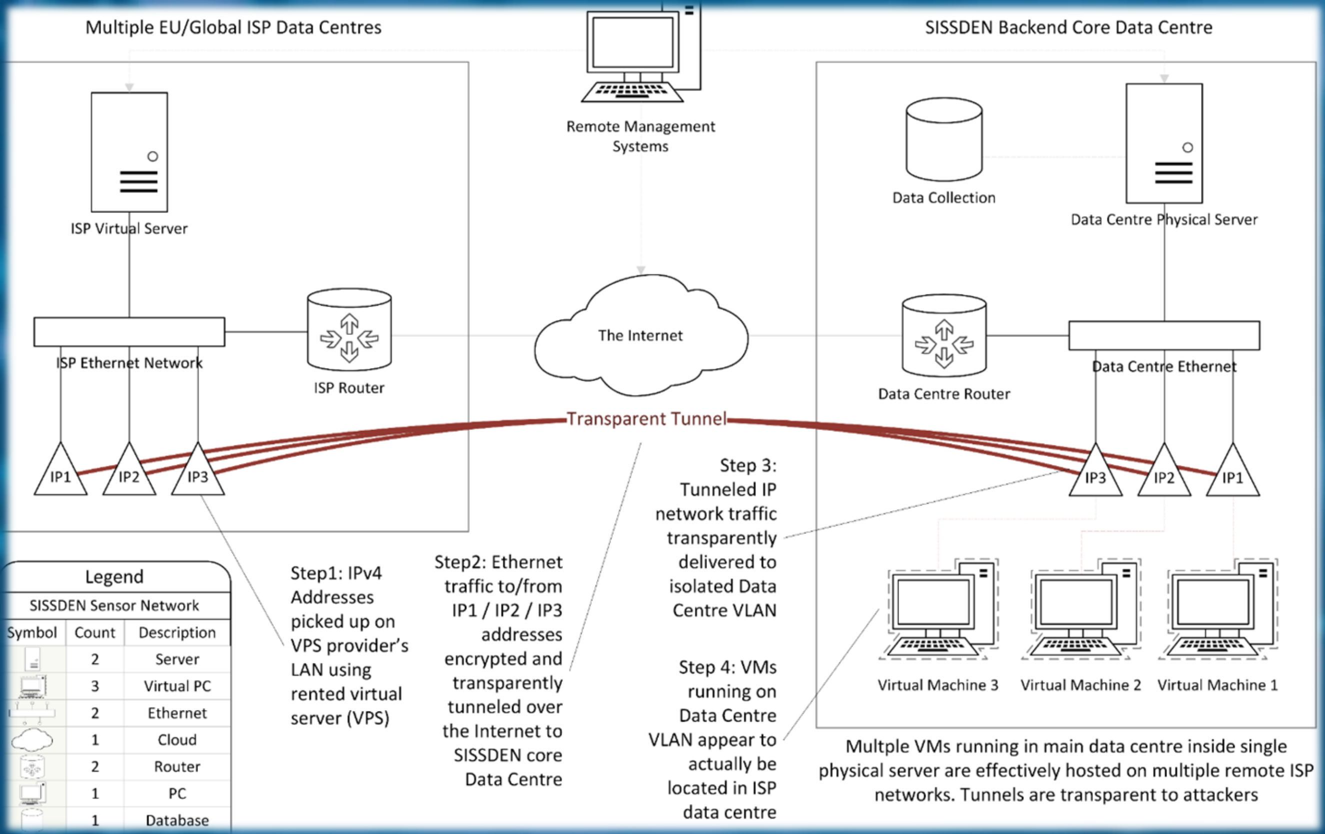
ECLEXYS SAGL (CH)

POSTE ITALIANE – SOCIETA PER AZIONI (IT)

STICHTING THE SHADOWSERVER FOUNDATION EUROPE (NL)

- Create a large, distributed sensor network
  - Over 100 sensors, located in all EU countries
  - Sensors deployed by third parties (at least 20 by the end of the project)
  - Multiple IPs and honeypots for each sensor
- Advancements in attack detection
  - New types of honeypots, darknets, probes
  - IoT, RDDoS, mobile threats
- Advancements in malware analysis and botnet tracking
  - Beyond-state-of-the-art sandbox technologies
  - Long-term sandboxing
- Improving the fight against botnets
  - Detailed long-term studies of botnet infrastructures, support for LEA

- Collect, store, analyse and reliably process Internet scale security data sets
  - Explore „big data” approaches
- Share high quality information on a large scale
  - Free data feeds for national CERTs, network owners, etc.
- Provide objective situational awareness through metrics
  - Overview of threats, effectiveness of remediation
- Create and publish a large scale curated reference data set
  - New resource for security research in Europe



Step1: IPv4 Addresses picked up on VPS provider's LAN using rented virtual server (VPS)

Step2: Ethernet traffic to/from IP1 / IP2 / IP3 addresses encrypted and transparently tunneled over the Internet to SISSDEN core Data Centre

Step 3: Tunneled IP network traffic transparently delivered to isolated Data Centre VLAN

Step 4: VMs running on Data Centre VLAN appear to actually be located in ISP data centre

Multple VMs running in main data centre inside single physical server are effectively hosted on multiple remote ISP networks. Tunnels are transparent to attackers

Legend

SISSDEN Sensor Network

Symbol	Count	Description
	2	Server
	3	Virtual PC
	2	Ethernet
	1	Cloud
	2	Router
	1	PC
	1	Database

European perspective

- Full compliance with EU data protection requirements
  - Note – this is not at all easy, and GDPR is coming!
- Wide coverage of the EU network
  - All EU member & candidate countries included
- Simple cooperation with European entities
- Support for future EU security research and innovation
  - Large-scale, publicly available curated data set based on EU sensors

Not just promises!

- Fully operational system
  - The entire core of the system is TRL9
  - Novel analyses will be TRL7 prototypes.
- Post-project sustainability explicitly considered

CORE 1 – data collection and reporting (TRL9)

- Initial launch – May 2017
  - Using temporary hardware and 10 sensors
- Target platform – October 2017
  - Target backend with much greater power
  - Sensors added constantly
    - 44 sensors at the moment
    - 100 sensors to be reached this year
    - ~400 sensors expected in the final year of the project
- Already fully functioning
- To be officially opened for users in May 2018
- Additional detection capability and situational awareness services still in development
  - E.g. metrics dashboard, new honeypots, etc.

CORE 2 – analytical platform (TRL7)

- In development (first report due in October 2017)
- Several analytical subsystems already working
- First integrated version expected in 2018

Other – Curated Reference Dataset

- Uses data from the CORE-1 platform, so still future work
- To be accessible to vetted researchers in 2018
- Several different datasets, some anonymized, some not

Open to community collaboration

- Sign up in advance:

  https://sissden.eu

- Deploy sensors, provide IP space, VMs, physical servers
- Contribute new honeypot/sensor technologies
- Third party feeds welcome
  - integrate and help enrich curated data
- Academics willing to do research on the curated data set welcome
- Open to collaboration with LE initiatives with data on malware and botnet activity
  - existing example – Cuing.org