Joining forces to fight botnets

Catalin Patrascu
Head of Information Security
and Monitoring Department
CERT-RO
14-15/04/2014

Agenda

- Who are we?
- The 3 pillars of the project
- How are we building this?
- Standing of the Project at Bulgarian Posts PLC
- Benefits and collaboration opportunities

ACDC
the Advanced Cyber Defence Centre

ACDC

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

Joining forces to fight botnets

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 R-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 Luxembourg
- XLAB

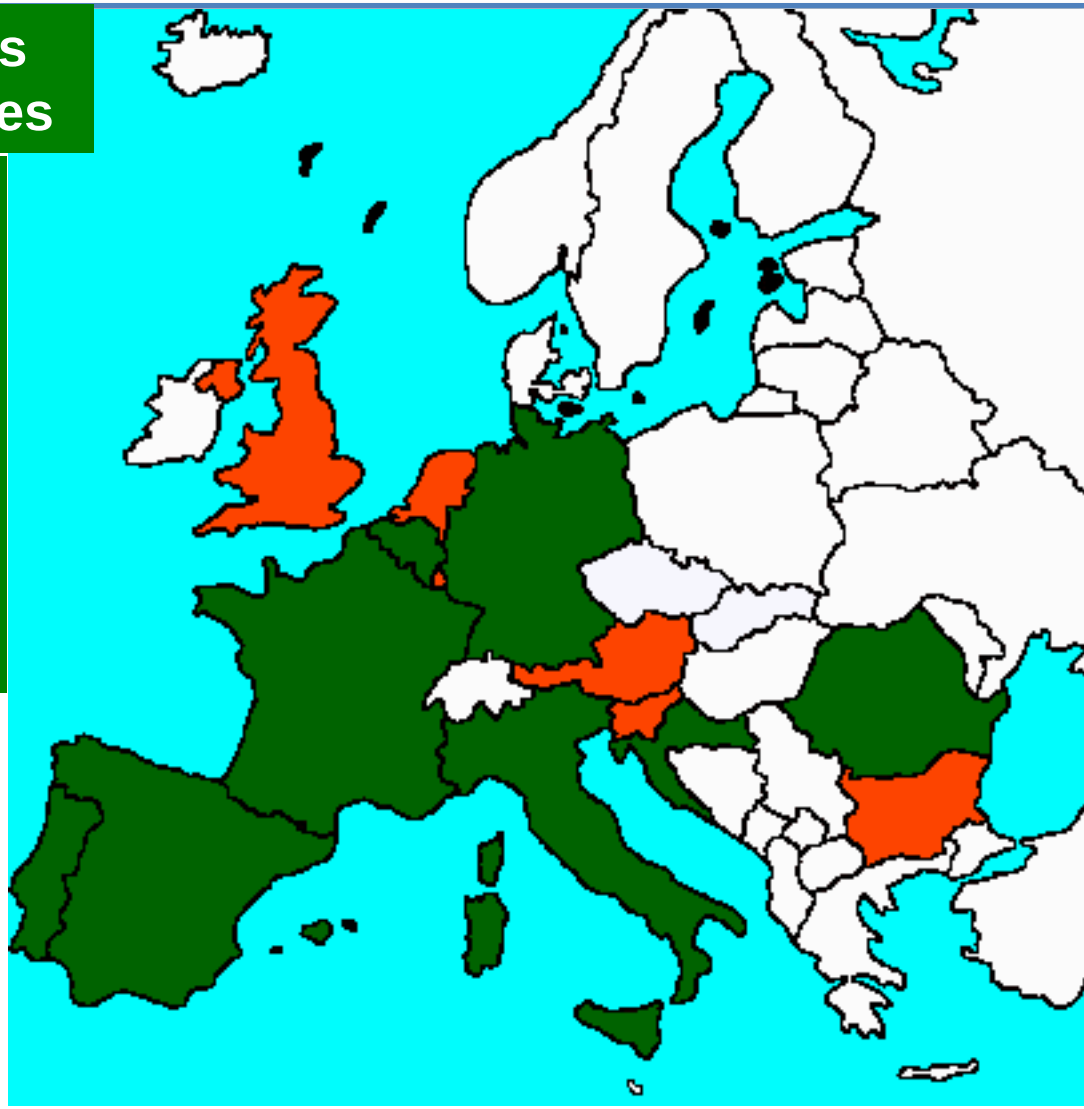
28 partners
14 Member States

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

ACDC
the Advanced Cyber Defence Centre

ACDC across Europe

ACDC partners	ACDC partners Support centres
Austria	Belgium
Bulgaria	Croatia
Luxembourg	France
Slovenia	Germany
The Netherlands	Italy
United Kingdom	Portugal
	Romania
	Spain



ACDC
the Advanced Cyber Defence Centre

ACDC Partners

Providing security tools and services used to identify and fight botnets

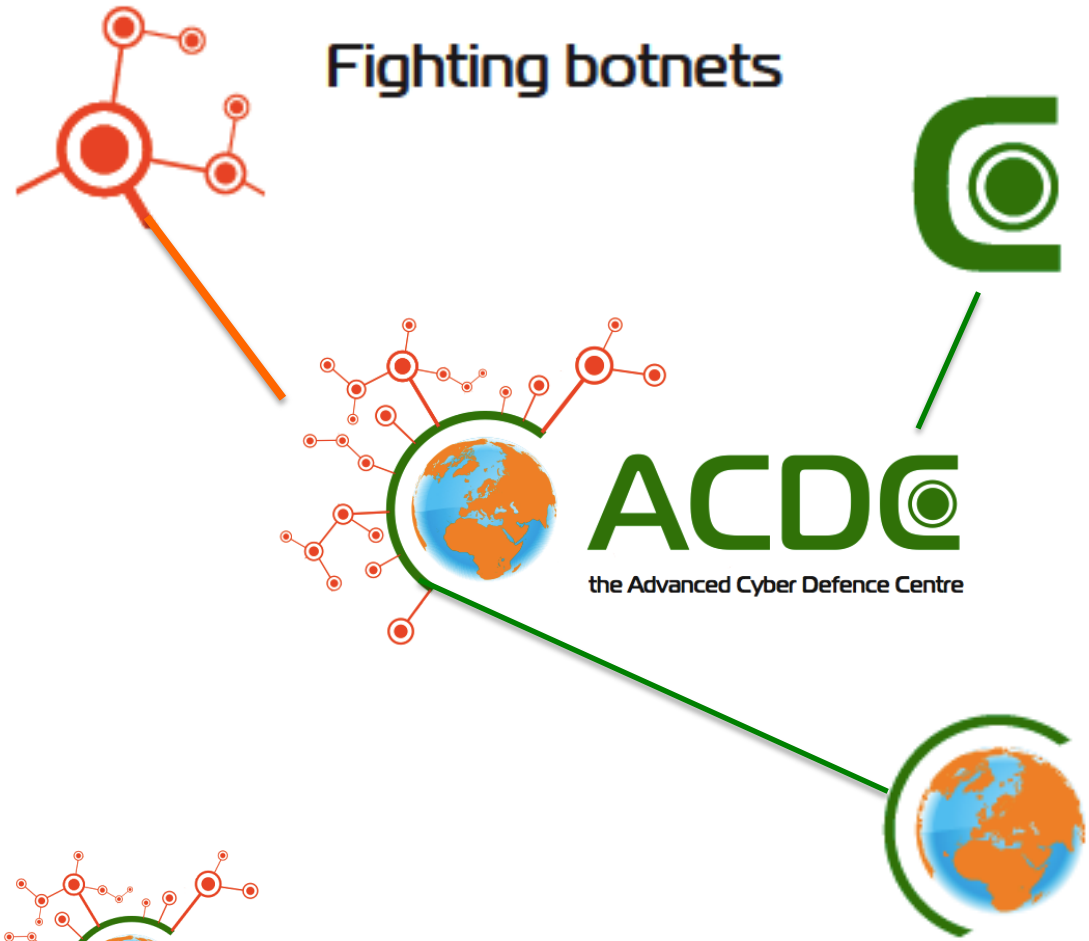
ACDC

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



1 cyber defence centre

8 national support centres

End-to-end approach

ACDC – 3 pillars

Fighting botnets

Detection

- 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
the Advanced Cyber Defence Centre

ACDC – 3 pillars

End-to-end approach

Detection

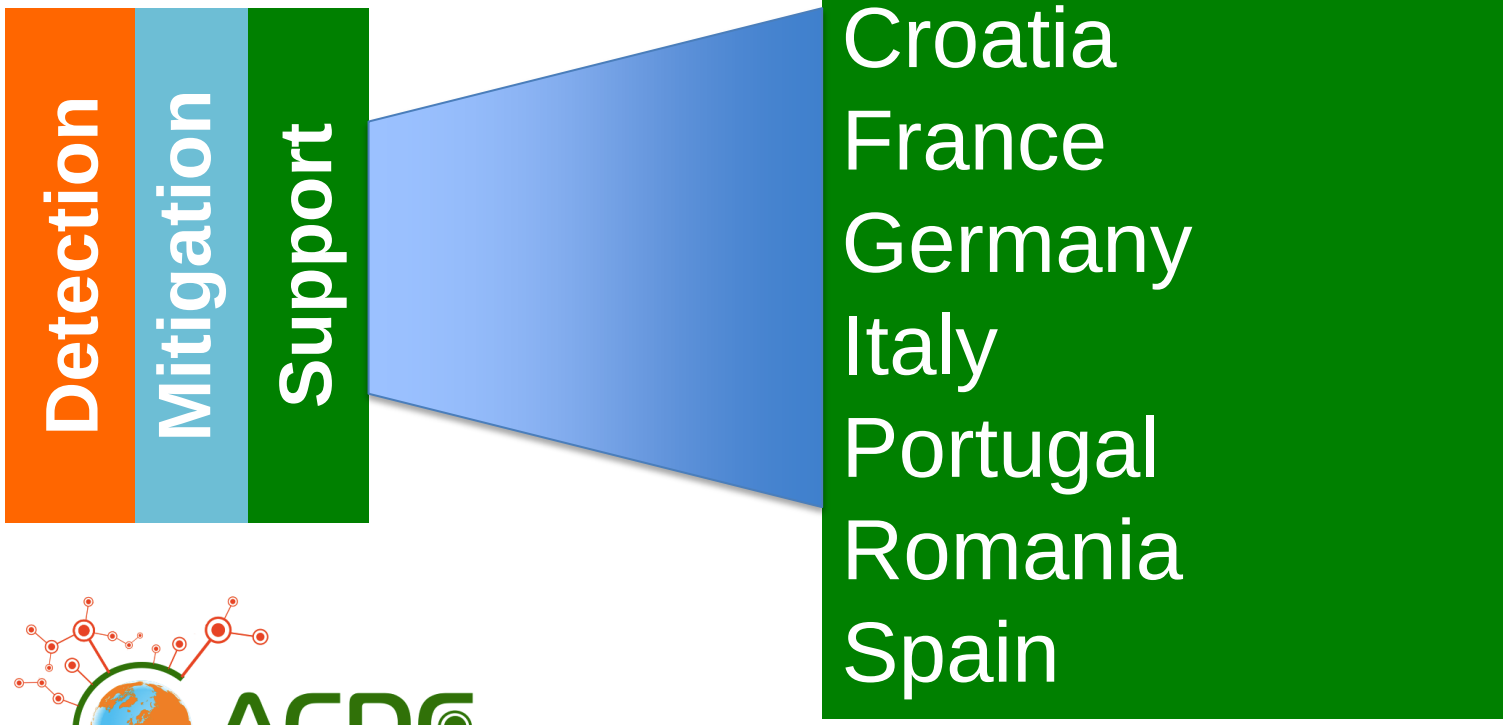
Mitigation

- 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



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

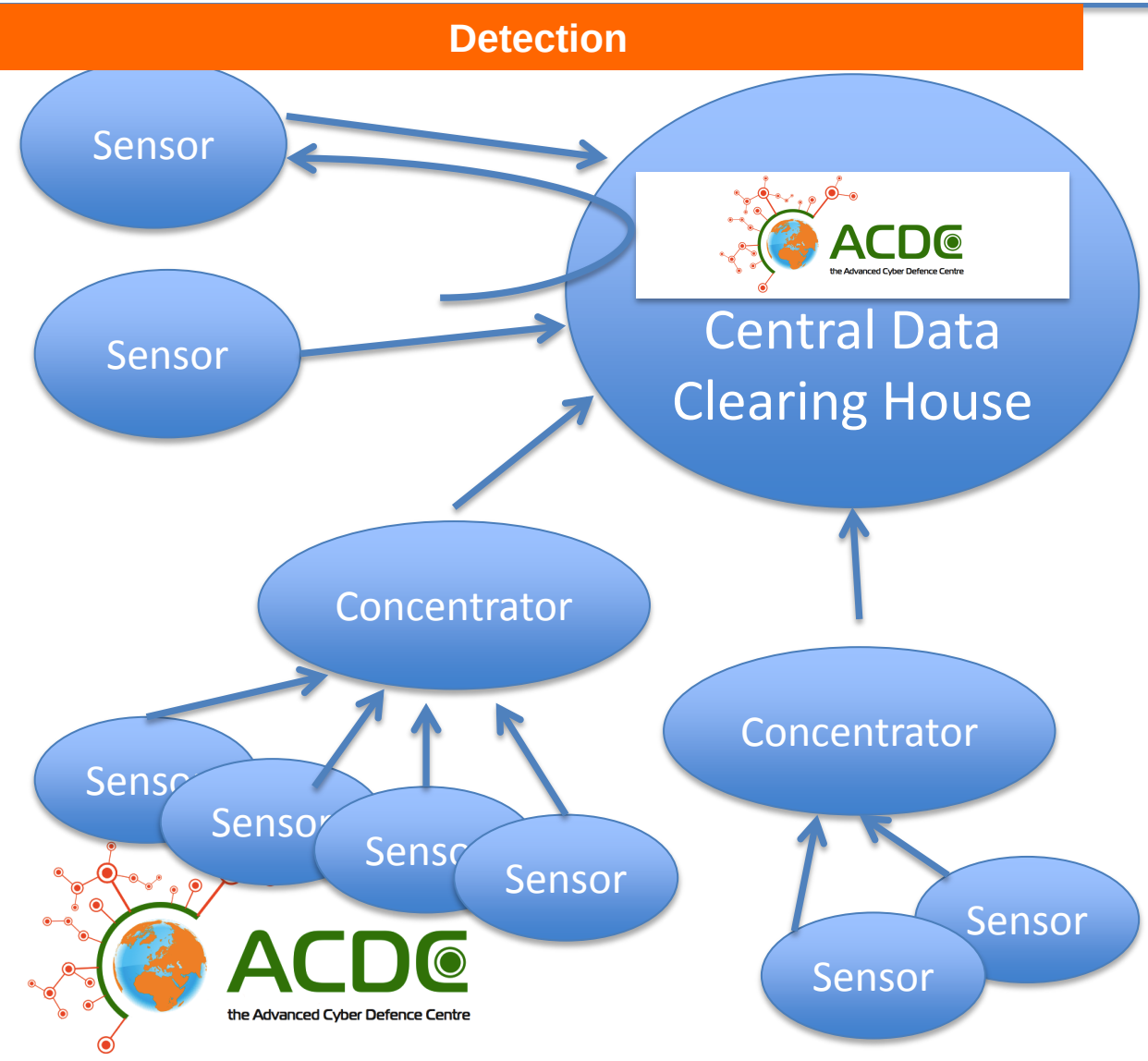
Hosting provider

Redirect to botfree.eu

Mitigation – helping affected customer

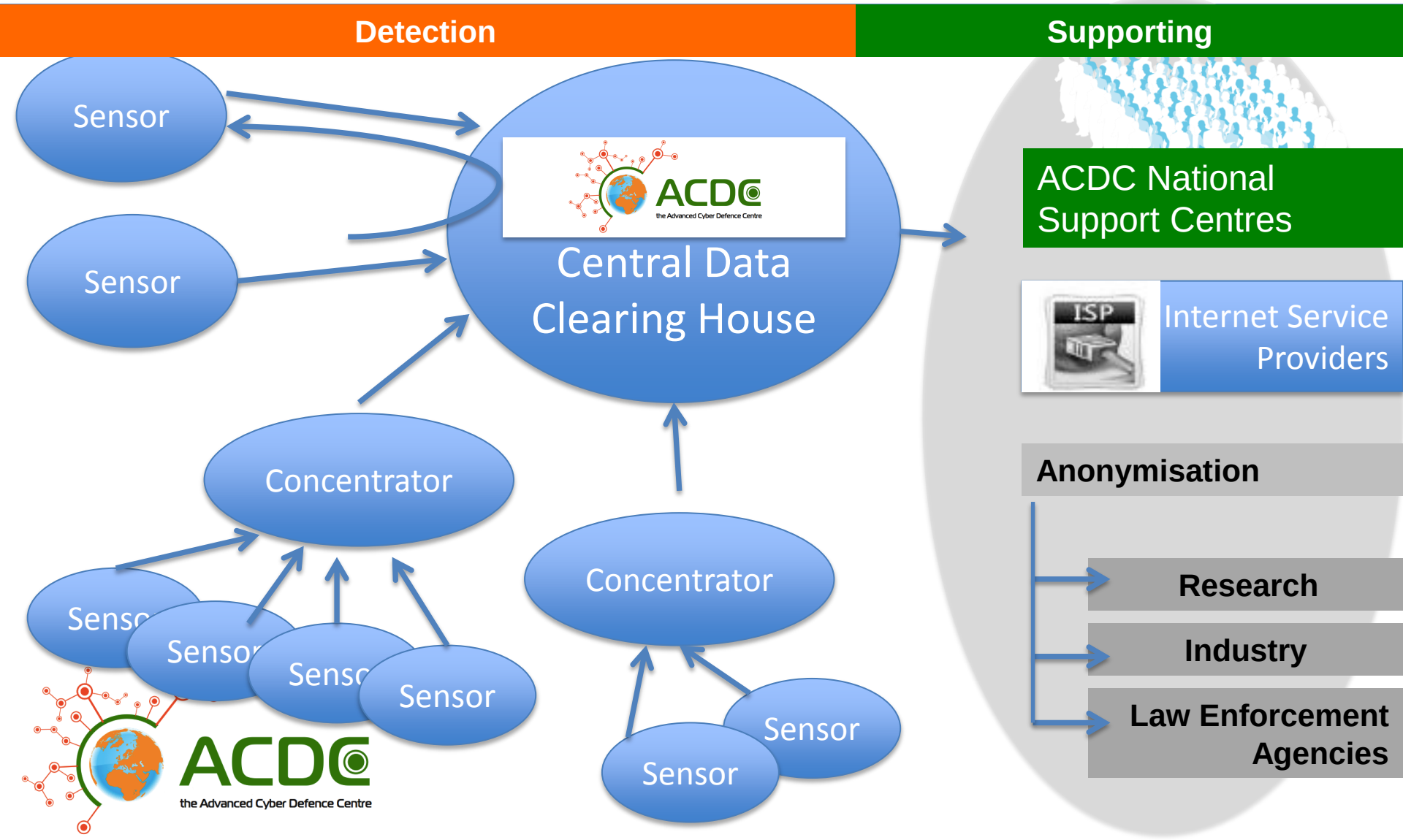
ACDC
the Advanced Cyber Defence Centre

ACDC – central Data Clearing House



- ✓ Sensors delivering data directly or through concentrators
- ✓ Sensors can request additional feeds to work with
- ✓ 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

ACDC – central Data Clearing House



ACDC – Tools & experiments
Example - Protecting mobile users

XLAB **CARNet** **LSEC**

Creating a new solution by combining tools from different partners

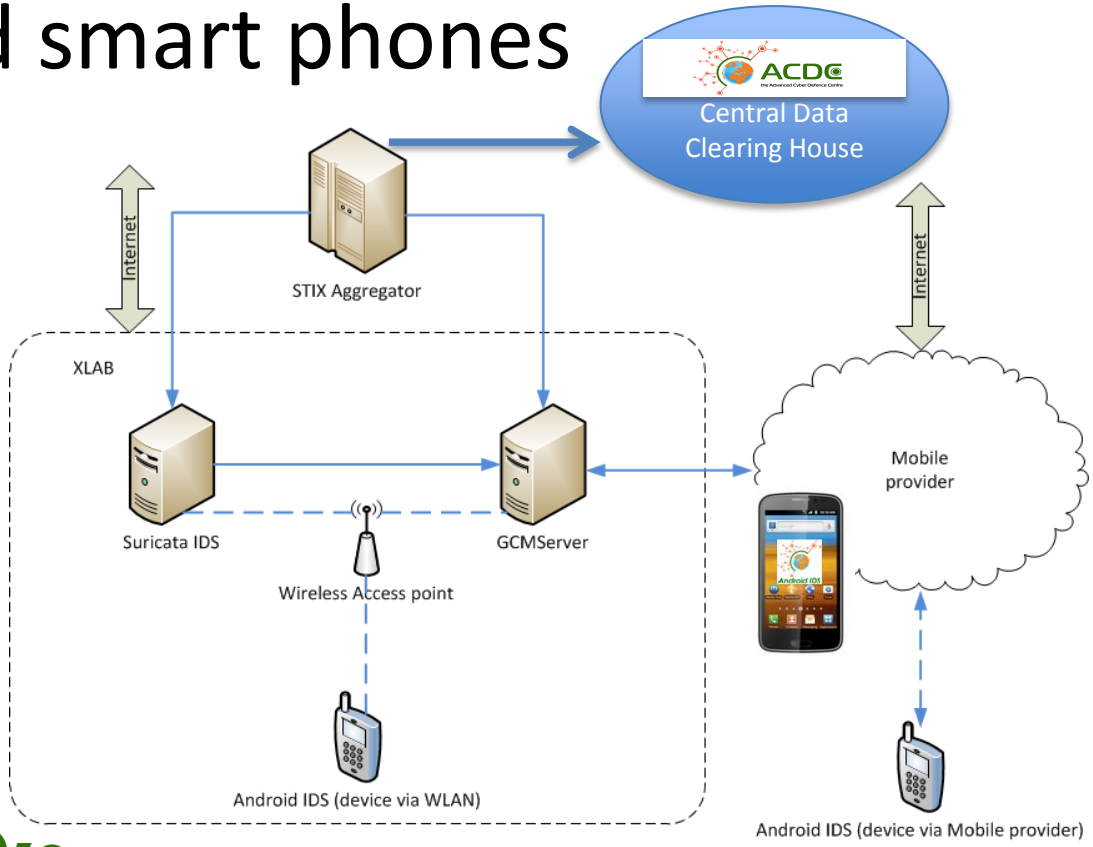
ACDC
the Advanced Cyber Defence Centre

ACDC Partner Tool

XLAB NOT IDLE

Mobile device protection

- ✓ Intrusion Detection System for Android smart phones



ACDC the Advanced Cyber Defence Centre

cip competitiveness and innovation framework programme 2007-2013

ACDC – linking tools to deliver enhanced protection

ACDC EXPERIMENT

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

ACDC
the Advanced Cyber Defence Centre

cip competitiveness and innovation framework programme 2007-2013

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 through concentrator

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

ACDC
the Advanced Cyber Defence Centre

cip competitiveness and innovation framework programme 2007-2013

Standing of the Project at Bulgarian Posts PLC

WP2 - Performing activities of Bulgarian posts PLC (BGPOST)

- ***Co-operation with CarNet (Croatia)***
  - Implementation of Spamtrap, Honeypot, WebSites sensors
  - Development of testing environment
- ***Co-operation with CERT-RO (Romania)*** – installing of Dioanea and Kippo sensors, developed & made by the Romanian partner
- ***Working with FKIE*** - *implementation of sensors integrated with the development of* **CarNet**
- ***Planning the participation of BGPOST*** *in the started experiments &testing with WP3 in three of the four possible directions* – SPAM, WebSites, DDoS that are applicable to our IT infrastructure.

ACDC the Advanced Cyber Defence Centre

1879 БЪЛГАРСКИ ПОЩИ традиции·качество·доверие

cip competitiveness and innovation framework programme 2007-2013

Standing of the Project at Bulgarian Posts PLC

Primary Results

############ Spamtrap data ##################

Total XX spams received

Timestamp: 2013-12-06 01:43:15 Sender IP: 173.163.179.6 Content: en
Recipient: zshkjoaafai@softechnique.com Has keywords: 1
Malicious attachment: Statement_061213.zip-324190-0
Checksum: f16cb7f555a5c373c3e2f120c3ce5873

Timestamp: 2013-12-06 01:37:28 Sender IP: 109.155.234.156 Content: en
Recipient: zshkjoaafai@softechnique.com Has keywords: 0
Malicious attachment: ATO_TAX_061213.zip-324181-0
Checksum: 71678f17d5436484f7edfd35b708e871

ACDC the Advanced Cyber Defence Centre

1879 БЪЛГАРСКИ ПОЩИ традиции·качество·доверие

cip competitiveness and innovation framework programme 2007-2013

Standing of the Project at Bulgarian Posts PLC

Primary Results

############## Glastopf data ###################

Total XX attackers today:

Attacker data:
Timestamp: 2013-12-06 14:02:57 Attacker IP: 46.246.62.142 Source port: 53401 Destionation port: 80 Protocol: http Country code:
None
Samples used by the attacker:
2f73f0142db788ad93e70d56d9ea9ba0 (This sample was used 7 times before)
Compromised URL used: http://Www.Web-Systems.pl/ Host: www.web-systems.pl Country code: FR

Attacker data:
Timestamp: 2013-12-06 14:03:12 Attacker IP: 5.10.83.54 Source port: 48401 Destionation port: 80 Protocol: http Country code: NL
Samples used by the attacker:
471d96e1b1fd8b07022c9291dd14c859 (This sample was used 8 times before)
Compromised URL used:http://theceramiccurlingiron.blogspot.com Host: theceramiccurlingiron.blogspot.com Country code: None

ACDC
the Advanced Cyber Defence Centre

1879
БЪЛГАРСКИ ПОЩИ
традиции·качество·доверие

cip competitiveness and innovation framework programme 2007-2013

Standing of the Project at Bulgarian Posts PLC

WP5 - Presenting the results on the project and distributing of information to the target groups, operation and applicability perspectives

The main activities of Bulgarian Posts PLC during the current period is presenting the results on the project and disseminating the information to the target groups **:**

- ***State-owned enterprises***
- ***Banking and credit institutions***
- ***Telecommunication operators***
- ***Legal entities & Natural persons***

The project has put into effect 15 publications in national media, 4 radio-interviews, 2 presentations on IT conferences with international participation.

- ✓ ITC 12th International Conference on Information Security and Data Storage 26.Sept.2013
- ✓ IDC Conference on "Information Security and Datacenters Evolution" 20th March 2014

ACDC the Advanced Cyber Defence Centre

1879 БЪЛГАРСКИ ПОЩИ традиции·качество·доверие

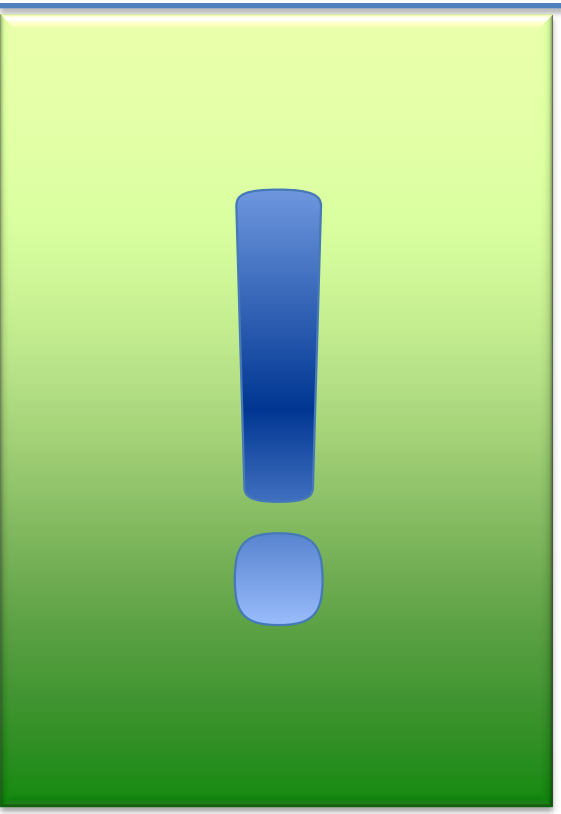
cip competitiveness and innovation framework programme 2007-2013

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

ACDC
the Advanced Cyber Defence Centre

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, 20 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

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

ACDC
the Advanced Cyber Defence Centre

The ACDC Community

Get involved!

The ACDC outreach team

Peter Meyer – peter.meyer@eco.de

Véronique Pevtschin – veronique.pevtschin@eng.it

Kazim Hussain karim.hussain@atosresearch.eu

ACDC
the Advanced Cyber Defence Centre