ACDC
the Advanced Cyber Defence Centre

Joining forces to fight botnets

Dan Tofan
Head of the Technical Division
CERT-RO
17/02/2014

Agenda

- Who are we?
- Benefits and collaboration opportunities

ACDC

- European funded pilot project - 16 mil. €
- Selected under the CIP programme
- Operating from 01/02/2013 → 31/07/2015

cip competitiveness and innovation framework programme 2007–2013

Joining forces to fight botnets

ACDC
the Advanced Cyber Defence Centre

The ACDC project partners

- Atos
- BARCELONA DIGITAL
- Bulgarian Posts
- Cassidian Cybersecurity
- Croatian Academic and Research Network - CARNet
- CyberDefcon
- DE-CIX
- DFN-CERT
- eco – Association of the German Internet Industry
- Engineering Ingegneria Informatica
- FCCN - Foundation for National Scientific Computing
- Fraunhofer FKIE
- G Data Software AG
- Institute for Internet Security - if(is)

- Inteco
- ISCOM – Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione
- KU Leuven - B-CCENTRE (Belgian Cybercrime Centre of Excellence for Training, Research and Education)
- LSEC - Leaders in Security
- Microsoft EMEA
- Montimage
- CERT-RO
- SignalSpam
- TECHNIKON Forschungsgesellschaft mbH
- Telecom Italia
- Telefónica I+D
- TU Delft
- University of Luxemburg
- XLAB

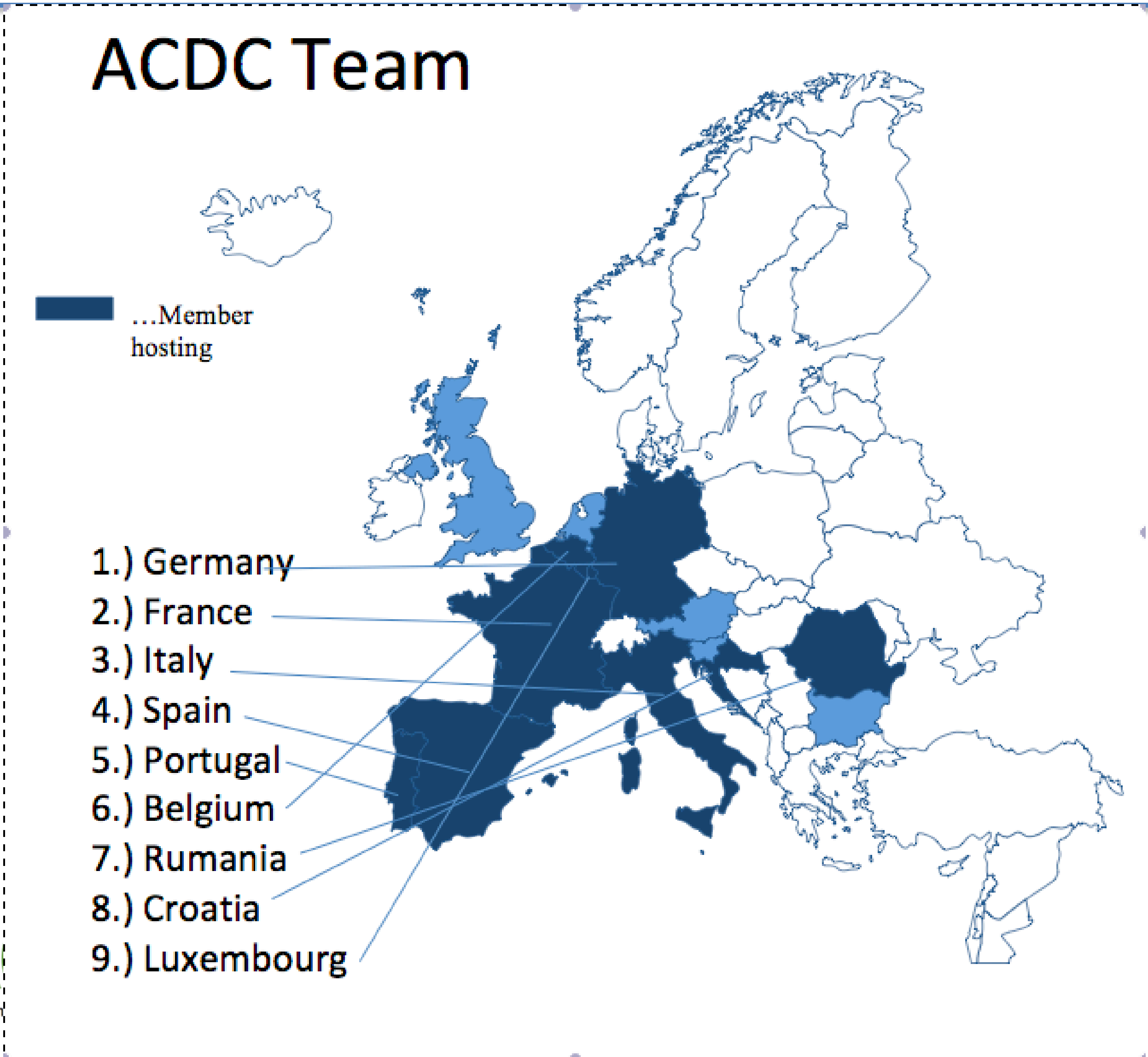
28 partners

14 Member States

Austria
Belgium (NSC)
Bulgaria
Croatia (NSC)
France (NSC)
Germany (NSC)
Italy (NSC)
Luxembourg
Portugal (NSC)
Romania (NSC)
Slovenia
Spain (NSC)
The Netherlands
United Kingdom

the Advanced Cyber Defence Centre

ACDC Partners



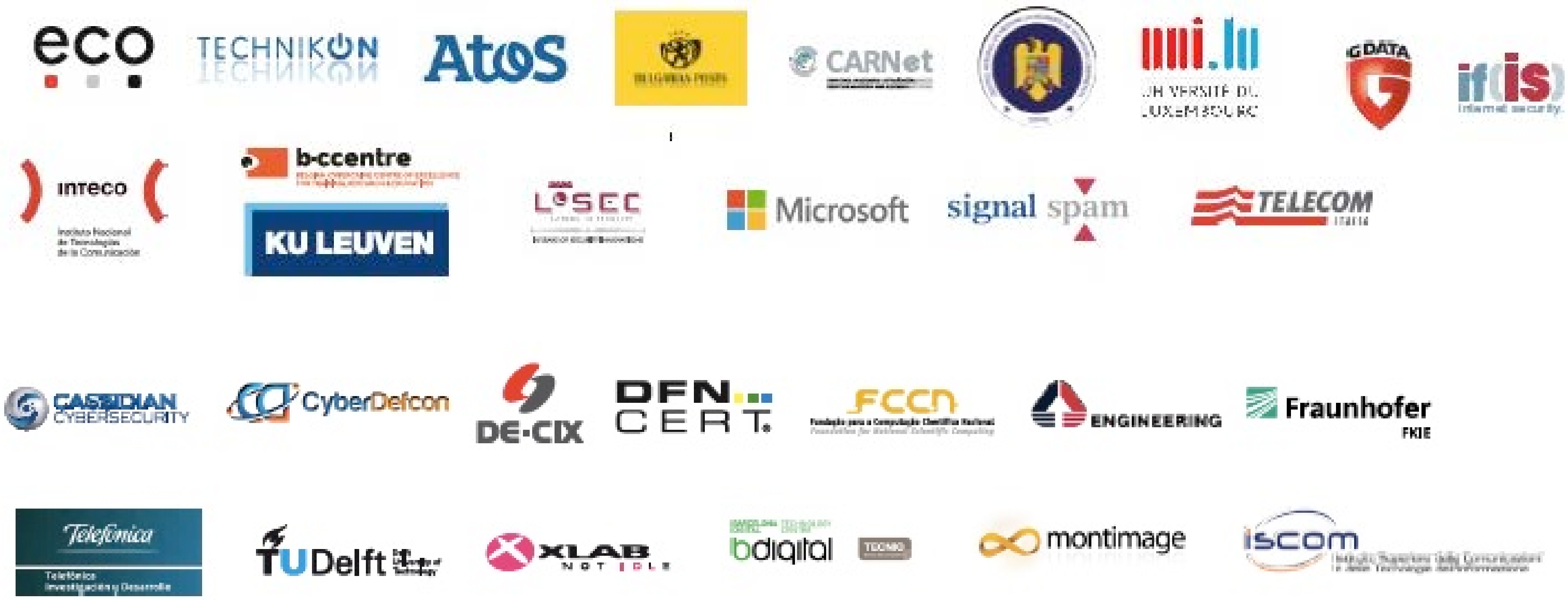
ACDC Team

🟦 …Member hosting

1.) Germany
2.) France
3.) Italy
4.) Spain
5.) Portugal
6.) Belgium
7.) Rumania
8.) Croatia
9.) Luxembourg

ACDC Partners

Providing security tools and services used to identify and fight botnets



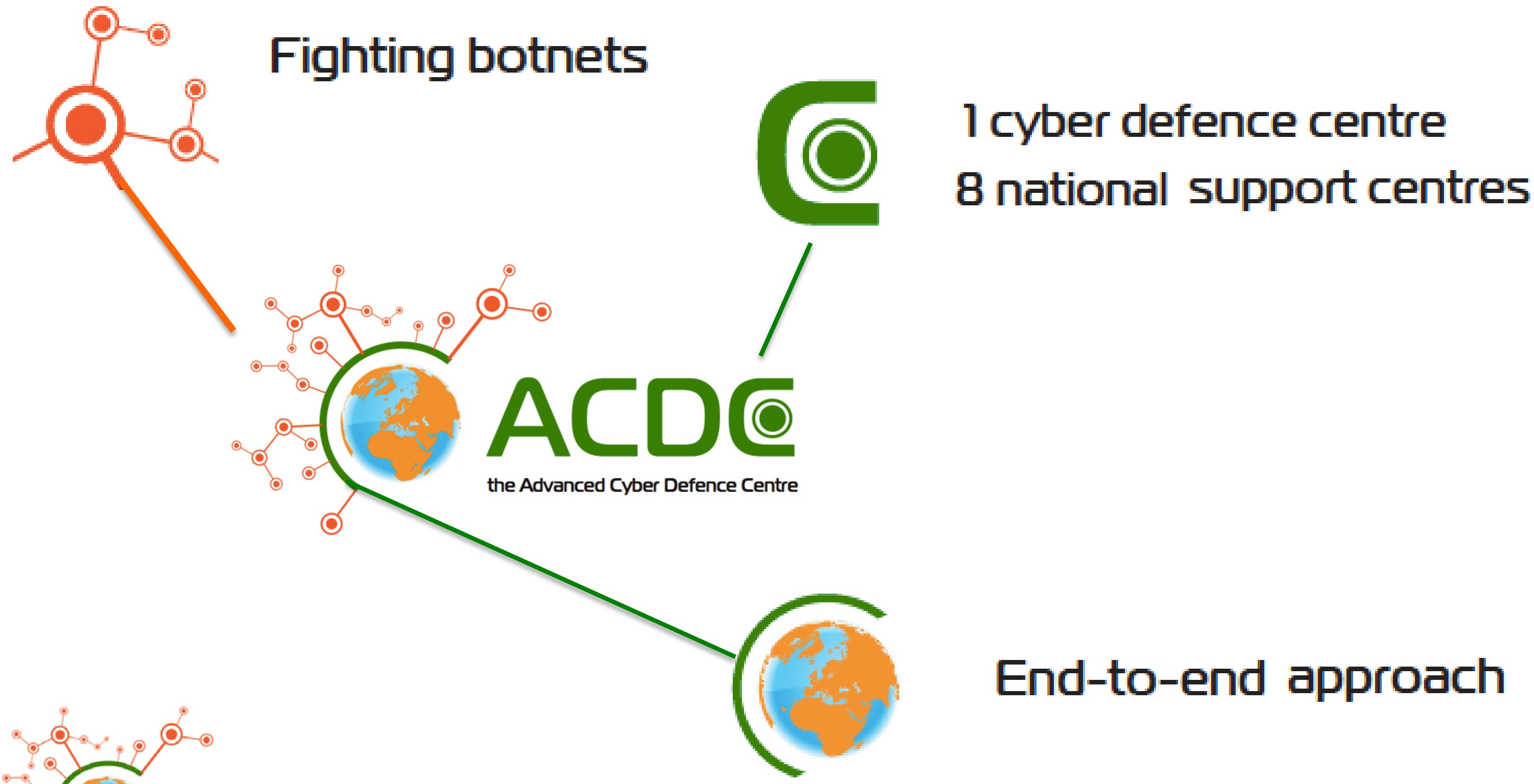
ACDC

Improve the early detection of botnets
Support their mitigation

- foster an extensive **sharing of information** across Member States
- create a **European source of data sets** stored in an ACDC data clearing house
- provide a complete **set of solutions** accessible online for mitigating on-going attacks
- use the **pool of knowledge** to create best practices that support organisations in raising their cyber-protection level
- create a **European wide network** of cyber defence centres

ACDC
the Advanced Cyber Defence Centre

The 3 pillars of ACDC



Fighting botnets

1 cyber defence centre

8 national support centres

End-to-end approach

ACDC

the Advanced Cyber Defence Centre

ACDC – 3 pillars

Detection

Fighting botnets

- ACDC central data clearing house
- Acquire data from ISPs and other providers
- Make data available to
  - support earlier detection of botnets
  - enable research & innovation

ACDC – 3 pillars

End-to-end approach

Detection

Mitigation

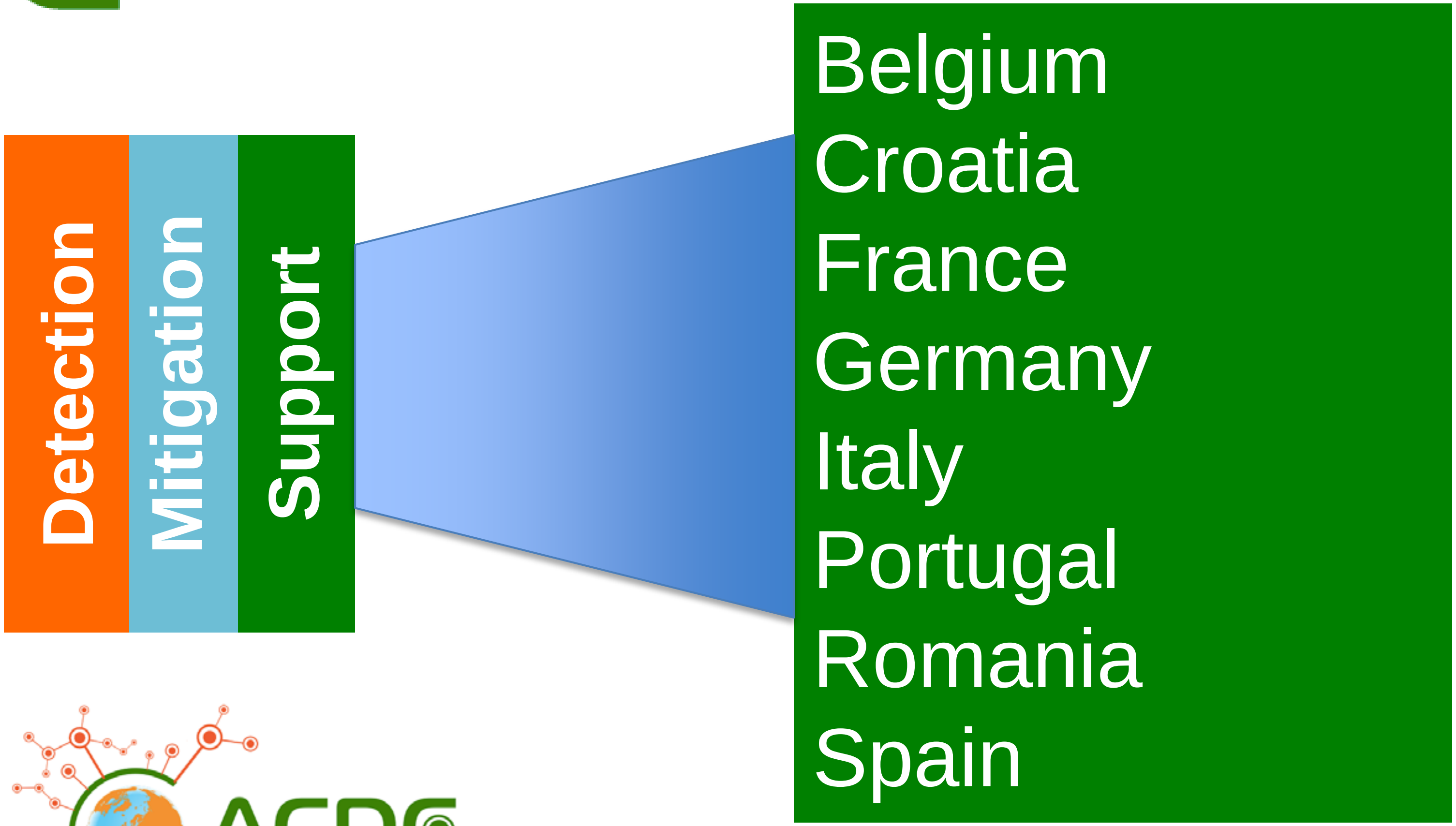
- Deliver improved solutions to mitigate botnets across networks, web sites, computers, mobile devices
- Sources from the 28 ACDC partners
- Open to solutions from other sources

ACDC
the Advanced Cyber Defence Centre

ACDC – 3 pillars

1 cyber defence centre

8 national support centres



Detection

Mitigation

Support

Belgium
Croatia
France
Germany
Italy
Portugal
Romania
Spain

ACDC

the Advanced Cyber Defence Centre

How are we building this?

Delivering tool groups

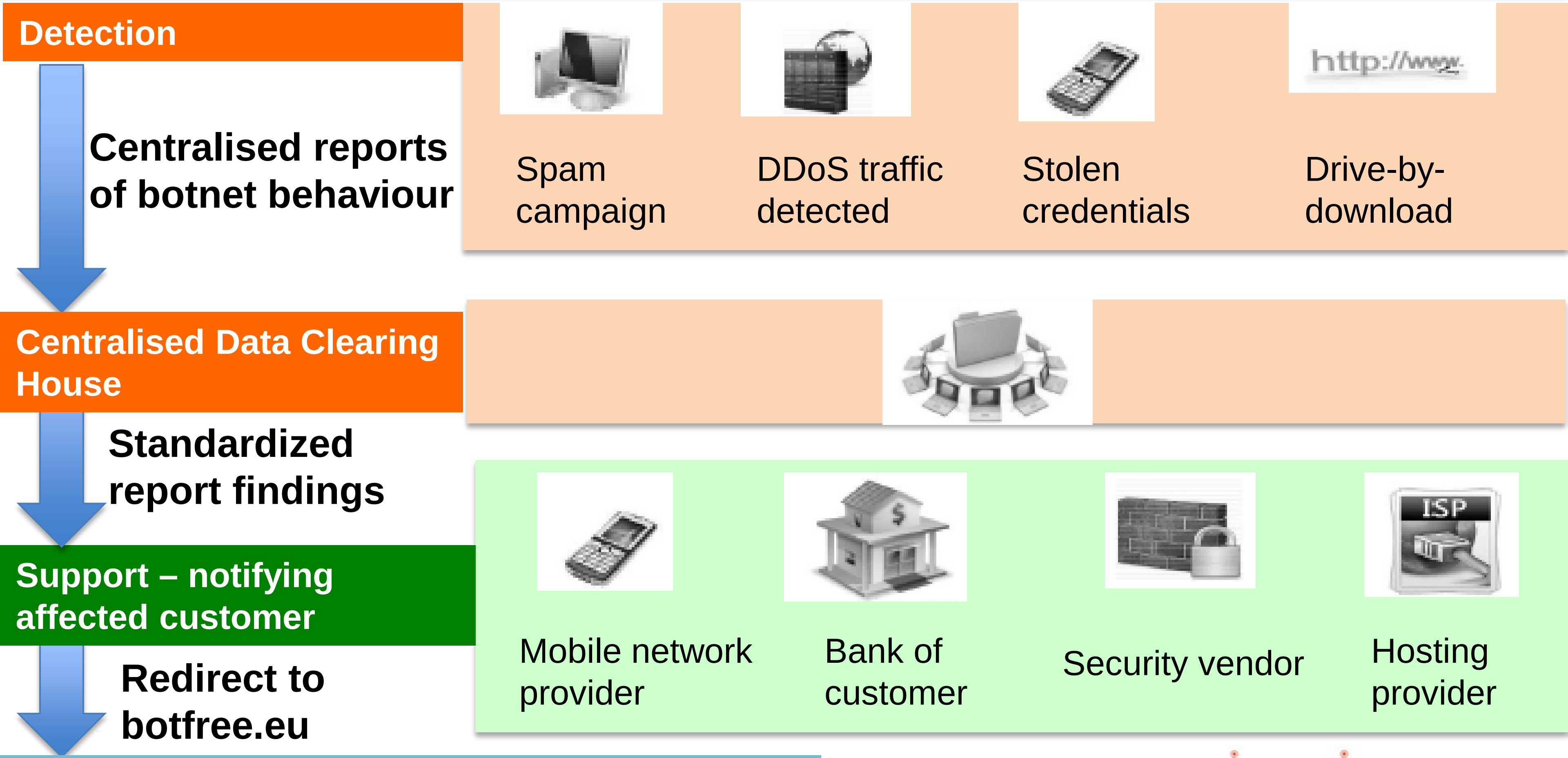
Running experiments

Creating the central data clearing house

Expanding beyond the ACDC partners

ACDC
the Advanced Cyber Defence Centre

ACDC – a service approach



Detection

Centralised reports of botnet behaviour

Spam campaign

DDoS traffic detected

Stolen credentials

Drive-by-download

Centralised Data Clearing House

Standardized report findings

Support – notifying affected customer

Mobile network provider

Bank of customer

Security vendor

Hosting provider

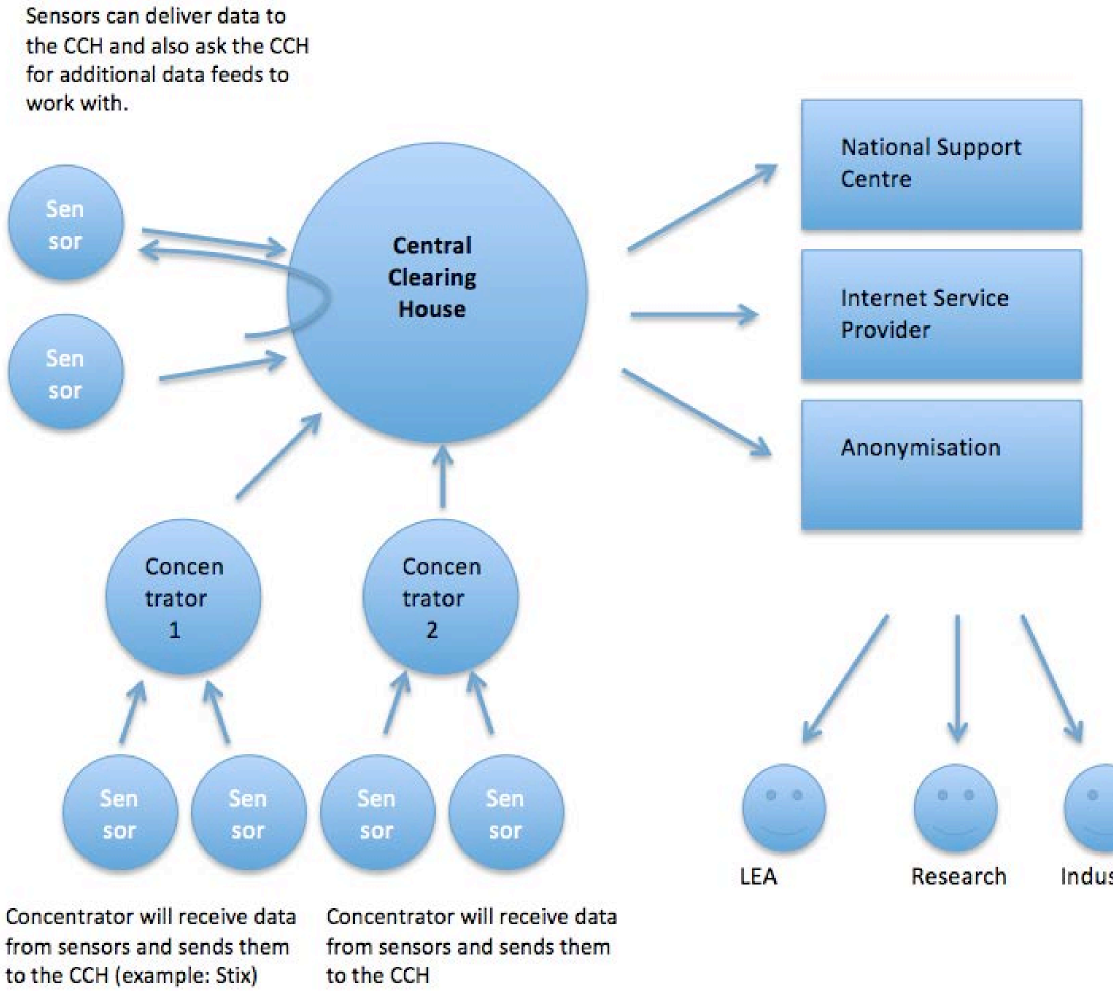
Redirect to botfree.eu

Mitigation – helping affected customer

ACDC
the Advanced Cyber Defence Centre

ACDC – central data clearing house

- ✓ Data input in any format
- ✓ Data output in JSON or YAML
- ✓ Central Clearing House facility correlates data
- ✓ Data flagging for special purposes
  - □ Experiments,
  - □ Research or
  - □ Investigations



Sensors can deliver data to the CCH and also ask the CCH for additional data feeds to work with.

Concentrator will receive data from sensors and sends them to the CCH (example: Stix)

Concentrator will receive data from sensors and sends them to the CCH

ACDC – Tools & experiments
Example - Protecting mobile users

XLAB **CARNet** **LSEC**

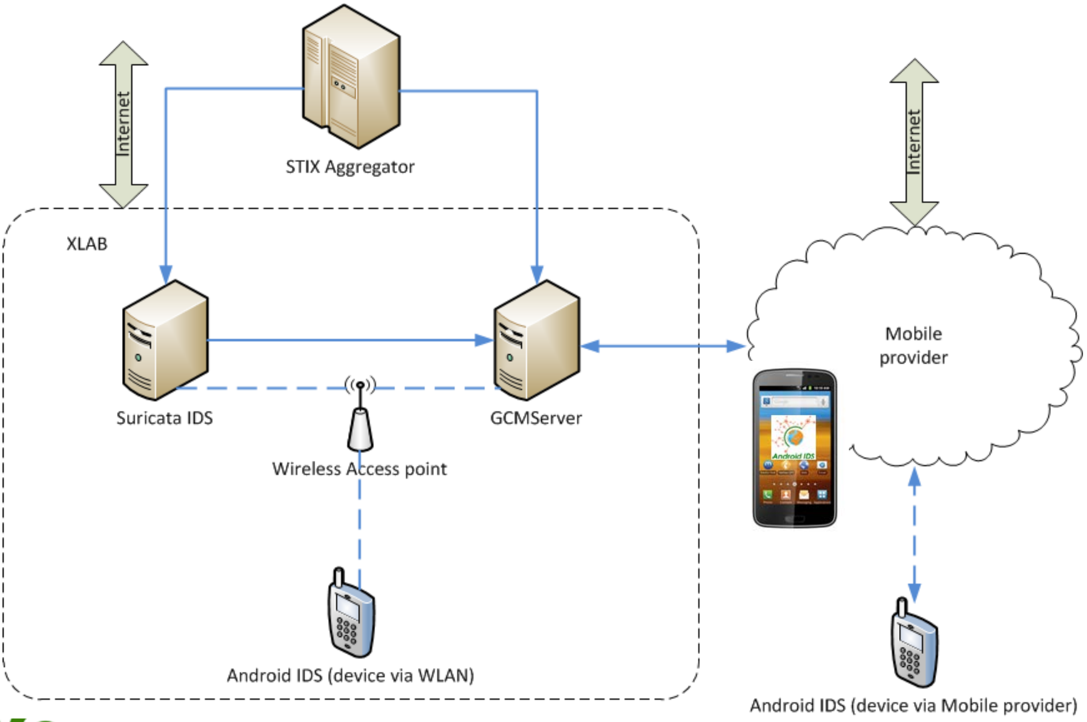
Creating a new solution by combining tools from different partners

ACDC
the Advanced Cyber Defence Centre

ACDC Partner Tool

Mobile device protection

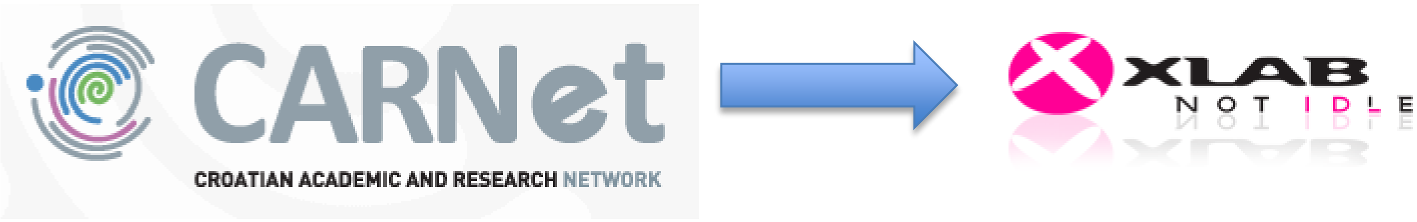
- ✓ Intrusion Detection System for Android smart phones



the Advanced Cyber Defence Centre

ACDC – linking tools to deliver enhanced protection

ACDC EXPERIMENT



- ✓ Linking tools
- ✓ Goal: use CARNet botnet intelligence to enhance the XLAB IDS solution

ACDC Partner Service

LSEC
LEADERS IN SECURITY

Using open format to link tools

- ✓ aggregate data from partner tools
- ✓ provided in the Mitre STIX XML format
- ✓ Connect to ACDC clearing house

STIX™ Structured Threat Information eXpression

A Structured Language for Cyber Threat Intelligence Information

ACDC
the Advanced Cyber Defence Centre

cip competitiveness and innovation framework programme 2007-2013

ACDC – Tools & experiments
Example - Protecting mobile users

XLAB **CARNet** **LSEC**

Creating a new solution by combining tools from different partners

- ✓ User protected from accessing rogue URL
- ✓ Real-time checking

Expanding beyond the ACDC partners

- ACDC Community
- Open to all
- Different involvement possibilities
- Supported by an online community portal (06/2014)

ACDC
the Advanced Cyber Defence Centre

ACDC wants you

Participate to

the EU-wide **sharing** of data

to **fight** botnets

together

ACDC

the Advanced Cyber Defence Centre

Collaboration opportunities

- **Access new solutions** as they are delivered
- **Earlier detection** of emerging bots by trends from the data clearing house
- **Create an ACDC support** centre, increase services delivered to your users
- **Bring a new tool** into an experiment
- **Share expertise** with a wider community

ACDC
the Advanced Cyber Defence Centre

Collaboration – new support centres

National support centres

– Support necessary from many levels in a country

– Adding ACDC services to existing organisations

TODAY

– Centre set up in Germany

– Centres opening in Spain, Italy

– Putting in place the mechanism to for new centres beyond the initial ones

– Mechanism available by June 2014

Collaboration – share data

- Data gathered from public and industry
- Data is analysed
- Patterns, hosters, C&C, perpetrators
- Data is shared, with
  - Internet industry
  - Academia
  - CERTs
  - Law enforcement

TODAY

✓ Data clearing house set up
✓ Initial data sets in (ACDC partners)
✓ Access available to external partners in June 2014

ACDC
the Advanced Cyber Defence Centre

Collaboration – become part of the ACDC community

- Participate
- Receive data analysis results
- Discuss outcome
- Deliver output
- Cooperate on the experiments
- Align support to governmental needs

ACDC

the Advanced Cyber Defence Centre

How do you join?

- Sign a Letter of Interest to join the ACDC
- To date, 18 signed Letters of Interest
  - Governmental level, CERTs
  - Telco, tool providers, research
- Joining can be through the ACDC consultative board, through one or more activities, as data provider etc.

ACDC
the Advanced Cyber Defence Centre

ACDC – letters of interest
CERTs & Governmental level

EUROPOL

CIRT
MONTENEGRO
Computer
Incident
Response
Team

Authority for
Consumers & Markets

Posteitaliane

CSIRT.SK
www.csirt.gov.sk

Centrale d'enregistrement et d'analyse pour la sûreté de l'information
MELANI

National Coordinator for Security and Counterterrorism
Ministry of Security and Justice

ZSIS

ACDC
the Advanced Cyber Defence Centre

ACDC – letters of interest
Tools, ISPs, Research, Associations

ugr Universidad de Granada

HPI Hasso Plattner Institut

T Hrvatski Telekom

Avira

dhpa Dutch Hosting Provider Association

cyscon

MACCSA

abuse information exchange

F-Secure.

TREND MICRO

nsn

ACDC
the Advanced Cyber Defence Centre

ACDC – join us

2013

Set up ACDC central data clearing house
Define groups of tools towards new solutions
Create community structure

2014

Today - sign Letter of Interest
April - timeline of experiments
June - opening of community portal
- add ACDC support centres

2015

8 support centres deployed
Analysis tools added to ACDC data clearing house
Tool groups available through ACDC infrastructure

The ACDC Community

Get involved!

The ACDC outreach team

Peter Meyer – peter.meyer@eco.de

Wout de Natris – denatrisconsult@hotmail.nl

Véronique Pevtschin – veronique.pevtschin@eng.it

Kazim Hussain karim.hussain@atosresearch.eu

ACDC

the Advanced Cyber Defence Centre