☹

A CIP-PSP funded pilot action
Grant agreement n°325188

Deliverable	**D6.3.4 – Final report on ACDC user community - lessons learned, proposals for future involvements**
Work package Due date Submission date Revision Status of revision	WP6 31/07/2015 20/07/2015 – updated 27/11/2015 3.01 Final
Responsible partner Contributors	Engineering Ingegneria Informatica Véronique Pevtschin (EII), Ioana Cristina Cotoi (EII), Barbara Pirillo (EII), Peter Meyer (eco), Tiziano Inzerilli (ISCTI), Angela Garcia (INCIBE), Catalin Patrascu (CERT-RO), Thomas Fontvielle (SignalSpam), Darko Perhoc (CARNet), Jorge de Carvalho (FCCN)
Project Number Project Acronym Project Title Start Date of Project	CIP-ICT PSP-2012-6 / 325188 ACDC Advanced Cyber Defence Centre 01/02/2013

Dissemination Level	
PU: Public	✓
PP: Restricted to other programme participants (including the Commission)	
RE: Restricted to a group specified by the consortium (including the Commission)	
CO: Confidential, only for members of the consortium (including the Commission)	

Version history

Rev.	Date	Author	Notes
1.01	3/06/2015	EII – Ioana Cotoi	Creation of deliverable – scope of document and table of content
1.02	06/06/2015	EII – Veronique Pevtschin	Validation of the methodology
1.03	15/06/2015	ECO – Peter Meyer	Content Contribution
1.04	15/06/2015	SignalSpam – Thomas Fontvielle	Content Contribution
1.05	15/06/2015	INCIBE – Angela Garcia	Content Contribution
1.06	15/06/2015	CARNet - Darko Perhoc	Content Contribution
1.07	15/06/2015	CERT RO – Catalin Patrascu	Content Contribution
1.08	15/06/2015	FCCN – Jorge de Carvalho	Content Contribution
1.09	15/06/2015	ISCTI – Tiziano Inzerilli	Content Contribution
1.10	20/06/2015	EII – Ioana Cotoi	Integration of partners' contribution
1.11	14/07/2015	EII – Barbara Pirillo	Content contribution
1.12	15/07/2015	EII - Veronique Pevtschin	Review
1.13	20/07/2015	EII – Ioana Cotoi	Final Version
2.00	20/11/2015	EII - Véronique Pevtschin	Update following final review
3.01	27/11/2015	EII – Ioana Cotoi	Final update

Table of contents

Table of tables

Table of figures

Glossary

ACDC	Advanced Cyber Defence Centre
CCH	Central Clearing House (the ACDC shared data repository)
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DAM	Data Access Manager
DoW	Description of Work
EC3	European Cybercrime Centre
ECI	European Critical Infrastructures
ECB	External Consultative Board
ENISA	European Network and Information Security Agency
EU	European Union
ICT	Information and Communication Technologies
ISP	Internet Service Provider
JSON	JavaScript Object Notation
LEA	Law Enforcement Authority
LoI	Letter of interest
MAAWG	Messaging Anti-Abuse Working Group
NSC	National Support Centres (ACDC relay nodes)

1. Executive summary

Over the lifetime of ACDC, the project focused on identifying stakeholders and reaching out to them to create not only awareness of- but also active participation to- the activities organised by the project, in order to create the ACDC community and pave the way to sustainability.

Creating this member-based community was driven first and foremost by the **participative dimension**, through which specific activities were designed to attract stakeholders with different profiles to join efforts in fighting botnets.
The participative dimension built on different levels of involvement offered through the community, including:

- support – uptake of the ACDC National Support Centre model to create a national ACDC node
- technical – involvement in the ACDC experiments to create new solutions and services, thereby improving the detection, prevention, mitigation of botnets / contribution of solutions and services to enhance support;
- data – sharing data sets to improve the detection of botnets and providing a European repository of data for further research by IT providers and researchers;
- regulatory – active sharing of experiences acquired during the implementation of actions such as data sharing, in which national and European regulations have an important impact;

Over its 30 months duration as a pilot project, ACDC participated to more than 200 events and obtained 40 letters of Interest from stakeholders available for active participation, more than doubling the initial ACDC community of close to 30 partners. ACDC created and implemented incentive pages focused on different stakeholders' profiles to explain the interest of joining ACDC. To provide a single and easily accessible focal point for the ACDC community, ACDC deployed an online community portal implementing all the dimensions mentioned above, prepared and launched a support campaign to increase the visibility of the Community Portal and to animate it.

The role initially foreseen for the ACDC Community Portal in the Description of Work indicated (Task 6.2) a social platform environment to support interaction and participation. Following the evolution of ACDC, the community portal evolved from this initial role as "interaction and participation" support into "the single entry point for ACDC", including the support for sharing policies of sensitive data, the interface to the actual ACDC Central Clearing House acting as the data repository (CCH), the full management of access keys and the information, visualisation and participation to experiments. This approach is an important evolution to support *operational* involvement of stakeholders in the activities of ACDC, far beyond the originally foreseen interaction model of stakeholders. It is also a key element easing the sustainability of ACDC beyond the end of the project.

D6.3.4 is a self-contained report meaning that it encapsulates all the information from the initial setting up and strategy for a community portal and ending with the lessons learned. Therefore, D6.3.4 presents not only the interests of stakeholders to join, but also the concrete results obtained in terms of user participation to the online and physical resources deployed by the ACDC partners, namely the Community Portal and the National Support Centres as well as the set of tools. The final part of the deliverable focuses on the lessons learned during the 30 months of the project and the ACDC Community Portal.

The major lessons learned include

- creating an active community is easier when driven by concrete activities requiring shared involvement rather than remaining at the knowledge / information sharing level
- addressing consolidated user needs through experiments that involve multiple tools from different organisations creates valuable results, but the mechanism is costly in terms of time to

define, set-up and operate. Future evolutions should analyse how to evolve the "experiments" approach

- defining a flexible model for creating national support centres eases the process of extending beyond the initial ACDC partners
- building trust between stakeholders across Member States is easier to achieve when built bottom-up (from smaller groups to larger groups) and concentrating on common tasks (from operational levels to more strategic ones)
- operating first as a pilot in a research like environment enables data sharing to operate *concurrently* to handling the legal barriers – bringing a practical approach to a complex topic that also enables the immediate testing of new approaches to sharing on a smaller scale.

2. Overview of the link between WP5 and WP6 deliverables

The community approach deployed in WP6 forms an integral part of the dissemination plan and is considered as one of the implementation tools of dissemination addressed by WP5.

The strategy for the community approach of WP6 is to enable stakeholders beyond the ACDC partners to become involved in ACDC with different levels of involvement, whilst the role of WP5 is to support this strategy through concrete dissemination activities. As these WPs are strongly interconnected, the following table provides an overview of which deliverable provides what information. This section is repeated in all WP5 and WP6 deliverables.

Deliverables	*What is in the deliverable?*
D6.1.1 – user profiles and categorization	The different attributes used to categorize stakeholders, easing the prioritisation of the outreach activity of WP6 and the analysis of the different groups contributing to creating the ACDC community.
D6.1.2 – identified users list	The analysis of the stakeholders identified through different activities. This analysis is based on contacts established with 90% of the 426 identified stakeholders.
D6.2.1 – ACDC social platform	The description of the ACDC platform and the extension of its functionalities with respect to the original role foreseen in the DoW.
D6.2.2 – Adding social analytics to ACDC social platform	The addition of tools in the ACDC platform to monitor the activities and create a statistical overview of user activities
D6.3.1 – Involvement model for users in ACDC	A detailed description of the different activities that users can choose to be involved in ACDC, presented a UML graphs.
D6.3.2 – Report on user activities	A list of the activities carried out by ACDC partners over the first 12 months (updated on M20) of existence to lead to user involvement. Next steps identify the different activities proposed to users to become involve in ACDC; these activities are supported by the detailed approach in D6.3.1.
D6.3.3 – Report on users communities activities	The report presents the steps and actions proposed to users to become involve in ACDC and monitors their involvement from M12 to M24
D6.3.4 - Final report on ACDC user community - lessons learned,	The report focuses on the ACDC user community and on how it was created, how (and why) user

proposals for future involvements	profiles were selected, what were the problems encountered, what are the lessons learned and how the ACDC involvement model could be expanded, improved and re-used.
D5.1.1 – Dissemination plan	The full list of activities defined to create awareness about ACDC and support the outreach activities of WP6
D5.1.2 – Intermediate dissemination report	The report of the dissemination activities of the first 12 months; this report is complemented by D6.3.2 for the section on individual meetings with organisations to reach the first level of involvement, i.e. letters of interest.
D5.1.3 – Intermediate dissemination report	The report of the dissemination activities of the second reporting year; this report is complemented by D6.3.2 and D6.3.3 for the section on individual meetings with organisations to reach the first level of involvement, i.e. letters of interest.
D5.1.4. – Final dissemination report	The final dissemination report focuses on the one hand on the collection of the major activities that ACDC has undertaken, but also on the lessons learned on the user community aspect in connection to WP6.

Table 1 – overview of the WP5 – WP6 deliverables over the first 30 months of operation

The timeline below highlights the main activities done in WP5 and WP6, offering an operational view of the connection between the two WPs.

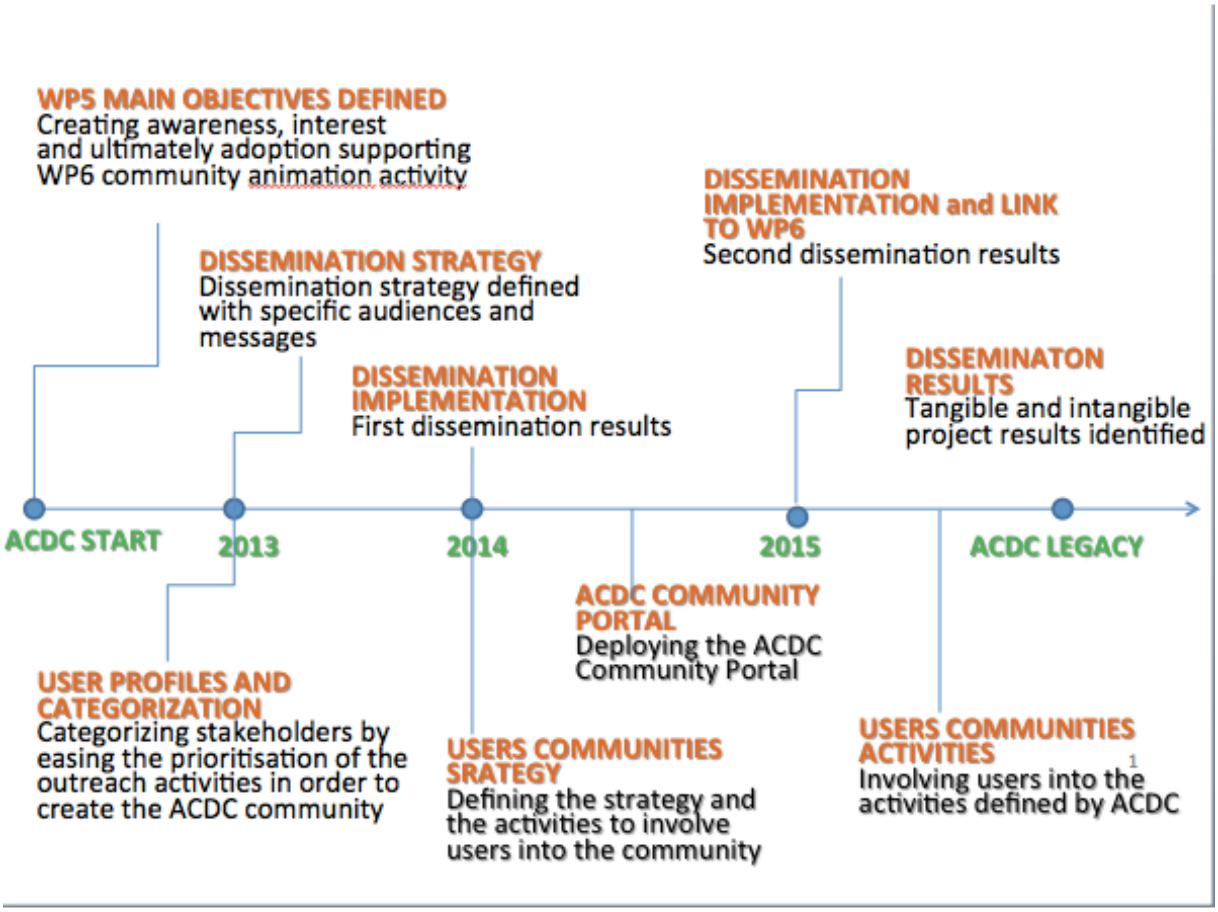

WP5 MAIN OBJECTIVES DEFINED
Creating awareness, interest and ultimately adoption supporting WP6 community animation activity
DISSEMINATION STRATEGY
Dissemination strategy defined with specific audiences and messages
DISSEMINATION IMPLEMENTATION
First dissemination results
DISSEMINATION IMPLEMENTATION and LINK TO WP6
Second dissemination results
DISSEMINATON RESULTS
Tangible and intangible project results identified
ACDC START
2013
2014
2015
ACDC LEGACY
ACDC COMMUNITY PORTAL
Deploying the ACDC Community Portal
USER PROFILES AND CATEGORIZATION
Categorizing stakeholders by easing the prioritisation of the outreach activities in order to create the ACDC community
USERS COMMUNITIES SRATEGY
Defining the strategy and the activities to involve users into the community
USERS COMMUNITIES ACTIVITIES
Involving users into the activities defined by ACDC

Figure 1 – WP6 &WP5 connection

3. ACDC – a structured approach to creating a community

Our dependence on technology continues to grow and, at the same time, the internal complexity of organisations' ICT systems and the external threat environment continue to grow and evolve in dynamic and daunting ways.

One approach to cyber security risk management focuses ***inward*** on understanding and addressing incidents, vulnerabilities, weaknesses and potential impact. Meanwhile, effective defence against current and future threats requires the addition of a balancing, ***outward*** focused approach, on understanding the adversary's behaviour, capability, and intent.

Those called to deal with incidents or responsible for managing cyber security programmes are faced with an overwhelming amount of information, often raw and unstructured, to the point where making efficient use of these information flows has become a challenge in itself. Effective decision-making may therefore be hampered, especially in times of crisis.

SMEs face a particular challenge in terms of acquiring information that is relevant for their cyber protection and the necessary expertise to analyse this information in order to address the cyber security threats they face.

Effective decision-making, early warning systems and cyber security management require tools and techniques that enable organisations to efficiently process the flow of information from both internal and external sources and manage the implementation of cyber security solutions.[1]

In this context, ACDC's approach was implemented through the creation of a community of organisations built on active participation, whose roles in the fight against botnets were identified across one or more of the following dimensions:

- **a support level** – creation of ACDC support centres. This role was mainly taken over by CERTs and other support infrastructures, as well as network operators and ISPs interested in easing the channelling of information to end-users, whilst decreasing the actual load on the operators themselves.
- **a technical level** – involvement into ACDC experiments to create and test new solutions and services , thereby improving the detection, prevention, mitigation of botnets. Innovation was achieved by uniting existing or upcoming solutions / services into a new integrated solution, aligned to a specific user need such as fighting DDOS attacks etc. Organisations involved in this role were therefore mainly IT providers and researchers.
- **a data level** – sharing data sets to improve the detection of botnets and providing a European repository of data for further research by IT providers and researchers. Innovation in this level was achieved by implementing different sharing policies in an integrated environment, giving data providers full control of what, how and with whom to share data and data users, such as researchers and IT providers, access to data on which to build new innovations and test existing solutions. Organisations involved in this role were therefore mainly network operators, IT providers and researchers.
- **a regulatory level** – active sharing of experiences acquired during the implementation of actions such as data sharing, in which national and European regulations have an important impact. This role was, in practice, implemented by organisations with legislative and regulatory expertise and by network operators involving their legal departments.

Whilst the ACDC model was specifically tested for the fight against botnets, the actual community approach is not specifically limited to fighting botnets; the infrastructure put in place during the project has already expanded beyond the foreseen scope and its exploitation in the increasingly challenging cyber-security context is at the forefront of a group of stakeholders of the ACDC community.

4. Result: the ACDC community

Key results

- ✓ 1 single access point to all ACDC facilities
- ✓ supporting social interaction to continuously enrich shared knowledge
- ✓ navigating "who's who" in cyber security in Europe
- ✓ trust building process operational, allowing for sharing of attack information through user controlled sharing policies
- ✓ 180 stakeholders joined

[1] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/1053-ds-04-2015.html

Following the approach presented in the previous section, the ACDC community currently includes:

- 180 organisations active within a dedicated online portal
- a structured presentation of the different benefits to different profiles of organisations, ranging from providers and researchers to prosecutors, law enforcement, CERTs and critical infrastructure operators
- a mentoring mechanism that supports the joining process for new organisations through the link to- and support by- existing members
- full support for access to all ACDC activities, including the support, data, technical and regulatory dimensions

The creation of a stakeholders' community is a major contribution to the out-reach approach proposed by the ACDC project in fighting the botnet issue across Europe.

The creation of the ACDC community followed two connected lines of action. The first line focused on the identification of potential stakeholders, the definition of their relevance with respect to cyber-security in general, and to the botnet topic in particular, and the initial contact to invite them to join the community.
The second line of action focused on the definition of the community governance, and on the creation of the community platform, used as the main channel for community members to interoperate. The community platform implements the ACDC governance, a key structuring phase to ensure that interactions operate within a given set of shared rules.

The approach to ACDC community building was developed based on an overall process shown in the next figure.

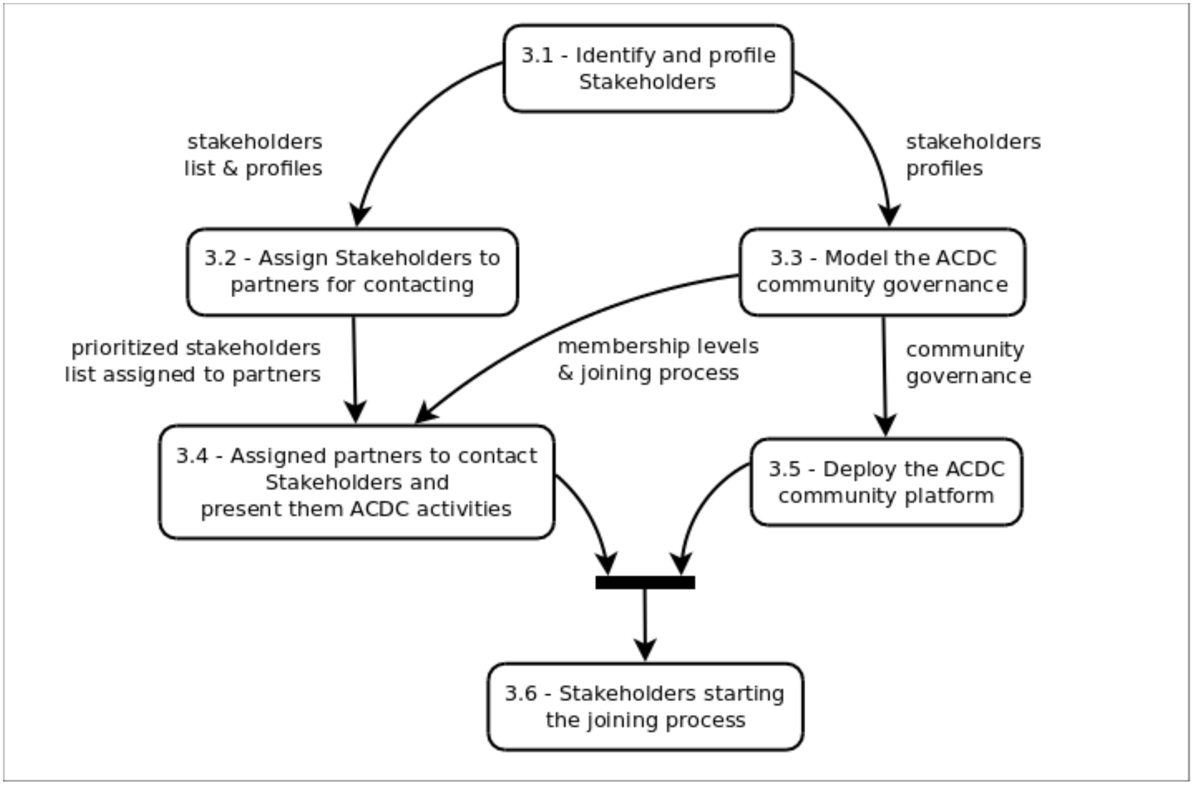

3.1 - Identify and profile Stakeholders
stakeholders list & profiles
stakeholders profiles
3.2 - Assign Stakeholders to partners for contacting
3.3 - Model the ACDC community governance
prioritized stakeholders list assigned to partners
membership levels & joining process
community governance
3.4 - Assigned partners to contact Stakeholders and present them ACDC activities
3.5 - Deploy the ACDC community platform
3.6 - Stakeholders starting the joining process

Figure 2 – ACDC Community building process

Each block in the diagram represents a step in the process, while the links between the steps represent the information that is provided by each step to the following one. The black rectangle in the lower part of the diagram represents a synchronization point for activities 3.4 and 3.5, meaning that activity 3.6 started from a stakeholder once the community platform was available (from step 3.5) and the stakeholder has been contacted (in step 3.4).

All these steps are therefore oriented towards creating, supporting and animating an active community, by setting up coherent activities designed to bring the community to life:

- the approach adopted by ACDC to create the community: what are the different steps implemented by ACDC partners? How will each partner contribute to this approach?
- the criteria used to classify target stakeholders, ensuring that the community approach is tailored to specific needs and therefore encourages adoption by addressing each sub-group.
- detailed information about the different parameters for the criteria to be implemented in the social community platform

4.1. Activities done to reach out to users

The set of activities implement to reach out to users included

a) the definition of user profiles
b) the creation of benefit oriented incentive pages per user profile
c) the participation to a large number of events

All these activities are detailed below.

4.1.1. Definition of user profiles

This step aimed at defining the parameters to identify and profile stakeholders for the ACDC community. In order for the community to be useful for ACDC aims, the identification of stakeholders started from considerations such as to whom does ACDC bring benefits as well as which stakeholders could usefully contribute to increase ACDC's knowledge base, and the involvement criteria that needed to be met.

In order to identify and profile the stakeholders the first step was to categorize them. The aim of categorizing the potential stakeholders was threefold. Firstly, it created, among the consortium, a shared vocabulary and a common understanding of the terms and concepts related to the stakeholder's identification processes. Secondly, it allowed the analysis of the ACDC community composition and behaviour from different points of view. Thirdly, it impacted the modelling of the ACDC community governance and, later on, the development of the related community platform. Therefore, the stakeholders' categorization criteria were of primary importance for the activities and for the success of WP6 work package.

The criteria identified initially vary both in purpose and in scope, ranging from the most general ones to the cyber-security field, down to the botnet topics that are covered by the ACDC activities. In particular, four categorization criteria were identified: Country, Sector, Positioning and Interest.

a. Country criteria

The definition of the categorization criteria started from considerations about the types of stakeholders that were particularly relevant for ACDC project activities. Firstly, considering the European dimension of the ACDC initiative, it was important to understand how the different countries were involved in the fight against botnets.

In this context, it was essential to diversify between national-level stakeholders and international, European-level, ones. Therefore, a *Country* categorization criterion was important to highlight differences on the way stakeholders interact in a community.

b. Sector Criteria

The introduction of Sector criteria that categorizes stakeholders basing on their sector(s) of operation was of great value for the ACDC community. Such a sectorial categorization had many advantages, mainly, partitioning stakeholders basing on sectors allowed the project to understand the main cybersecurity concerns for each sector, thus enabling the identification of which set of solutions would fit better the needs of each sector, moreover, the targeting of communications and interactions to the set of stakeholders operating in a given sector.

The initial list of Sectors identified for stakeholders of the ACDC community derived from the sectors initially identified by the ECI Directive proposal:

Sector	Description
Energy & Nuclear Industry	Oil and gas production, refining, treatment, storage and distribution by pipelines; electricity generation and transmission; production and storage/processing of nuclear substances
Information, Communication Technologies, ICT	Information system and network protection; instrumentation automation and control systems (SCADA, etc.); internet; provision of fixed telecommunications; provision of mobile telecommunications; radio communication and navigation; satellite communication; broadcasting
Water	Provision of drinking water; control of water quality; stemming and control of water quantity
Food	Provision of food and safeguarding food safety and security
Health	Medical and hospital care; medicines, serums, vaccines and pharmaceuticals; bio-laboratories and bio-agents
Financial	Payment and securities clearing and settlement infrastructures and systems; regulated markets
Transport	Road transport; rail transport; air transport; inland waterways transport; ocean and short-sea shipping
Chemical industry	Production and storage/processing of chemical substances; pipelines of dangerous goods (chemical substances)
Research facilities	Research facilities
Security services	Police structures and equipments; military structures and equipments

Table 2 – Critical Infrastructure sectors

c. Cybersecurity Positioning Criteria

The *Positioning* criteria refers to the positioning of the stakeholder with respect to the cybersecurity field. The present picture in the cybersecurity landscape is complex and subject to changes. Moreover, most of the actors in cybersecurity usually play more than one role (e.g. an ICT company acting both as ISP and mobile operator, and also running its own CSIRT).

For this reason the Positioning criteria has been structured in an initial list of positioning areas, that grouped the possible positioning(s) that each stakeholder could have in the field.

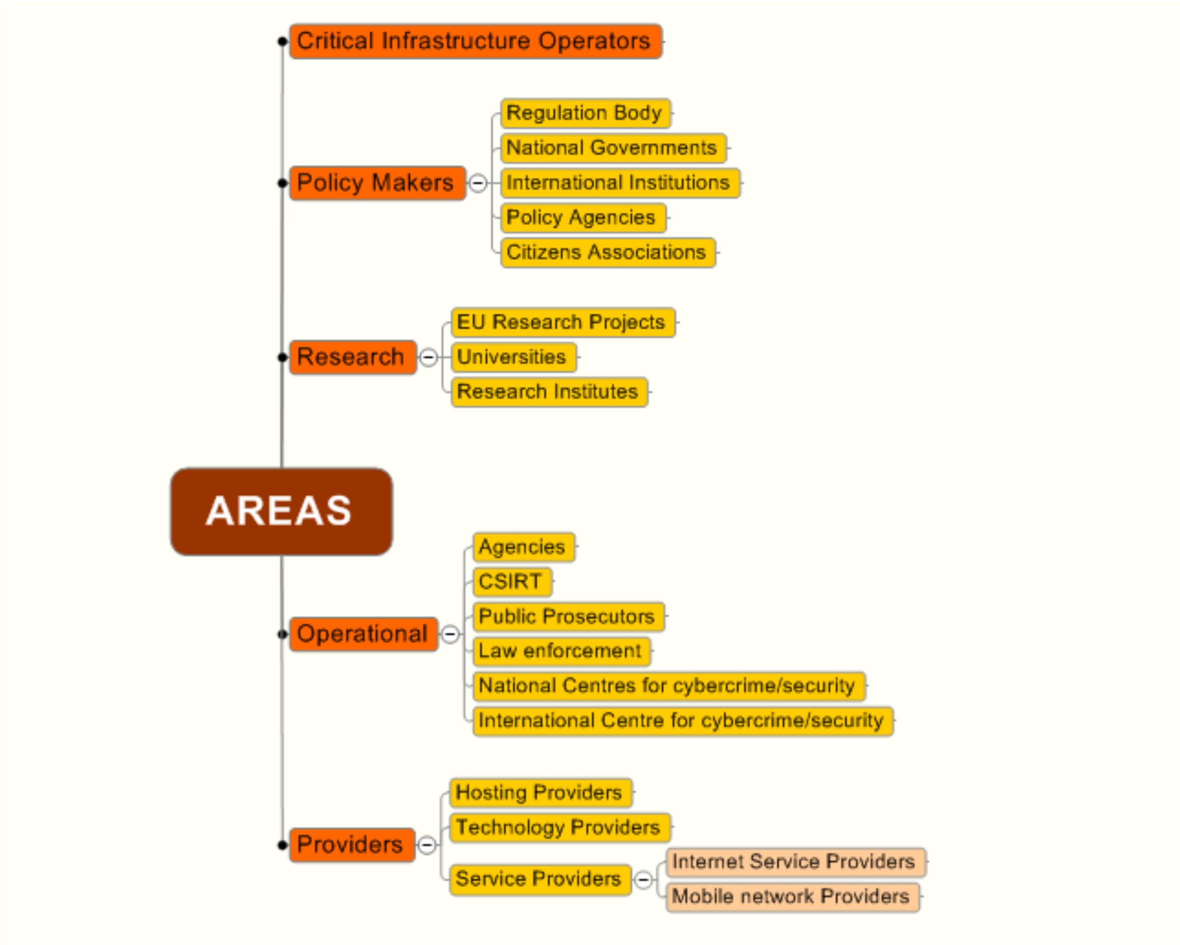


Figure 3 – Identified Areas for the Stakeholders Positioning

d. The ACDC potential involvement criteria

The goal of this criteria was to identify stakeholders who have access to botnet related data (for instance ISPs detecting on their networks etc), willing to provide data, interested in accessing data, requiring one-to-one partnerships for data sharing, providing new solutions at trial level etc.

Based on the Stakeholders categories identified above, it was then important to focus on the information needed for stakeholders profiling. Besides the information that came out from the stakeholder categorization, organisation information was also relevant to distinguish them among stakeholders that are relevant for the ACDC community. This information was used in multiple steps during the ACDC project, starting from the collection of information about potential stakeholders, to the stakeholders contacting phase, down to the modelling of stakeholders in the portal, and, finally, during the interaction of members in the community. For this reason it was important to have a common modelling and understanding of stakeholders' information.

The table below shows the set of parameters that were used to identify stakeholders for the ACDC community.

Parameter Name	Parameter Description	Notes
Organization name	Organization Legal Name	This field is mandatory.
Organization address	Organization Legal Address.	This field is mandatory.

Organization scope	The scope of the organization, either national or European. This parameter derives from the Country categorization from section 4.1.	This field is mandatory. It indicates that an organization operates at the European scale and has no particular linking to one or more countries of the EU.
Country(ies) of operation	The set of countries where a national organization is operating. This parameter also derives from the Country categorization from section 4.1. The initial set of options for this information will include EU countries only.	If the Organization Scope is national, one or more countries must be specified for the organization. This parameter is empty for European organizations.
Website	The website of the organization	This field is optional. This allows to identify “just-born” organizations that do not have their website online yet
Contact work positioning	This is the working positioning of the contact in the organizational chart. To avoid dealing with details of each organization’s chart, the choice is limited to the following positions: • *Top Level* – e.g. owner, CEO, etc. • *High Level* – e.g. director, general manager, etc. • *Middle Level* – e.g. young manager, project coordinator, etc. • *Entry level* – e.g. junior worker, specialist, etc.	This field is optional. In case more than one contact is known in the organization the most relevant one (usually the higher in the organization’s hierarchy) should be indicated.

Table 3 – Identified information for the Stakeholder profiling

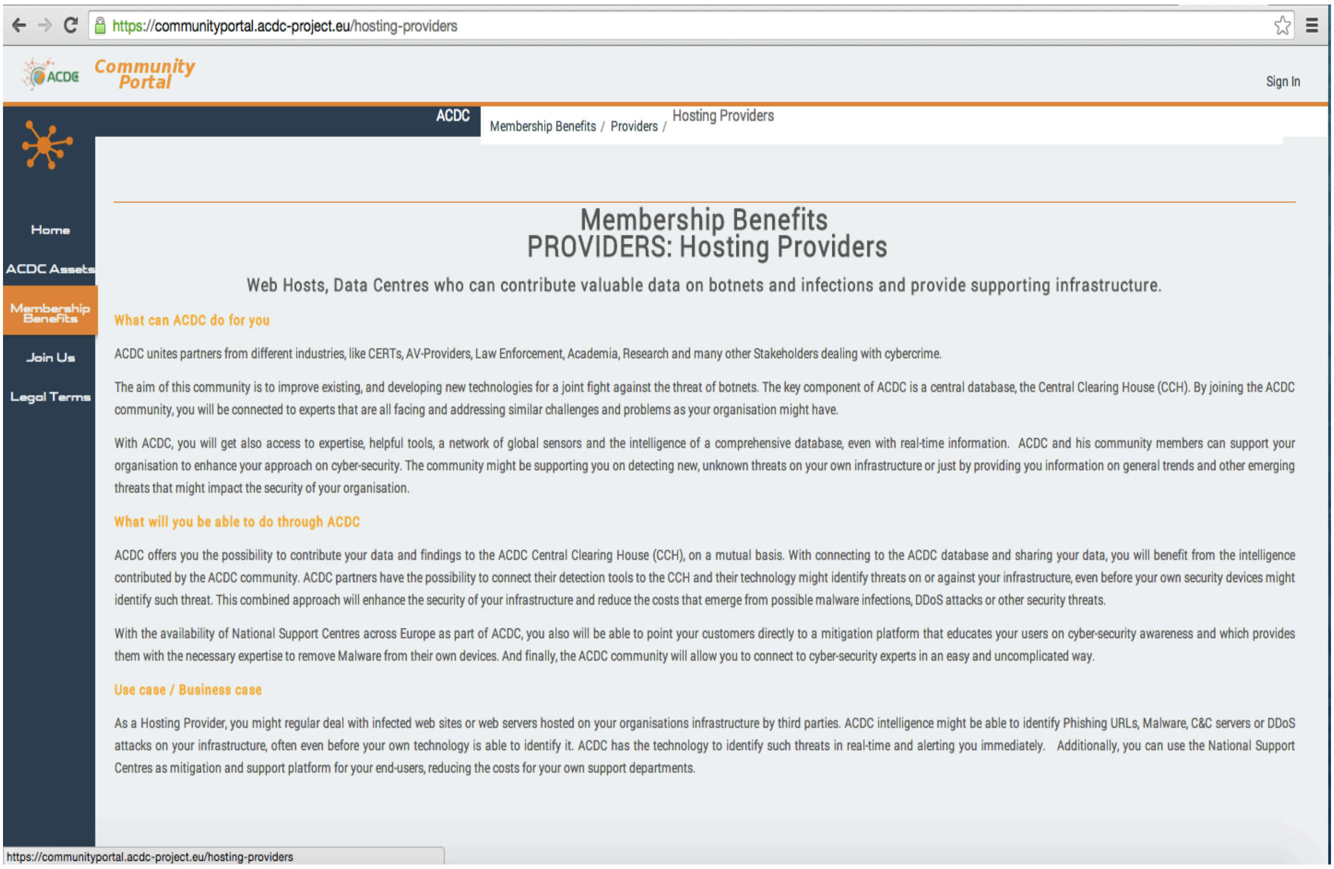
4.1.2. Incentive pages: the benefits per organisation profile

Besides the definition of the parameters to identify and profile stakeholders for the ACDC community, **incentive pages** oriented to each profile of stakeholder were prepared. The idea of the Incentive Pages started from the objective to provide an immediate message to users on the *benefits* they can get from ACDC.

The incentive pages are structured in two parts:
a) a description of the benefits each kind of stakeholder can expect from ACDC (What can ACDC do for you? What are you able to do through ACDC?)
b) concrete use cases based on the ACDC assets, oriented to each kind of stakeholder.

The incentive pages were used to facilitate the out-reach activities and were also made available on the public page of the ACDC Community Portal. The structure of the incentive pages in the ACDC Community portal is as follows:

- initial short description of the main assets of the ACDC project: description of the 3 channels Data Clearing House, National support centres, ACDC Community portal;
- What can ACDC do for you? What are you able to do through ACDC? – this section was provided for each user category
- Concrete example of use of one (or more than one) of the ACDC assets per each category;


https://communityportal.acdc-project.eu/hosting-providers
ACDC
Community Portal
Sign In
ACDC
Membership Benefits / Providers / Hosting Providers
Home
ACDC Assets
Membership Benefits
Join Us
Legal Terms
https://communityportal.acdc-project.eu/hosting-providers

Membership Benefits
PROVIDERS: Hosting Providers

Web Hosts, Data Centres who can contribute valuable data on botnets and infections and provide supporting infrastructure.

What can ACDC do for you

ACDC unites partners from different industries, like CERTs, AV-Providers, Law Enforcement, Academia, Research and many other Stakeholders dealing with cybercrime.

The aim of this community is to improve existing, and developing new technologies for a joint fight against the threat of botnets. The key component of ACDC is a central database, the Central Clearing House (CCH). By joining the ACDC community, you will be connected to experts that are all facing and addressing similar challenges and problems as your organisation might have.

With ACDC, you will get also access to expertise, helpful tools, a network of global sensors and the intelligence of a comprehensive database, even with real-time information. ACDC and his community members can support your organisation to enhance your approach on cyber-security. The community might be supporting you on detecting new, unknown threats on your own infrastructure or just by providing you information on general trends and other emerging threats that might impact the security of your organisation.

What will you be able to do through ACDC

ACDC offers you the possibility to contribute your data and findings to the ACDC Central Clearing House (CCH), on a mutual basis. With connecting to the ACDC database and sharing your data, you will benefit from the intelligence contributed by the ACDC community. ACDC partners have the possibility to connect their detection tools to the CCH and their technology might identify threats on or against your infrastructure, even before your own security devices might identify such threat. This combined approach will enhance the security of your infrastructure and reduce the costs that emerge from possible malware infections, DDoS attacks or other security threats.

With the availability of National Support Centres across Europe as part of ACDC, you also will be able to point your customers directly to a mitigation platform that educates your users on cyber-security awareness and which provides them with the necessary expertise to remove Malware from their own devices. And finally, the ACDC community will allow you to connect to cyber-security experts in an easy and uncomplicated way.

Use case / Business case

As a Hosting Provider, you might regular deal with infected web sites or web servers hosted on your organisations infrastructure by third parties. ACDC intelligence might be able to identify Phishing URLs, Malware, C&C servers or DDoS attacks on your infrastructure, often even before your own technology is able to identify it. ACDC has the technology to identify such threats in real-time and alerting you immediately. Additionally, you can use the National Support Centres as mitigation and support platform for your end-users, reducing the costs for your own support departments.

Figure 4 – Incentive page implementation

Incentive pages are presented for 6 categories, namely

- **Providers** of technical solutions and services to fight botnets
- **Critical infrastructure operators** who operate information networks and can benefit from deploying ACDC solutions and contribute data to speed up botnet detections
- **Policy makers** who can gain valuable insight into both statistics of botnets and join discussions to understand the reality of data sharing and botnet detection
- **Researchers** who can use ACDC data information for testing new solutions
- **Operational stakeholders** who fight attacks on a daily basis, including CERTs, law enforcement and prosecutors, and centres focused on cyber-security
- **Intermediaries**, such as user associations and sectoral associations who focus on supporting victims.

4.2. ACDC Community Portal

The Community Portal of ACDC (www.communityportal.acdc-project.eu) aims to foster a wider level of information sharing and, therefore, a faster and more effective communication between stakeholders active in the cyber security area with the final aim to fighting botnets across Europe.

The creation of a participative stakeholders' community is a major objective in the ACDC project and is in line with the overall project's approach based on fostering a wider level of information sharing and, therefore, a faster and more effective communication between stakeholders active in the cyber security area.

The role of the ACDC community portal is to ease access to the different activities that can be shared by ACDC community members, with a view of:

✓ *Improving the detection*

Improving the detection of botnets can be achieved by increasing the speed at which a botnet is detected; this in turn can be achieved by increasing the amount of data sets provided by Internet Service Providers (ISPs) to the ACDC centralised data clearing house and improving the correlation and analysis of this data using state-of-the art tools and techniques. Supporting this through the ACDC Community Portal requires features to organise the provision of data to the centralised data clearing house, as well as retrieval of the data. These processes required the building of trust among the providers; one major contribution of ACDC is linked to this trust building. Indeed, on the regulatory side, a detailed analysis was made of the European regulations – on the operational side, a complete approach to "sharing policies" enabled organisations to manage, through the online ACDC resources, the sharing approach – sharing data bilaterally with an identified organisation, sharing with a profile of users, sharing based on geographic locations etc.

This also constitutes an important change that was brought by ACDC with respect to its original description of work; indeed, rather than managing the "community approach" and the "data sharing approach" in two separate environments, the ACDC consortium decided to enhance its approach by positioning the community portal as the single entry point to all ACDC facilities – and to further enhance this approach by also creating sharing policies that can be managed by the users themselves.

✓ *Improving the prevention*

The detection of botnets introduced in the previous paragraph can only contribute to improve the prevention if information is sent as fast as possible on the one hand to the ISPs and on the other hand to users of fixed and mobile devices to avoid the creation / spreading of the botnet. Supporting this through the ACDC community portal requires on the one hand foster stakeholders joining the community and on the other hand creating channels to share knowledge.

✓ *Improving the mitigation*

Improving the mitigation is another aspect to which ACDC contributes to, through new tools and services developed during the piloting phase implemented by WP2 and WP3. To move from technology to uptake, the organisation of the solutions was done and made accessible to a wide community of stakeholders. In return, specific features in the ACDC Community Portal implement this.

4.2.1.1. ACDC Community Portal Features

In addition to supporting active participation to ACDC, the ACDC **community** portal is organised not only to present information, but to allow social interaction around this information – allowing users to rate tools and solutions, allowing stakeholders to navigate "who's who" in cyber in Europe – and most of all allowing users to continuously enrich the knowledge that is presented.

It is important to highlight the fundamental change that was brought to the ACDC Community Portal by the consortium with respect to its original description of work; indeed the role initially foreseen for the community portal in the Description of Work indicated (Task 6.2) a social platform environment to support interaction and participation. Following the evolution of ACDC, the community portal evolved from this initial role as "interaction and participation" support into "the single entry point for ACDC", including the support for sharing policies of sensitive data, the interface to the actual CCH, the full management of access keys and the information, visualisation and participation to experiments. This approach is an important evolution to support *operational* involvement of stakeholders in the activities of ACDC, far beyond the originally foreseen interaction model of stakeholders. It is also a key element easing the sustainability of ACDC beyond the end of the project.

The ACDC Community Portal was designed to:

- ➢ Provide a single front-end to access the ACDC Central data Clearing House (CCH)
- ➢ Foster the visibility (and uptake) of activities for the ACDC community
- ➢ Support interaction with stakeholders
- ➢ Enable fast and effective information sharing among members by providing different functionalities and different interaction areas.

The ACDC community portal is structured in two environments, one that is public and accessible to everybody and one that is restricted to ACDC members only.
The Portal is organized across different sections and provides a wide spectrum of online collaboration tools with the objective to share information and knowledge, improve communication between other stakeholders all over the Europe, share data and participate to experiments.

The community portal is structured as follows:

- **Public environment** available at communityportal.acdc-project.eu
  - o **Welcome Page –** short description of the platform and link to the ACDC Community Portal video;
  - o **ACDC Assets -** description of the main assets;
  - o **Membership Benefits** – description of the benefits each category of stakeholders can have by joining the Community;
  - o **"Join Us"** – the section where a new stakeholder can join the ACDC Community Portal
  - o **Legal Terms** – the page contains the terms of use of the Community Portal and Privacy Policy
  - o **CCH Schemata –** the page contains public references to the Json schemata that can be used to send information to the ACDC Central Clearing House

- **Private environment**
  - o **News –** This section gathers all the latest steps taken in ACDC, new features of the community portal, latest events, latest news about cyber security, availability of new solutions, etc.
  - o **Initiatives** – ACDC brings all the initiatives related to cybersecurity together and presents it to the user along with the stakeholders participating in them. A graphic view allows the user to relate initiatives to stakeholders and vice versa. This way, all the information is presented at once and it is easier to comprehend and visualize the current situation of cybersecurity at national or European level. The final goal is therefore to improve user's awareness by presenting information about all existing cybersecurity related initiatives. A unique feature of "initiatives" is that it allows the user to

navigate through the maze of organisations and activities – a feature that has been identified as needed during the first ENISA – industrial workshop held in Brussels on 9th July 2015;

○ **Tools&Services –** ACDC brings a list of available tools and services that can be implemented to protect against cyber attacks, users can also add new tools and services provided o used by them. Each Tool or Service can be ranked by users with votes from 0 to 5.

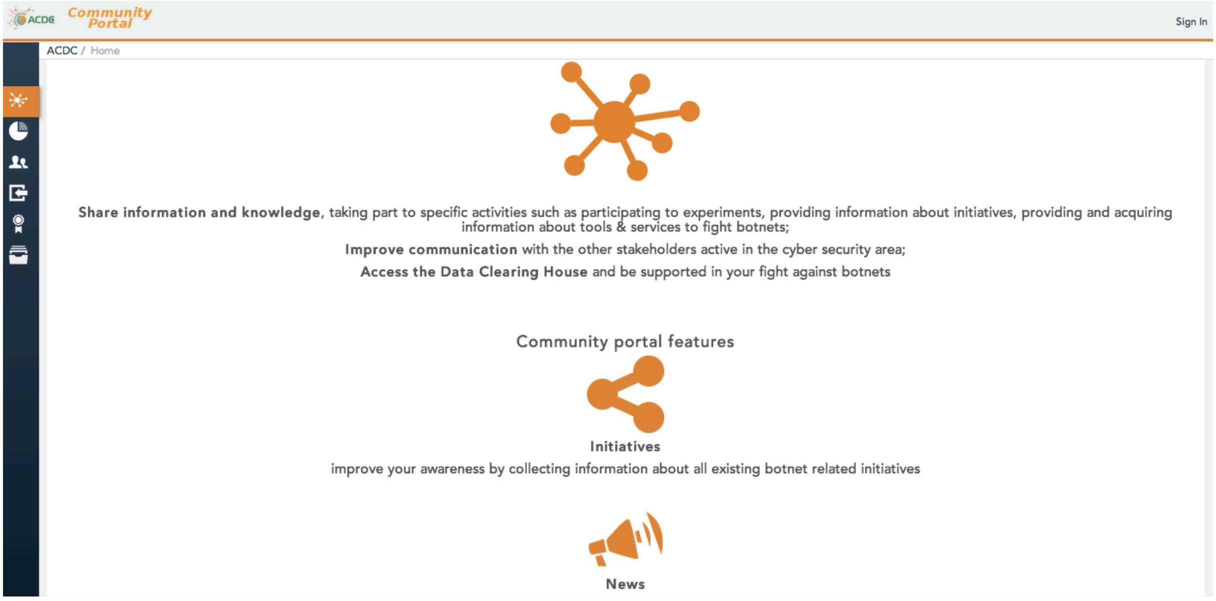
○ **Forum** - is the place collecting all the discussions among community members. The stakeholder uses this application to see all the comments, messages, threads and related posts published in the portal.

○ **Documents** – is the place collecting all the documents related to the community, like documents referring data sharing, experiments, data protection etc.

○ **Experiments** – This section is dedicated to the experiments that took place inside the project. It provides general information about the experiments and stakeholders can send request to participate to it. By participating to an experiment a stakeholder is able to get access to the dedicated Experiment Workspace, where a set of specific information (experiment news, experiment documentation, participants list, etc.) are available.

○ **Data Sharing** – In this section stakeholders are able to share data with other stakeholders and receive data from other stakeholders. The sharing of data happens through the Central Clearing House (CCH). The role of the community portal in the data sharing is to identify stakeholders entitled to ask for (or provide) data among the community and to allow them to set the rules that constrain the data sharing within the community.

○ **ACDC Analytics** – This section provides the visualization of some statistics regarding the number of users and stakeholders that joined, the initiatives published and the tools and services available on the Community Portal.



Share information and knowledge, taking part to specific activities such as participating to experiments, providing information about initiatives, providing and acquiring information about tools & services to fight botnets;

Improve communication with the other stakeholders active in the cyber security area;

Access the Data Clearing House and be supported in your fight against botnets

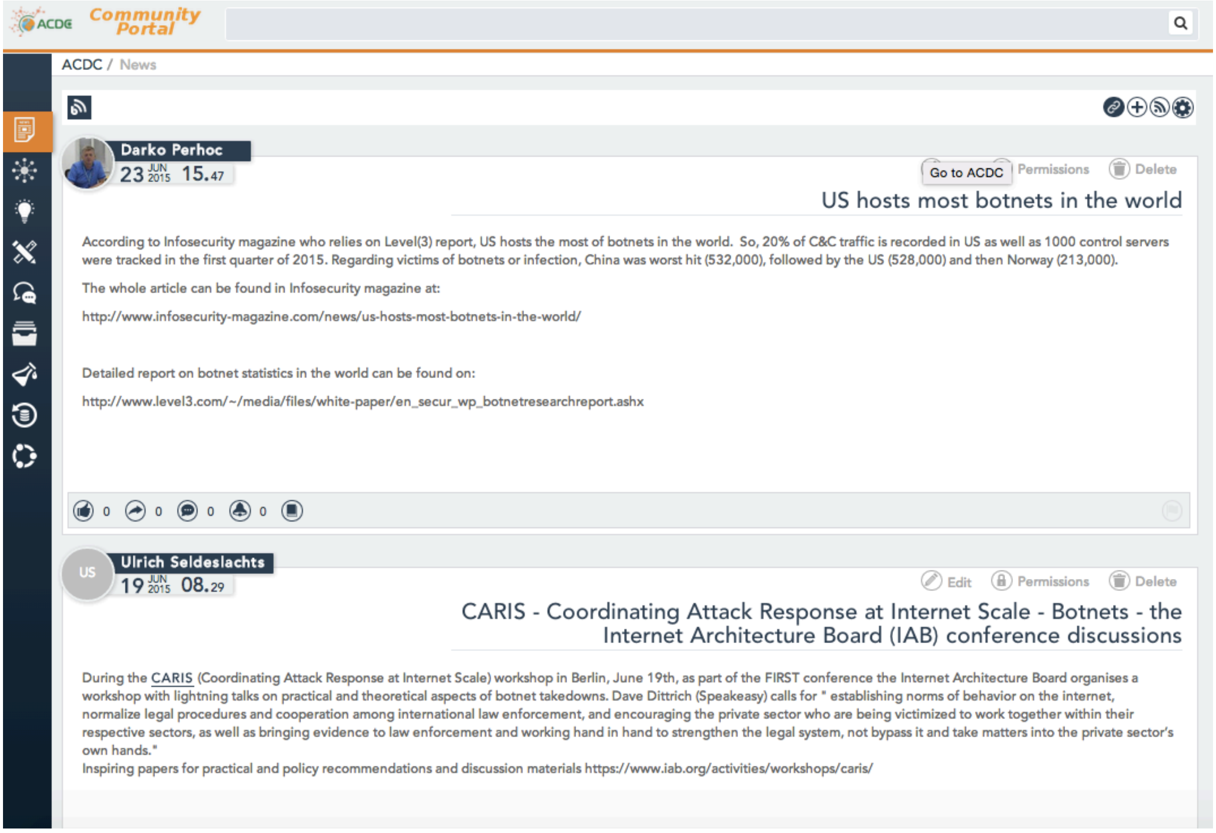
Community portal features

Initiatives

improve your awareness by collecting information about all existing botnet related initiatives

News

Figure 5 – ACDC Community Portal Public Environment



Darko Perhoc
23 JUN 2015 15.47

US hosts most botnets in the world

According to Infosecurity magazine who relies on Level(3) report, US hosts the most of botnets in the world. So, 20% of C&C traffic is recorded in US as well as 1000 control servers were tracked in the first quarter of 2015. Regarding victims of botnets or infection, China was worst hit (532,000), followed by the US (528,000) and then Norway (213,000).

The whole article can be found in Infosecurity magazine at:

http://www.infosecurity-magazine.com/news/us-hosts-most-botnets-in-the-world/

Detailed report on botnet statistics in the world can be found on:

http://www.level3.com/~/media/files/white-paper/en_secur_wp_botnetresearchreport.ashx

Ulrich Seldeslachts
19 JUN 2015 08.29

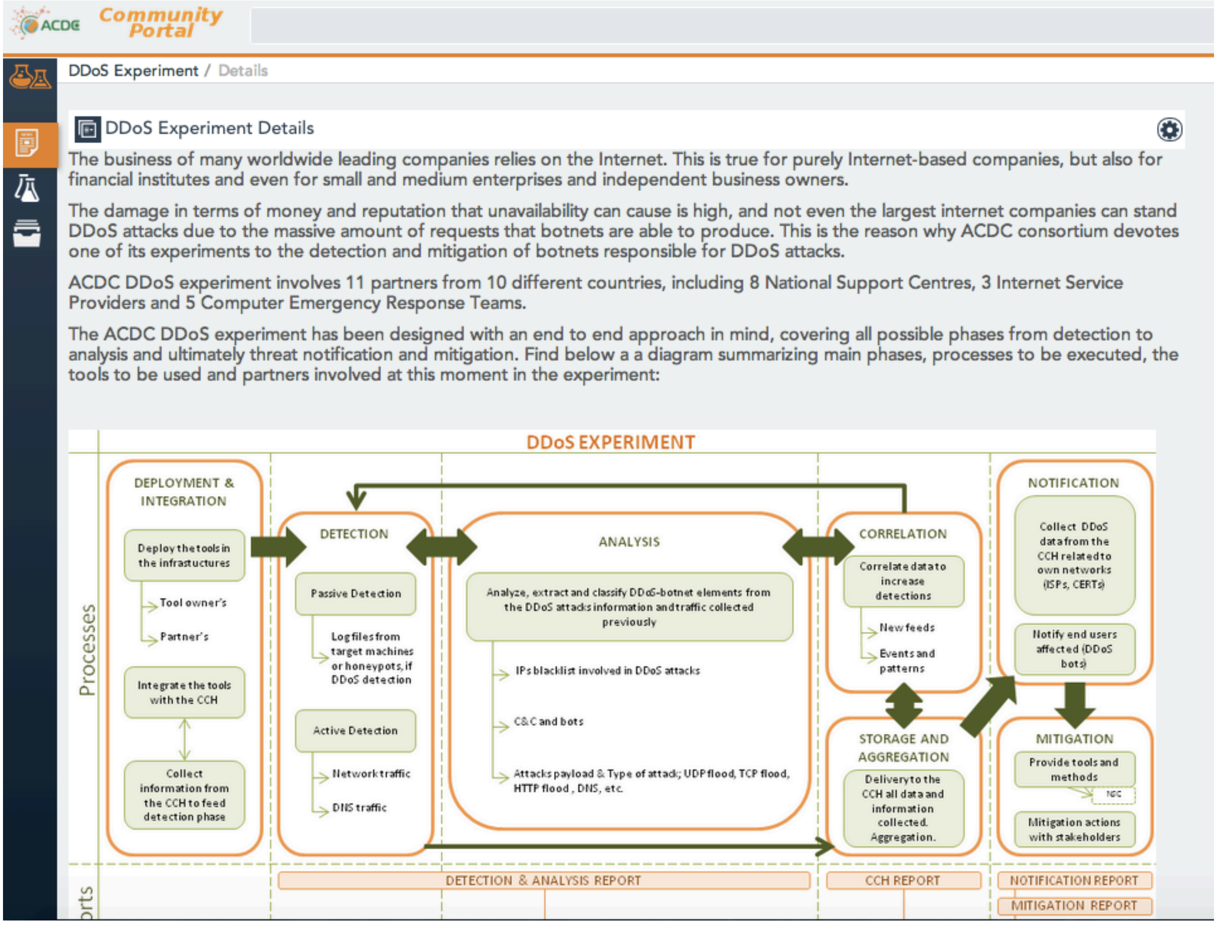
CARIS - Coordinating Attack Response at Internet Scale - Botnets - the Internet Architecture Board (IAB) conference discussions

During the CARIS (Coordinating Attack Response at Internet Scale) workshop in Berlin, June 19th, as part of the FIRST conference the Internet Architecture Board organises a workshop with lightning talks on practical and theoretical aspects of botnet takedowns. Dave Dittrich (Speakeasy) calls for " establishing norms of behavior on the internet, normalize legal procedures and cooperation among international law enforcement, and encouraging the private sector who are being victimized to work together within their respective sectors, as well as bringing evidence to law enforcement and working hand in hand to strengthen the legal system, not bypass it and take matters into the private sector's own hands."
Inspiring papers for practical and policy recommendations and discussion materials https://www.iab.org/activities/workshops/caris/

Figure 6 – ACDC Community Portal Private Environment

Moreover, there were created a number of workspaces, each one dedicated to an experiment, where sets of applications (tasks management, participants list, etc.) are available for the stakeholders who are willing to participate to an experiment. Concretely, the stakeholder is able to:

- test new solutions to fight botnets,
- get access to experiment results.



The business of many worldwide leading companies relies on the Internet. This is true for purely Internet-based companies, but also for financial institutes and even for small and medium enterprises and independent business owners.

The damage in terms of money and reputation that unavailability can cause is high, and not even the largest internet companies can stand DDoS attacks due to the massive amount of requests that botnets are able to produce. This is the reason why ACDC consortium devotes one of its experiments to the detection and mitigation of botnets responsible for DDoS attacks.

ACDC DDoS experiment involves 11 partners from 10 different countries, including 8 National Support Centres, 3 Internet Service Providers and 5 Computer Emergency Response Teams.

The ACDC DDoS experiment has been designed with an end to end approach in mind, covering all possible phases from detection to analysis and ultimately threat notification and mitigation. Find below a a diagram summarizing main phases, processes to be executed, the tools to be used and partners involved at this moment in the experiment:

DDoS EXPERIMENT
Processes
DEPLOYMENT & INTEGRATION
Deploy the tools in the infrastuctures
Tool owner's
Partner's
Integrate the tools with the CCH
Collect information from the CCH to feed detection phase
DETECTION
Passive Detection
Log files from target machines or honeypots, if DDoS detection
Active Detection
Network traffic
DNS traffic
ANALYSIS
Analyze, extract and classify DDoS-botnet elements from the DDoS attacks information and traffic collected previously
IPs blacklist involved in DDoS attacks
C&C and bots
Attacks payload & Type of attack; UDP flood, TCP flood, HTTP flood , DNS, etc.
CORRELATION
Correlate data to increase detections
New feeds
Events and patterns
STORAGE AND AGGREGATION
Delivery to the CCH all data and information collected. Aggregation.
NOTIFICATION
Collect DDoS data from the CCH related to own networks (ISPs, CERTs)
Notify end users affected (DDoS bots)
MITIGATION
Provide tools and methods
NSC
Mitigation actions with stakeholders
orts
DETECTION & ANALYSIS REPORT
CCH REPORT
NOTIFICATION REPORT
MITIGATION REPORT

Figure 7 – DDoS Experiment Workspace

The table below aligns the different needs to the ACDC community portal features; the following section explains the portal features, based on the modelling provided in deliverable D6.3.1.

Fighting botnet needs	ACDC community portal feature
Improving the prevention	*Initiatives*: improving awareness by collecting information about all existing botnet related initiatives *News*: used to announce new events, availability of new solutions etc. *Tools and services:* used to list available tools and services that can be implemented by users to protect against botnets. This section complements the "*experiments*" section, where the focus is more on how these tools and services operate, with specific contexts in which the experiment was run. *Forum*: the place to easily share and discuss information about botnets.
Improving the detection	*Data sharing*: provision and retrieval of data sets provided mainly by ISPs. *News*: providing a fast link to news about botnets, the place to indicate a new botnet detected, increasing the speed of information of users.

	Experiments: the place where community members can ask to join an experiment (usually ISPs, IT providers, researchers) – can find results of an experiments (all community members) – thereby discovering *how* new solutions can help based on a concrete pilot. This is a key difference with the "tools / services" section.
Improve the mitigation	*Downloads:* the section where community members can download solutions to be implemented on their devices. Downloads is supported through the national support centres and the ACDC public website.

Table 4 – linking the ACDC portal features to fighting botnets

More information about the features of the ACDC Community Portal can be found in D6.2.1

4.2.2. ACDC Community Portal Deployment

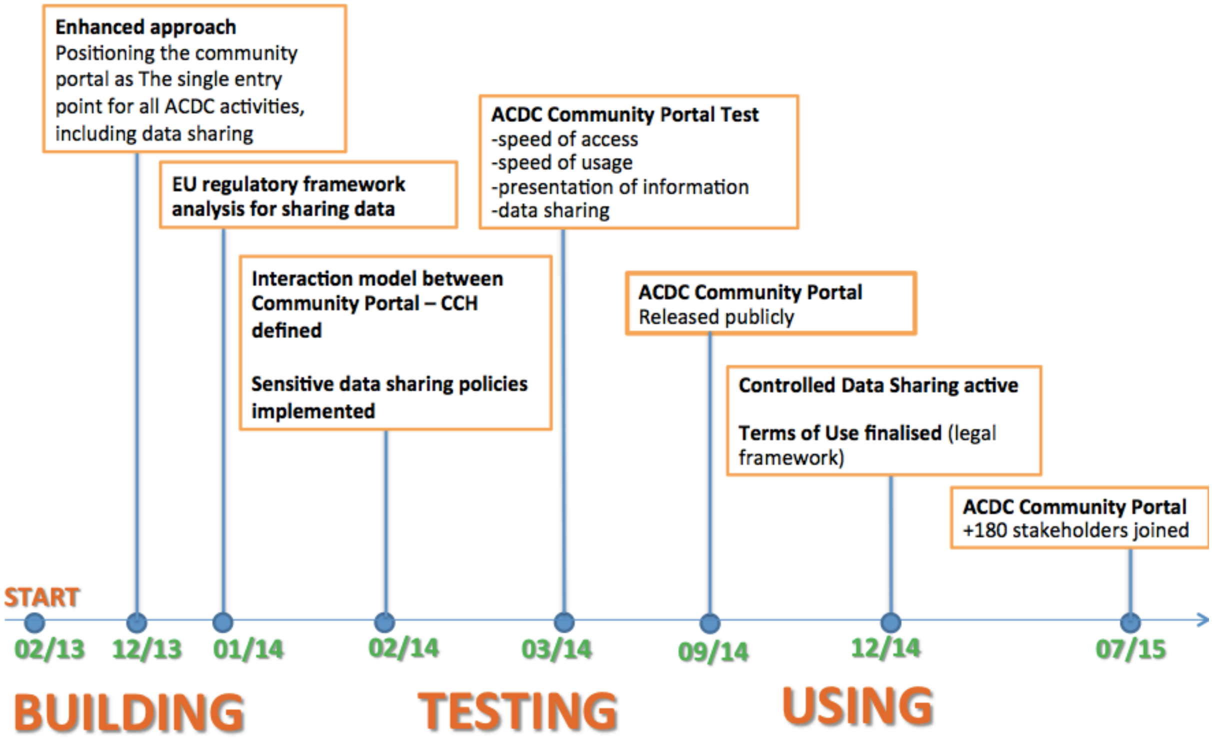

Enhanced approach
Positioning the community portal as The single entry point for all ACDC activities, including data sharing
EU regulatory framework analysis for sharing data
Interaction model between Community Portal – CCH defined
Sensitive data sharing policies implemented
ACDC Community Portal Test
-speed of access
-speed of usage
-presentation of information
-data sharing
ACDC Community Portal
Released publicly
Controlled Data Sharing active
Terms of Use finalised (legal framework)
ACDC Community Portal
+180 stakeholders joined
START
02/13
12/13
01/14
02/14
03/14
09/14
12/14
07/15
BUILDING
TESTING
USING

Figure 8 – ACDC Community Portal Timeline

The ACDC community portal was officially launched publicly during Internet Security Days 2014, an event that gathered pioneers of Internet security, fostering their interaction and collaboration with one another. The goal was to facilitate synergies and discussions around on-going challenges, with a view to fostering new solutions.

The activities related to the launch of the community portal were structured as follows:

- Internal testing of the portal within ACDC: the first release in March 2014 enabled the ACDC consortium to test the portal in terms of functionalities, ease of use and speed and to detect a number of issues solved to present a totally enhanced release for the official launch in

September 2014. The enhancements include: speed of access, speed of usage, presentation of information;

- Launch event organised: the ACDC Community portal was officially launched on the 24th September 2014, with a dedicated announcement during ISD 2014 (day 1, session "Next level of defence – mitigation strategies" taking place at 16:30). The session was moderated by Thorsten Kraft from eco;
- ACDC Community portal presentation: in addition to the announcement, a dedicated presentation was introduced during the same session. This session was presented by Paolo Roccetti from Engineering Ingegneria Informatica, who focused on the interaction opportunities in ACDC using the community portal.
- Press release: a press release was prepared and released by all partners on 24th September 2014 for national releases.

In addition to the activities organised to launch the portal, supporting activities included:

- the inclusion of the updated experiments planning in the ACDC community portal for participation and visibility (WP3);
- the inclusion and links to the list of tools coming from ACDC (WP2);
- the extension of the content presented on the ACDC community.

4.2.3. ACDC Community Portal Support Campaign

The WP6 team has prepared a support campaign in order to increase the visibility of the Community Portal and to animate it. Therefore, the campaign follows two approaches: on the one hand the campaign focuses on how to *increase* the visibility of the Community Portal in order to attract new organisations, and on the other hand the campaign presents several actions that are taken by both, ACDC partners and new organisations, in order to keep the Community Portal alive and *support* the stakeholders joining the community.

In order to increase the visibility of the Community Portal, several actions were implemented through an iterative process:

- sending of one email (and reminders) with a joining invitation to all stakeholders who expressed their interest in ACDC (end of March 2015). The list of stakeholders has been consolidated by the ACDC Partners and includes the contact details of people engaged during the project's dissemination activities;
- publication of promotional messages regarding the Community Portal and the services offered by it through the social media channels, in the ACDC website and in the community portal (public area);
- ACDC Community Portal was presented and promoted during specific events (ISD 2014, CSP Forum 2015, ACDC Bulgarian Conference 2015)

To support this through a consistent approach, WP6 team prepared an email template to highlight the advantages of ACDC Community Portal.

To support stakeholders who joined the community portal, several actions were taken in order to improve his experience on the portal and to optimise the stakeholder experience. Therefore the following actions were taken and repeated with the new stakeholders:

- Sending of a first welcome email with the first information about the portal;
- The new stakeholder was contacted to see if he has already navigated through the portal, his/her specific interest, etc.;
- a short training was made available that can be used whenever it's necessary or requested;

WP6 team prepared a standard welcome email, a standard email that was used one week after the confirmation and materials (documents, tutorials, videos) were created to support the training.

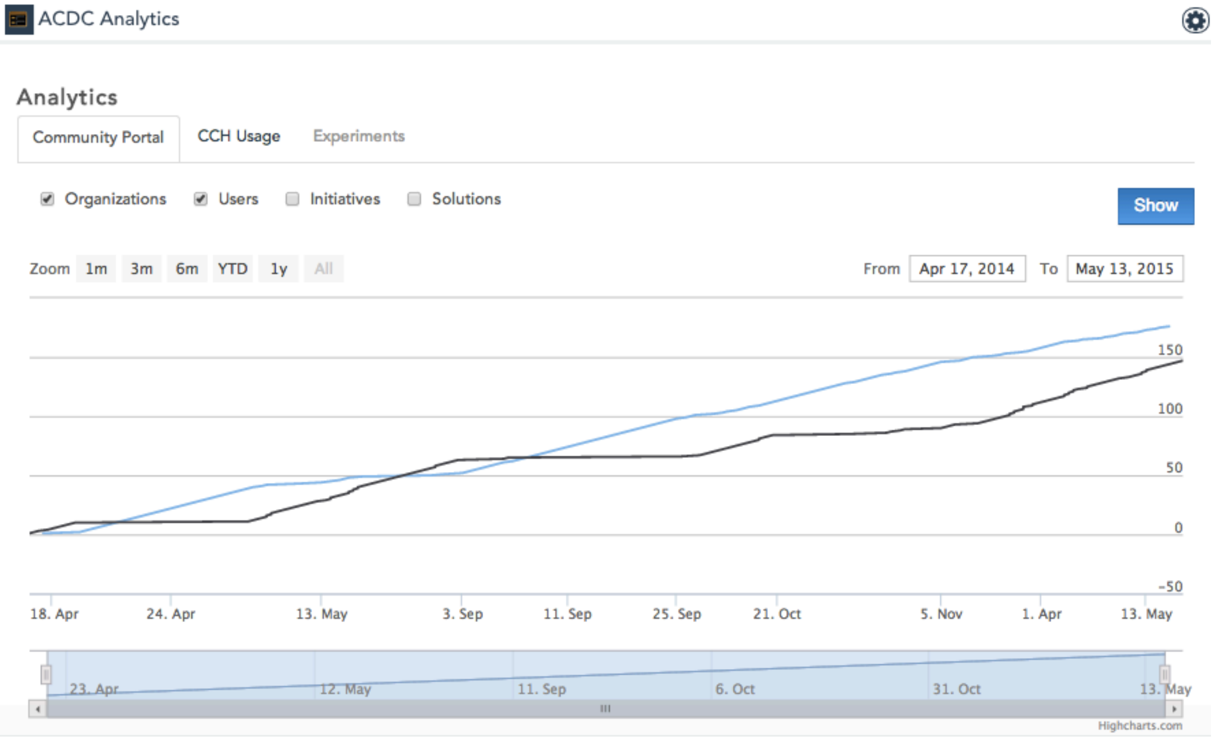
More information about the ACDC Community Portal Support Campaign can be found in D6.3.3.

4.3. Community membership

As mentioned before, ACDC Community Portal was officially launched on the 24th September 2014, with a dedicated announcement during ISD 2014 Event (this followed a previous release in April 2014 open to ACDC partners only).

After less than one year from the official launch, ACDC Community Portal has more than 180 stakeholders and 150 users who joined the portal, actively involved in the activities proposed by ACDC. The figure below shows the evolution of the ACDC Community Portal in terms of joint stakeholders and users. The Support Campaign was launched at the end of March, and as it can be noticed in the figure below, in less then 2 months 50 users joined the ACDC Community Portal.

In analysing these numbers, it is important to note that this represents active participation and a joining process – in line with the fact that the community portal is not a passive Web information site but a participatory web site.



☑ Organizations ☑ Users □ Initiatives □ Solutions

From Apr 17, 2014 To May 13, 2015

Figure 9 – ACDC Community Portal – overview of Users and Organisations

The Announcements section was updated by users with 55 news related to the cyber security area, the ACDC project or on-going botnet attacks. Users can add new announcements or like, follow or comment the announcements already published.

Users added 33 new cyber security and botnets initiatives at national and European level in the **Initiatives section** – showing the value of a "who's who" participation based approach.

The Tool and Services section was updated by the users with 32 tools currently used by them. Users can also add new tools, or evaluate the existing ones or leave a comment.

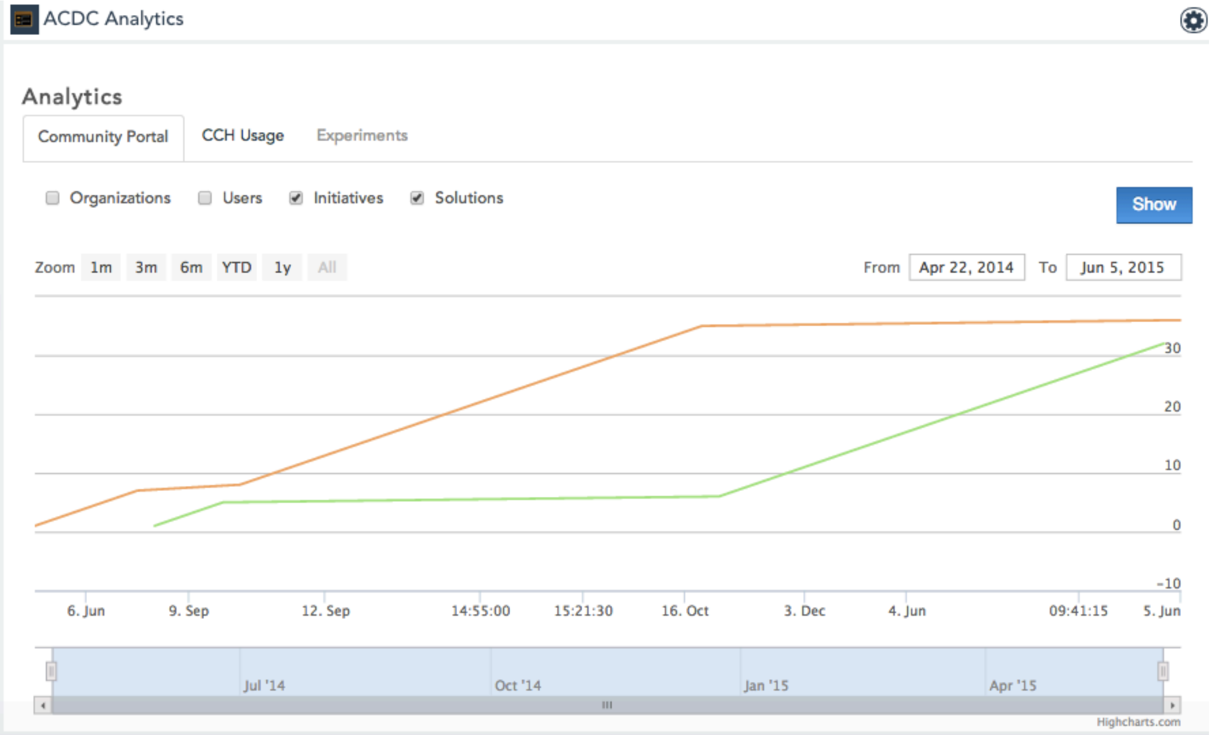


Figure 10 – ACDC Community Portal – overview of Initiatives and Solutions

The ACDC users also utilized The Forum and Documents Sections by proposing new topics, documents and getting involved in discussions. Users can also like, follow or comment the documents already published.
Moreover, both the Document and Forum Sections inside the Experiments Workspaces were extensively used by the stakeholders involved in the experiments, as each dedicated workspace of the ACDC Community Portal was the single environment used to support the interaction between the users and sharing the results. This leads to the conclusion that a community actually happens when there is a **common activity on which to work**, rather than only information sharing.

More information with respect to the social analytics of the ACDC Community Portal can be found in D6.2.2.

During the lifetime of the project, ACDC partners attended more than 200 conferences and events, in order to reach out and encourage stakeholders to get involved in ACDC activities, which were carefully chosen to cover a wide audience across Europe. The full list of events attended by the ACDC partners can be found in Annex.

The events as well as the workshops and the conferences were organised to meet as many representatives of the targeted user profiles as possible, thereby aligning the impact of the communication to the objectives of ACDC.

From the total number of events attended, 54% were at international level, while 46% at national level. *At national level* the main focus was put on participation and visibility of the national support centres, while at *international level* the main focus laid on intensifying outreach and fostering participation.

Besides the workshops and conferences attended by partners, several other individual meetings and calls took place during the 30 months in order to consolidate the interest of stakeholders and to establish concrete activities with them.

Thanks to these common and individual outreach meetings, ACDC partners were able to raise interest from more than 400 stakeholders all over the Europe (detailed under deliverable D6.1.2). The stakeholders' list was used in the ACDC support campaign, where stakeholders were invited to join the Community Portal and actively participate in the activities proposed by ACDC.

As a result of the participative dimension of ACDC, 40 stakeholders signed a letter of interest that enabled them to be actively involved in the ACDC activities. This list is detailed in the following table. Including the 28 partners of ACDC and the 40 additional organisations joining the community, the ACDC community represents different profiles grouped in 6 categories (these have been used also to create the benefits / incentive sections as detailed earlier):

- Policy makers: 4
- Operational (support organisations): 11
- Intermediaries (associations of users and sectorial organisations): 11
- Critical infrastructure operators: 1
- Research facilities: 20
- Solution providers: 21

Period	Organisation Name	Country	Scope	Sector	Cyber security positioning	Context
June 2013	**Europol**	The Netherlands	EU-level		Policy maker / contributor: international bodies and institutions	EC3 meeting
	Dutch Hosting Providers Association (DHPA)	The Netherlands	National-level	Information & Communication Technologies	Intermediaries: focus groups including trade associations	Outreach individual meeting
August 2013	**Tehničko veleučilište u Zagrebu**	Croatia	National-level	Research facilities	Research	Outreach individual meeting
September 2013	**Swiss MELANI**	Switzerland	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	Internet Security Days
	ACM	The Netherlands	National-level		Intermediaries: end users & citizens organisations	Internet Security Days
	NCSC	The Netherlands	National-level		Policy maker / contributor: public authority, national government	Internet Security Days
October 2013	**Croatian Telekom**	Croatia	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	Outreach individual meeting
	Csirt-sk	Slovakia	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	EC3-ENISA meeting
	Avira	Germany	International-level	Information & Communication Technologies	Providers: security solutions	Outreach common meeting

	Cyscon	Germany	National-level	Information & Communication Technologies	Providers: security solutions	Outreach common meeting
November 2013	**F-Secure**	Finland	International-level	Information & Communication Technologies	Providers: security solutions	ICT 2013 Conference
	Industrial Cybersecurity Center	Spain	National-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	ICT 2013 Conference
	University of Granada	Spain	National-level	Research facilities	Research	ICT 2013 Conference
December 2013	**MACCSA**	United Kingdom	International-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	Outreach common meeting
January 2014	**Hasso Plattner Institute**	Germany	National-level	Research facilities	Research	Outreach individual meeting
	Abuse Hub	The Netherlands	National-Level	Information & Communication Technologies	Operational team: national centres on cyber-security / defence	Internet Security Days
February 2014	**Fakultet organizacije i informatike**	Croatia	National-level	Research facilities	Research	Outreach individual meeting
	ZSIS CERT	Croatia	National-Level	Information & Communication Technologies	Operational team: CERT, CSIRT	Outreach individual meeting
April 2014	**Switch - national CERT**	Switzerland	National-Level	Information & Communication Technologies	Operational team: CERT, CSIRT	Interpol European Expert Group on IT crime
	Dante	United Kingdom	EU-Level	Research Facilities	Research	Outreach individual meeting
May 2014	**LINK11**	Germany	National-Level	Information & Communication Technologies	Providers: system integrators	Outreach common meeting
	ACMA	Australia	National-level	Information & Communication Technologies	Policy maker / contributor: public authority, national	Internet Security Days

June 2014	**ECP - Platform voor de InformatieSamenleving**	The Netherlands	National-level	Information & Communication Technologies	Intermediaries: industry associations & sectoral federations	Outreach individual meeting
July 2014	**Information Service Plc**	Bulgaria	National-level	Information & Communication Technologies	Providers: system integrators	Outreach individual meeting
	University of National and World Economy	Bulgaria	National-level	Research facilities	Research	Outreach individual meeting
August 2014	**Financial Services – Information sharing and Analysis Centre**	United States of America	International-level	Financial	Intermediaries: end users & citizens organisations	ECP Conference
September 2014	**CERT-Bulgaria**	Bulgaria	National-level	Information & Communication Technologies	Operational team: CERT, CSIRT	Outreach individual meeting
	POSLUH – Hosting Solutions	Croatia	National-Service	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	Outreach individual meeting
	ITrust Consulting	Luxemburg	National-Service	Information & Communication Technologies	Providers: security solutions	Outreach individual meeting
	The Institute of Mathematics and Informatics – Bulgarian Academy of Science	Bulgaria	National-level	Research facilities	Research	Outreach individual meeting
	National Laboratory of Computer Virology	Bulgaria	National-level	Research facilities	Research	Outreach individual meeting
	Institute of Information and Communication Technologies	Bulgaria	National-level	Research facilities	Research	Outreach individual meeting

October 2014	**Professional Security**	Bulgaria	National-level	Information & Communication Technologies	Providers: security solutions	Outreach individual meeting
December 2014	**Higher School “College of Telecommunications and Post”**	Bulgaria	National-level	Research facilities	Research	Outreach individual meeting
	New Ideas Consult	Bulgaria	National-level	Information & Communication Technologies	Providers: system integrators	Outreach individual meeting
	State Enterprise “National Railway Infrastructure Company”	Bulgaria	National-level	Transport	Critical Infrastructure Operator	Outreach individual meeting
February 2015	**Veliko Tarnovo University**	Bulgaria	National-level	Research facilities	Research	Outreach individual meeting
	National Statistical Institute	Bulgaria	National-level	Research facilities	Research	Outreach individual meeting
April 2015	**Telenor**	Bulgaria	National-level	Information & Communication Technologies	Providers: Internet Service Providers (ISPs)	Outreach individual meeting

Table 5 – LoI signed

5. The participation of the ACDC community to the support level

Key results – 10 centres operating across 10 Member States

- ✓ 1 European Support Centre platform
- ✓ 1 ACDC National Support Centre model fully defined
- ✓ 8 centres created as initially defined in ACDC's project description of work
- ✓ ACDC National Support Centre model fully tested through the creation of 2 centres in addition to the original 8

The ACDC community has and is delivering the support dimension through

- **a central support facility** providing access to tools from different providers
- **an information sharing facility** to speed up the detection of botnets through enhanced and enlarged sharing and feeding the central support facility with early information. This is the Central Clearing House.
- **a model for national / local support facilities channelling the resources from the central support facility to end-users and organisations,** localising support closer to users in terms of language, support and needs
- **10 local facilities across 10 different countries,** testing and further refining the model.

Within the context of this deliverable, the key results related to the "community" dimension includes the support facilities, both as a model ready to be taken up by other organisations not yet involved and as the currently operating centres deployed across 10 countries. These are further detailed in the following pages.

The ACDC project included the aim to provide end-to-end protection and a set of services to protect users from botnets. One of the project goals was the provision of eight National Anti-Botnet Support Centres (NSC) across Europe - dedicated support services to End Users, including Small-and Medium Enterprises. Support services are of course also available to larger organisations, but have been designed with **a target of non expert users in mind**.

During the lifetime of the project ACDC deployed 1 European Support Centre, which provides a first contact for end-users. The platform then either points users to national support centres or takes over the role as an active support centre for Members States that do not run a national support centre. A valuable role of the platform is also to coordinate the relationship between the participating national support centres and to channel news and new solutions to each of the centres.

ACDC has successfully deployed the foreseen 8 National Support Centres (Belgium, Croatia, France, Germany, Italy, Portugal, Romania, Spain) and 2 additional ones in Bulgaria and Luxemburg.

The National Support Centres provide an easy, efficient solution for end user support especially for large-scale incidents, providing its own constituency with access to the different ACDC solutions to fight botnets, along with awareness and prevention coaching and free tools.

5.1. Standard requirements for operating a National Support Centre

The standard requirement addresses **what** the National Support Centre has to set up as a minimum set of features.

The primary purpose of a national support centre (NSC) is to reduce the number of botnet-infected computers in the operating country, educate users on the subject of Internet security, and provide assistance removing malicious botnet software from an infected end-device.

The target group of a NSC are end-users, same as small-and medium size enterprises. Services to these groups need to be free of charge.

National support centres participating in the ACDC-Project are fully independent entities. Each operator can decide based on available budget and other resources, which service level his NSC can provide, selecting these from the definition of services provided by ACDC.

The ACDC Support Centre Task Group has defined a set of minimal requirements that a provider needs to fulfil to comply as a national anti-botnet support centre under the ACDC brand.

The standards requirements for operating a NSC set out a clear set of rules that help providers quickly evaluate and identify which set / subset of ACDC services they have to commit to qualify as an ACDC support centre. This process has eased the outreach of ACDC and its value has been demonstrated already during the project lifetime by the creation of ACDC support centres in Bulgaria and Luxemburg that were not foreseen in the Description of Work.

Operator

The operator of a National Support Centre does not need to be a consortium member of the ACDC project, but needs to be an entity based in the country that the NSC is dedicated to.

As an example, a German organisation is not entitled to run a National Support Centre is Austria.

Languages

The website of a National Support Centre must be available in (all) the official language(s) spoken in the hosting country. An English version is not mandatory, but recommended.

Service level

The minimal requirement for the service of a National Support Centre is a static website.

Each National Support Centre must provide an option to contact the operating organisation and the responses need to handled in a timely manner.

Additional levels of technical support provided by a NSC are not compulsory, each organisation must decide which services it can provide based on its available budget and funding.

Further activities in social media, the availability of a support forum, a blog and further activities are appreciated, but not compulsory. It is recommended that NSCs use the synergies of other National Support Centres, e.g. by linking to available international support forums, blogs or social media accounts.

Branding

A National Support Centre needs to display the ACDC Logo and a link to the project website on its main website. Displaying the logo and the link on other subpages is appreciated, but not mandatory. Besides that, each National Support Centre has the right to implement its own design and layout.

It is recommended to host the NSC on its own domain and the national top-level domain. The domain name of the national support centre is not compulsory, but it is recommended following the naming convention of ***.botfree.***, ***.antibot.*** or localised variations.

Content

A NSC should apply a terminology, wording and language that are understandable by its target customer/visitor group. Information displayed on a NSC should include general information about botnets and should ideally also address other common and related IT-security threats like Phishing.

The website of a NSC should also include basic advice how to protect a computer device and how to “stay safe” on the Internet. This particularly includes the advice of the regular installation of updates and patches to tools, browser, plugins, apps or the operating system, the usage of security tools like an Anti-Virus product and a firewall.

The website of a NSC must provide guidance, help and assisting information that a user needs to take in case of an infection with Malware, Trojan or other security threats. This can include their own support services; own cleaning or removal tools, reference to other National Support Centres or links to external services that provide helpful information, services or tools.

Tools
All provided dissemination tools that are displayed, hosted or linked on the website of a NSC need to be free of charge. Useful tools developed or provided as part of the work of the ACDC project, should be displayed on the website of the NSC. Organisations are entitled to promote commercial tools, but these need to labelled accordingly and separated from the free of charge tools.

External Links
A national support centre should provide a strong and comprehensive directory of security websites, covering all areas of Internet security, privacy etc. The links may be marked with affiliate programs to additional funding of the NSC; the same option applies to sponsored ads. Any placed Ads on botfree.eu needs to be related to the aims of the ACDC-project with a clear focus on security related advertisement, brands and products. This section needs to be separated from free-tools and the EU cleaners.

Data Protection, Privacy & Terms of Use
A National Support Centre must to comply with data privacy standards based on National and EU directives. A data privacy statement and the terms of use must to displayed on the website of each NSC. Recommended, provided, promoted or linked tools need to be compliant with common data standards. A contact address needs to be provided.

Security
A National Support Centre needs to apply the highest security standards to its services. This includes the security of the website itself, same as all associated services, tools or plugins.
Unrestricted access to personal data by a third party must be safeguarded at any time. A penetration test or security audit/certification is recommended, but not mandatory.

5.2. Operating recommendations for a National Support Centre

The operating recommendations address **how** the National Support Centre can operate additional services. This differs from the requirements introduced in the previous section, as each national support centre will be able to decide based on its funding **how to setup** their service level for a national support centre. The options below are therefore recommendations on how to extend the service in addition to the required availability of a static website.

Accessibility
With the increasing number of mobile and tablet users, the service of a National Support Centre should also provide service to mobile users and not only to desktop PCs. Therefore, it is highly recommended that the website be customized for mobile access. The website of a NSC should also be optimized for search engines to achieve a high ranking in searches related to IT Security, Botnets and other relevant issues.

Email Support
Support by email should be handled through a central help desk system. Privacy needs to be in line with national regulations. Responses should be made in a timely manner, staffing adapted to the service volume. Staff of a NSC needs to have the appropriate technical skills and the ability to explain issues at the experience level of the basic end-users.
User should always receive a confirmation for their support request, providing tickets numbers to customers is recommended. The usage of standard templates for common requests is useful.

Telephone Support

The costs a phone call should not exceed the costs of a local call, ideally toll-free numbers should be made available.

A service during regular business hours/days mainly addresses small-and medium size enterprise customers, whereby end-users tend to address possible Malware removals after work or at the weekends. Each NSC should properly weigh in its operational telephone support time based on his target group and available budget, as especially support services outside the regular business or weekends correlate with additional costs.

Support-Forum / WIKI / FAQ

The operation of a support forum, a sophisticated wiki-system or other knowledge repository and a list of the Frequently Asked Questions will help keeping the efforts and costs for phone and email support at an adequate level.

A support forum needs to be living forum, so it is recommended to work with volunteers that actively contribute to the forum as well.

Support through Social Media

Support through social media should be taken into consideration, too, but the recommendation is to use these social channels just for the first contact. Advanced support should be provided by regular systems as phone, forum or email only.

Tools and Services

It is recommended that all promoted or provided tools should be presented along with a detailed tutorial and screenshots on the website.

The portfolio of tools should include specific threat-related removal tools, tools for general detection and analysis, same as additional tools for maintenance like for backups.

Based on the current threat landscape, the NSC should set their focus on the Microsoft Windows for desktops and Android for the mobile area. Support to other operating system should not be kept aside, but can play a minor role.

Local collaborations

A National Support Centre is encouraged to collaborate with the national ISPs, CERTs, government, industry, media and other stakeholders to receive a good visibility. A proactive outreach is recommended, and regular joint campaigns and initiatives desired. Dissemination towards the stakeholder groups like presentation at conferences gives a good visibility, too.

Online animation through Blogs & Social Media

It is recommended to provide a blog with recent activities of the National Support Centre, updates on IT-Security topics like urgent threat alerts, tool reviews and general information how to stay safe on the internet. This service should be included in the support centre website and content should be regularly maintained.

It is also helpful to be actively present on common social media platforms like Facebook, Twitter or YouTube. Activities can be either linked to the blog directly or maintained independently with additional content. A combination of a blog and social media channels ensure high visibility towards end-users.

Dedicated campaigns

In case of a campaign related to a specific Malware, Ransomware or Trojans with a high visibility in press or media, dedicated landing pages addressing a specific topic in more details is recommended. NSCs can decide to run campaigns aligned to the ones launched centrally by ACDC or launch additional campaigns linked to specific events taking place at national level.

More information about standards requirements and recommendations regarding the National Support Centres can be found D1.3.2.

5.3. Overview of the National Support Centres available

The table below, first published in D6.3.1, presents the overview and current status of the all National Support Centres deployed, 10 in total. The “Operator” column describes the actual organisation involved.

Analysing the profile of organisations operating ACDC NSCs, the table highlights that

- 3 centres are run by a CERT
- 2 centres are run by an academic partner
- 1 centres are run by a public administration
- 4 centres are run by a private organisation

Country	Operated	Overview	Website	Status
Pan-European Support Centre platform	ECO e.V.	The platform provides a first contact for end-users. It either points users to national support centres or takes over the role as an active support centre for Members States that do not run a national support centre. Its role is also to coordinate the relationship between the participating national support centres.	www.botfree.eu	Operating
Germany	ECO e.V.	The German Support Centre provides a centralized point of help/support for end-users. Support activities include phone and email, plus a user forum. The website is focussed on Information, Dissemination & Prevention.	www.botfrei.de	Operating
Belgium	LSEC	Provides a centralized point of information for business and end-users. Support activities include background and practical information in Dutch, French and English, and a series of mitigation tools and a user forum. Central is the website tool, focussed on Information, Awareness Creation and Prevention. The platform is intended to act as a central hub for citizens who are looking for 1st line support, background information, basic advice and key contacts for assistance in case of an incident likely to do with cyber security threats. The citizen or user will be guided through several steps, being indicated how technical solutions could be of assistance, both in mitigation and prevention. The Belgian national support centre aims to be a sustainable support centre, and a broad cyber security platform for end users (citizens). The Belgian Support Centre: • Creates awareness on IT and cyber security issues • Provides information about relevant risks, threats and infections, and how to prevent- counter measure / remediate from them • Provides access to tools, videos, documentation etc., all to support end users • Coordinates online and offline cyber security prevention campaigns in	www.botvrij.be www.sansbot.org	Operating

		Belgium • Becomes a 1st level support for cyber incidents with citizens and end users, a neutral platform, operator independent • Provides a controlled, visible interactive update on cyber threats, incidents, vulnerabilities, indicating the level of threat and creating awareness • Provides a central intelligence collective, a CCH-alike on a local basis for both professionals and individuals, maintaining and reporting on recent attacks and acting as a local information sharing relay.. • As the single point of contact for the international collaboration of support center activities, capable of organizing a CiSERT type of platform that transmits intelligence works. The Support Center will build relationships with 3rd parties, government, ISPs, telecom, critical infrastructure providers and other operators, experts from the security-industry and other organizations that are willing to support the ACDC NSC approach by means of added value content and functionality, visibility and eventually (leading to) financial contributions in order to create and maintain a sustainable platform that helps end users to protect their systems and information.		
Spain	INCIBE	The Spain Support Centre's main services are: • News: real histories, blog, security alerts, security newsletters. • Security knowledge tests for end users. • Security general information: malware, fraud, social networks, devices, networks, etc. • Security tools (free). • Support for end-users (email, forum, phone) • AntiBotnet Service.	www.osi.es	Operating
Croatia	CARnet	The Croatian Support Centre provides a centralized point of help/support for end-users. Support activities include email, plus blog and user comments. The website is focused on Information, Dissemination & Prevention. The web portal provides links to various antivirus	www.antibot.hr	Operating

		tools and online scanners. The portal also provides a link to document discussing botnets and is interlinked with the National CERT portal www.cert.hr The portal also automatically publishes spam campaigns and malware names distributed by spam every day.		
Romania	CERT-RO	The Romanian Support Centre provides a centralized point of help/support for end-users. Support activities include: • Inform section: general information about botnets; • Clean section: tutorials and security tools, which help users, remove a botnet infection. Support for end users (email, phone); • Protect section: alerts, news, articles and security tools; • Spam reporting center: consumers, businesses and other organizations are able to report commercial electronic messages sent without consent and/or commercial electronic messages with false or misleading content. The website is focussed on Information, Dissemination & Prevention.	www.botfree.ro	Operating
Italy	ISCTI	The Italian Support Centre provides a centralized point of help for end-users at national level. The website focuses on Information, Dissemination & Prevention. It also provides links to third-party detection and disinfection tools. The design and IT support was provided by Engineering Ingegneria Informatica. In the first phase of its operation it focuses on publication of general information for protection against botnets and collection of alerts from citizens and from the ACDC community. In the subsequent phase it will include additional interactive services (e.g. forum).	www.antibot.it	Operating
Portugal	FCCN	The Portuguese Support Centre provides a centralized point of information, help and support for end-users. Its management will be ensured by cert.pt. Its services are: • News/ Inform section: Security alerts,	www.antibot.pt	Operating

		• Clean section: Security tools and Support for end users by email; Protect section: Articles, Tips, Security general information, recommendations.		
France	CECyF SignalSPAM	The French Support Centre provides different level of information and tools regarding : • Awareness • Protection • Mitigation / Devices cleaning Partners involved in tackling botnets and protecting users.	www.antibot.fr	Operating
Bulgaria	Bulgarian CERT	The NSC in Bulgaria is currently available in Bulgarian only. The website is a translation and customization of the German ABBZ website, project partner ECO supported the Bulgarian CERT in setting up this service. The Bulgarian CERT is currently working with several National Internet Service Providers in establishing processes and services similar to Germany, involving and notifying end-users and SME's.	www.antibot.bg	Operating
Luxemburg	UNI.LU CIRCL BEE SECURE	The NSC in Luxemburg is currently available in English. The Centre provides different levels of information and tools in order to create awareness, protection and mitigation. The website is a translation and customization of the German ABBZ website.	www.botfree.lu	Operating

Table 6 – NSC status

5.4. Services offered by each National Support Centre

The table below presents the main info regarding each NSC deployed by the ACDC Partners (operator, website, status) and the services offered by each one of it.

Country	Operator	Website	Status	Available Services						
				Email-Support	Phone-Support	Blog	Social Media	Forum	Software availabl for download	Others

Germany	eco e.V.	www.botfrei.de	September 2010	Yes	Yes	Yes	Twitter, Facebook, Google Plus	Yes	Yes	
Belgium	LSEC	www.botvrij.be www.sansbot.org	March 2014	Yes	No	In course of 2015	Twitter	In course of 2015	Yes	Interactive maps, dynamic listing
France	SignalSpam CECyF	www.antibot.fr	October 2014	No	No	Yes	Twitter	No	Yes	
Italy	ISCTI	www.antibot.it	September 2014	No	No	No	No	No	No	General information page on botnet and specific information on how to check and remove botnet infections Links to free tools for check& clean As National CERT - notification of incident reports to Italian ISPs
Spain	INCIBE	www.osi.es Antibotnet specific section: http://www.osi.es/servicio-antibotnet	June 2014	Yes	Yes	Yes	Facebook, Twitter, Google Plus, Tuenti, RSS, Youtube	Yes	Yes	Anti-botnet service online: check connection and check code
Croatia	CARNet	www.antibot.hr	April 2014	Yes	Yes	Yes	Twitter	No	Yes	Publishing current list of spam campaigns and spam containing malicious URLs and attachments
Romania	CERT.ro	www.botfree.ro	February 2014	Yes	Yes	No	Yes	No	Yes	
Portugal	FCCN	www.antibot.pt	December 2014	Yes	No	No	No	No	Yes	On a daily basis is placed in site the most active malware collected by CCH

Table 7 – NSCs services

5.5. Usage level of the operating ACDC NSCs

The table below shows the end users involvement to each NSC, based on the services offered by them.

National Support Centre	Statistics

Country	Operator	Total visitors 01/09/14 – 30/06/15	Average Website visits per day?	Total Software downloads	Average emails/ month	Average calls/ month	Total followers on Social Media	Total news on blog
Germany	eco e.V.	1.280.400	4.240	177.095	217	76	9.689	188
France	SignalSpam CECyF	4628	15	NA	NA	NA	281 (1540 consultation on Google+)	NA
Italy	ISCTI	2510	9	63[2]	>120.000 [3]	NA	NA	NA
Spain	INCIBE	Global site: 1.299.340 Antibotnet section: 59.781 Source Google Analytics	9.860 Source Google Analytics	Plugin Antibotnet installations: 9.229 Conan Mobile installations: 47.416 Total Visits to Free Tools page 01/09/2014 – 30/06/2014: 192.533 (http://www.osi.es/es/herramientas-gratuitas) Source Google Analytics	135	367	Facebook: 30.879 Twitter: 15.858 Google +: 1.103 Youtube: 1.461	Blog: 423 Security Alerts: 414 Real stories: 28
Croatia	CARNet	35.317	117	9685	100	NA	NA	93
Romania	CERT.RO	5376	17,34	476	60	10	621	NA
Portugal	FCCN	2117 (since 01/12/14)	15	We don't have these values	0	NA	NA	NA

Table 8 – End users involvement

[2] Access to pages for disinfection tool downloads.

[3] Notification of incidents retrieved from CCH to Italian ISPs during WP3 experiment campaign.

6. Participation of the user community to the technical level

As described in the introduction to this deliverable, the technical level is provided mainly through

- provision of tools and solutions: this was the focus of WP2
- running experiments addressing a specific user need (DDOS attack, mobile devices protection etc) through a unique combination of different solutions: this was the focus of WP3

Whilst these activities are fully reported in the respective deliverables of each work package, the community dimension of these activities is integrated in this document.

Of particular relevance:

- **22 organisations provided 61 tools and solutions**. The community role was to a) provide a channel of visibility and uptake for new tools, solutions and research results, b) provide a link to ease the assessment by users of both open-source and commercial tools. As described in the previous page, a dedicated section of the online community portal supported this activity.
- **13 organisations participated across 5 types of experiments**. The community role was to a) ease the consolidation of the actual needs addressed by an experiment through online discussion, b) ease the participation of IT providers and researchers to an experiment, c) allow members of the ACDC community (beyond the ACDC partners) to indicate interest in either participating or remaining informed of the results of an experiment. As described in the previous page, a dedicated section of the online community portal supported this activity.

7. Participation of the community to the data level

As described in the introduction to this deliverable, the data level is provided mainly through the Central Clearing House (CCH) and the associated data access policies handled under the regulatory level (see next section). Whilst these activities are fully reported in the respective deliverables of WP1, the community dimension of these activities is integrated in this document.

And this is one domain where the community dimension has and is playing a fundamental role. Indeed, the initial idea of ACDC was on the one hand to animate a community built essentially sharing knowledge, and on the other hand to share data using a dedicated infrastructure. However, one of the earliest evolution chosen by the ACDC partners was to merge these two activities into a single environment – having in mind that the evolution of the ACDC community **should scale up** to more members with secure and comprehensive access to data sharing built in from the start.

This led to the **enhanced community portal** and the creation of the Data Access Manager, allowing community members to request access to and from the Central Clearing House through the community portal itself.
In this context, the community dimension played a key role in making the CCH more accessible, supporting the implementation of data access policies (see the "regulatory level" section) and allowing community members to not only access but also communicate and detect the availability of data from data providers.

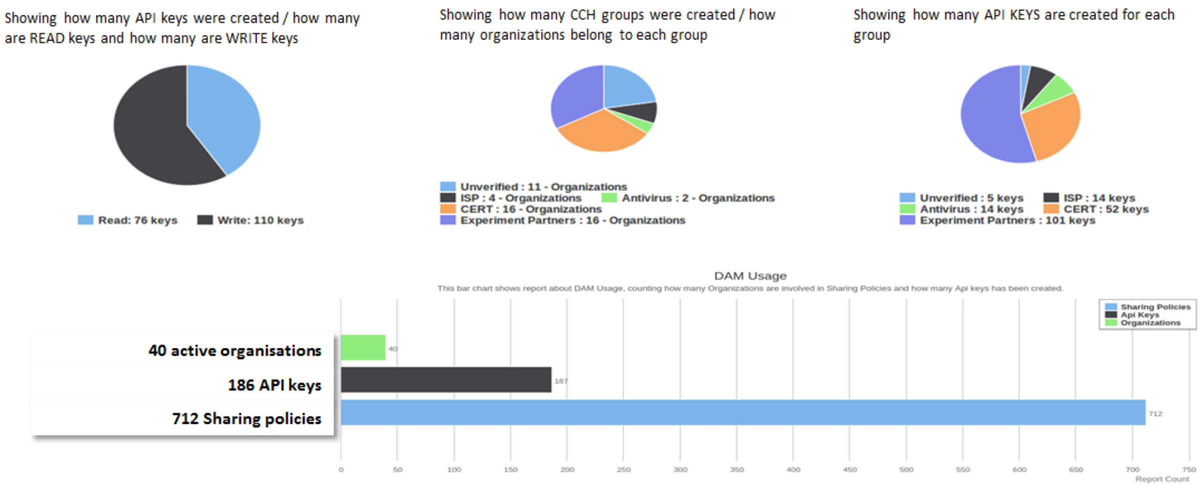


Figure 11 - DAM Statistics overview

The above figure shows the DAM overall numbers at the beginning of September 2015 (end of the ACDC project). In the pie graph on the top left can be noticed that a majority of the keys was used to report data to the CCH (110 keys) compared to the number of keys used to read data to the CCH (76 keys). This is in line with the approach proposed by the ACDC project, seeing a potentially large set of reporting organizations, compared to the number of those able to analyse the data and correlate them. Also, as from the diagram the most represented groups in data sharing are CERTs (16 Organizations). The *Experiment Partners* group was created to group all ACDC partners sharing data that were not falling in the other groups. The *Unverified* group has also a high percentage, it is meant to contain the organisations that are not yet trusted enough to be moved to a different group (organisations that are in the Unverified Group cannot create read keys, thus they cannot access data, only provide them to the CCH). The third pie chart on the top right shows the number of keys created by each group. Reasonably, a vast majority of keys were created by the Experiment Partners group (to run ACDC experiments), followed by the CERT group (52 keys) and ISP & Antivirus groups (14 keys each).

Another contribution of the community approach to the data level is the "botnet metrics", a feature of the community that essentially provides understandable statistics and analysis (on a country per country, per type of attack etc.) from shared data. This role is a key contribution in making complex information accessible to non-technically expert users – a fundamental role given the variety of profiles in the ACDC community.

8. Participation of the community to the regulatory level

ACDC was a technically driven pilot, demonstrating the usefulness of collaborating at different levels. At the same time, it included a strong data sharing component, which built on the legal expertise of partner KUL and its valuable study of how can data be legally shared across Member States (refer to WP1).
This work in turn guided the practical approach to define and implementing data sharing policies, a work that has been reported under the WP1 deliverables.

In this dimension, the community role was and is very important in creating **practical** and **viable** solutions to data sharing, based on the experiences of providers of data and the interest of users of data, such as researchers.

Data sharing has been put in place using a bottom- up approach, and access and configuration of the policies have been done through the community portal.

9. Lessons learned

Lessons learned

- ✓ A community happens when there is a common activity on which to work together and for which there is a clear added value in sharing this work
- ✓ A community portal requires pro-active animation leaders
- ✓ ACDC Community portal link to the DAM is an effective way of supporting an evolutive model for sharing of sensitive data
- ✓ Building trust in a community portal requires a bottom-up approach
- ✓ Experiments are useful in involving different providers into a single activity but are costly
- ✓ ACDC Community Portal delivers value in connecting CERTs together
- ✓ Setting out a clear set of rules for National Support Centres helps pre-existing support structures to quickly evaluate and identify which set / subset of ACDC services they have to commit to qualify as an ACDC support centre.

The implementation of the WP5 and WP6 activities put forward several aspects that are relevant for the Community, its establishment and its functioning. Therefore, this section summarizes the main findings in terms of lessons learned that came out during the 30 months of the project:

1. Concrete activities in a community actually happen when there is a common activity on which to work, beyond information sharing. This means that in order to create and consolidate a community, the main challenge is to identify the common activity that is of high interest for all members of the community – this is also a key opportunity, meaning that creating a community starting from concrete activities is a tested approach;

2. Community portal requires pro-active animation leaders, meaning that each section has to be monitored and in some cases fed by dedicated individuals that monitor the content to avoid problems and update it to provide/ initiate continuity;

3. Community portal link to the Data Access Manager (DAM – link between the community portal and the CCH) is an effective way of supporting an evolutive model for sharing of sensitive data. One important value of the "evolutive" dimension is that it supported first bilateral sharing, and then progressively implemented profile based sharing and is now ready for future evolutions of sharing with a sub-set of organisations;

4. Building on point 3, the community portal approach is a valuable element in contributing to **building trust in a bottom-up approach** that allows smaller groups to work together on very focused activities (for instance one experiment) and then expand out to other groups once they are in the habit of working together. In the context of cyber space this is an important contribution;

5. Creation of benefits oriented incentive pages that target a variety of profiles is an important point in **personalising the experience** and value of participating to a community;

6. The activity regarding the experiments is a mechanism that is useful to involve different providers into a single activity BUT is costly in terms of setting up and monitoring. This leads to the conclusion that a more flexible engagement mechanism should be analysed;

7. In a context where ISPs are confronted with high costs of supporting end-users facing cyber attacks, the ACDC community portal delivers value in connecting the intermediary supporting structures (aka CERTs) together to ensure that when different countries face similar attacks, CERTs have the same information at their disposal and can use this to reach out to end-users. This takes advantage of the multiplying effect of CERTs, guarantees a higher quality in the content and

consistency of the information channelled to end users whilst at the same time decreasing the cost for individual ISPs;

8. The standards requirements for operating a NSC set out a clear set of rules that help pre-existing support structures to quickly evaluate and identify which set / subset of ACDC services they have to commit to qualify as an ACDC support centre. This process has eased the outreach of ACDC and its value has been demonstrated already during the project lifetime by the creation of ACDC support centres in Bulgaria and Luxemburg that were not foreseen in the Description of Work.

10. Beyond the ACDC Community Portal

ACDC Community value

- ✓ High visibility (+200 events attended)
- ✓ Significant support demonstrated by stakeholders through the Letter of interest (+40)
- ✓ Relevant number of stakeholders joined the ACDC Community Portal (+180)
- ✓ The social activity run into the community portal and particular in the experiments section

The value earned by the participants who joined the ACDC community is also the result of the successful community portal experience.

These results show the interest of the targeted, and operationally involved, stakeholders in being part in the ACDC community.
During the 30 months of the project, ACDC managed to create through the community portal, a concrete interest for SMEs, policy makers, other support centres, and users, to actually *stay in* the community. Specifically,

- SMEs, often unable to get the information needed to start prompt reactions against the cyber threats they face as well as to get a complete understanding of cyber security – needed to activate proper countermeasures in line with a sane cyber security strategy- may find in the ACDC community portal an invaluable source of *information*
- Policy makers interested in the *lessons learnt* got from the ACDC experiments run to test data sharing scenarios;
- Support Centres, benefit from the ACDC infrastructure linking to the ACDC CCH, *providing solutions* to fighting against botnets and *support* to early detection.
- Users get the advantage of receiving proper *education* by the Support Centre on the subject of Internet Security.

As such the results achieved during the project lifetime, go beyond the ACDC community itself, intended as a project-community, and are considered as relevant also for a wider group of stakeholders joining together, not only with the focus of fighting against botnets but also interested in a larger scope that fix the focus on cyber security.

ACDC added value to the cyber ecosystem

- ✓ The knowledge on the subject of botnet produced during the project lifetime
- ✓ A consolidated community (+400 stakeholders group interested and +180 active on ACDC Community Portal)
- ✓ Access to CCH, through a “sharing policies” approach (sharing data bilaterally with an identified organisation, profile of users etc.)

The objective is therefore to migrate all the knowledge produced in the ACDC Community portal by users’ interaction to the self-sustainable environment to sustain the **single-access point, cyber eco-system** supporting and fostering concrete **collaborative actions between stakeholders who will then** increase their level of protection against cyber-disruptions, being part of a **European network** of individuals and organisations.

By combining the ACDC value with a wider offer in terms of knowledge and by designing new forms of collaboration in a larger community, users will be provided with a more complete solution (portal). Finally, providing users with a single access point to the overall “cyber security knowledge”, will improve their customer experience and will therefore generate an increase in terms of customer engagement and satisfaction. The community, which started with the focus of botnet in ACDC, is therefore expected to grow.

11. Annex – list of events attended

The list of 200 events attended by ACDC during the lifetime of the project highlights how the outreach was organised to reach out to the full list of profiles identified as relevant to the ACDC community.
Analysis of the events show that the events were targeted to different profiles of audiences, fully aligned with the community approach of ACDC.

Event	**Main Leader/ACDC Partner**	**Start date**	**End date**	**Type of audience**	**Web site**
CPDP Conference	LSEC	25/01/13	27/01/13	research, industry, government	www.cpdp.org
Computer Privacy and Data Protection Seminar	LSEC	07/02/13	07/02/13	Business	www.lsec.be
M3AAWG General Meeting	ECO	18/02/13	21/02/13	Audience of specialists	http://www.maawg.org/events/upcoming_meetings
RSA Conference	LSEC	26/02/13	01/03/13	Business	
Security Innovation Forum	MI	26/02/13	26/02/13	IT specialists	
CeBIT 2013 Conference	ECO	05/03/13	06/03/13	General audience	http://www.cebit.de/home
ICST 2013 Conference	MI	18/03/13	21/03/13	public and private IT specialists	
Cyber Crime & Cyber Terrorism Roundtable	CyDef	08/04/13	09/04/13	Financial Services	http://www.archimedes-eu.eu/mailings/roundtable3_280213.html
LAP spring 2013	ECO	16/04/13	16/04/13	research, industry, government	icpen.org
ECO Kongress	ECO	17/04/13	17/04/13	general audience	Eco.de
Trust in the digital world Conference	ECO	18/04/13	19/04/13	Industry, military, public agencies	www.eema.org
APWG Conference	MI, CyDef	23/04/13	25/04/13	IT specialists	http://www.apwg.org/apwg-events/cecos2013
European Cyber Security Conference	TEC	16/05/13	16/05/13	IT specialists	http://www.eu-ems.com/summary.asp?event_id=146&page_id=1219
TERENA TF-CSIRT	CARNet	23/05/13	24/05/13	European CERT representatives	https://www.terena.org/events/details.php?event_id=2448
RCIS Conference	MI	31/05/13	31/05/13	It specialists	http://rcis-conf.com/rcis2013/document/RCIS2013IndustrialDayProgram.doc
MAAWG Conference	ECO/B-CCENTRE-KUL	04/06/13	06/06/13	Industry, military, public agencies	http://www.maawg.org
ICT Compliance & Security workshop	TI-IT	06/06/13	06/06/13	It specialists	http://www.osservatori.net/home
Cyber Intelligence Workshop	LSEC	29/08/13	30/08/13	research, industry, government	http://www.iipvv.nl/nl/

					content/veldraadplegin g-ncsra-ii
LSEC – Agoria ICT eHealth Workshop	LSEC	12/09/13	12/09/13	research, industry, government	
NIAS 2013 – Nato Information Assurance symposium	LSEC	12/09/13	14/09/13	business& government	
APWG Conference	ECO	14/09/13	17/09/13	Audience of specialists	
FSEC -vendor neutral technical security Symposium	CARNet	18/09/13	20/09/13	internet security specialists	http://fsec.foi.hr
NXP security days	LSEC	23/09/13	23/09/13	NWO & Dutch Goverment	
ISD 2013 Conference	ECO	24/09/13	25/09/13	Security experts	
Brucon 2013 Workshop	LSEC	25/09/13	27/09/13	business& government	
CERT-RO Cyber Security technical workshop	CERT-RO	01/10/13	01/10/13	audience of specialist	
ENISA/EC3 Workshop	ECO	02/10/13	03/10/13	Security experts	http://www.enisa.europa.eu/media/news-items/european-cyber-security-month-2013-get-involved
Provision Day Conference	CERT-RO	03/10/13	03/10/13	Network Operator & ISP	http://cybersecuritymonth.eu/ecsm-countries/romania
InnoVisions IT Security Day	FKIE	08/10/13	08/10/13	research, industry, government	http://innovisions.de/
The protection of critical infrastructure in energy and communication sectors Conference	CERT-RO	10/10/13	10/10/13	CERTs, LEA	http://cybersecuritymonth.eu/ecsm-countries/romania
Veiligheidsinnovatie Netherlands	LSEC	10/10/13	10/10/13	Government	
RIPE67	ECO	15/10/13	17/10/13	privacy specialists, research, cybersecurity	https://ripe67.ripe.net/
Belgacom Security Convention	LSEC	15/10/13	15/10/13	research, industry, government	
Cyberthreats Conference	CERT-RO	16/10/13	16/10/13	research, industry, government	http://cybersecuritymonth.eu/ecsm-countries/romania
IBM Finance Cyber Security	LSEC	17/10/13	17/10/13	business, industry	
M3AAWG General Meeting	ECO	21/10/13	24/10/13	Audience of specialist	
ISSE 2013 Conference	LSEC	22/10/13	23/10/13	research, industry, government	http://www.isse.eu.com/
CSA CEE Summit	XLAB	23/10/13	23/10/13	Security experts	
"Cooperare per crescere nella sicurezza" Workshop	ISCTI	25/10/13	25/10/13	private and public stakeholders	http://www.isticom.it/index.php/archivio-evidenza/2-articoli/313-cooperare-per-crescere-nella-sicurezza
RSA Europe 2013	LSEC	27/10/13	30/10/13	research, industry, government	

Infosecurity.nl	LSEC	30/10/13	31/10/13	business, industry, government	www.infosecurity.nl
Annual International CERT-RO Conference	CERT-RO	31/10/13	31/10/13	experts (inc. EU Cert, ENISA & Europol)	http://www.cert-ro.eu/articol.php?idarticol=777
Conference on Cyber Security	CERT-RO	31/10/13	31/10/13	audience of specialist	http://cybersecuritymonth.eu/ecsm-countries/romania
CERT-RO Cyber Security technical workshop	CERT-RO	01/11/13	01/11/13	audience of specialist	
ICT 2013	ECO/EII/CARNet/ATOS / XLab	06/11/13	08/11/13	research, industry, government	https://ec.europa.eu/digital-agenda/en/ict-2013-conference
BKA Herbsttagung	ECO	12/11/13	12/11/13	Police	
GORE 12 Conference	TID	12/11/13	12/11/13	It specialists	http://www.esnog.net/gore12.html
Cybersecurity Challenges Seminar	LSEC	14/11/13	14/11/13	industry, research	www.lsec.be
SBIR Cyber Security Workshop	LSEC	19/11/13	19/11/13	industry, research	
15th CARNet Users Conference	CARNet	20/11/13	22/11/13	CARNet users, ISPs	cuc.carnet.hr
DWT Forum Cyber Defence	FKIE	20/11/13	20/11/13	research, industry, government	https://www.dwt-sgw.de
ACDC Roadshow Netherlands	ECO / TU Delft	21/11/13	21/11/13	business, policy	
ENISE	INTECO	22/11/13	23/11/13	research, industry, government	http://www.enise.inteco.es
Rescom SDN Days	MI	26/11/13	27/11/13	CERT-RO partners	sdndays.loria.fr
Cyber Security Guide Launch Event	LSEC	28/11/13	28/11/13	industry, research, government	
CIP Event	LSEC	28/11/13	28/11/13	industry, research, government	www.lsec.be
FI-ISAC Europe Summit	ECO	02/12/13	03/12/13	ICT security specialists	https://www.fsisac.com/
Octopus Conference	ECO	04/12/13	06/12/13	Cybercrime experts	http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2013/Octopus2013_en.asp
Botconf 2013	LSEC/ XLAB	05/12/13	05/12/13	industry, research, government	
EII R&D strategy day	EII	10/12/13	10/12/13	Industry	Internal presentation to the R&D direction team
Future of Mobile Payments	LSEC	10/12/13	10/12/13	industry, research, government	
NIS Plenary	LSEC	11/12/13	11/12/13	industry, research, government	
Innovation Security Day 2013	INTECO	12/12/13	12/12/13	research, industry, government	http://grandesempresas.telefonica.es/panorama_tic/el-innovation-security-day-cierra-el-

					ano-el-dia-12-de-diciembre-en-madrid/
CSP Forum	LSEC	12/12/13	12/12/13	industry, research, government	
Poste Italiane	EII	13/12/13	13/12/13	Industry	Presentation of ACDC
MACCSA meeting	LSEC	13/12/13	13/12/13	Engineers and managers from Thales business divisions	
ICS Cyber Security Workshop	LSEC	16/12/13	16/12/13	Researchers and industry	
APT Incident Handling and Network forensic Workshop	CERT-RO	17/12/13	17/12/13	audience of specialist	http://www.cert-ro.eu/articol.php?idarticol=808
NIS WG2 Workshop	LSEC	08/01/14	08/01/14	Academia and industry	
ETSI Security Workshop	LSEC	15/01/14	16/01/14	Researchers and industry	http://www.etsi.org/news-events/events/681-2014-securityws
FIC 2014 Forum	LSEC	21/01/14	22/01/14	Security experts and stakeholders	http://www.forum-fic.com/2014/fr/
CPDP Conference	LSEC	22/01/14	25/01/14	general audience	
SMIG	LSEC	23/01/14	24/01/14	ICT Managers	
Cyber Security sharing	LSEC	29/01/14	29/01/14	Network Operator & ISP	
BELSPO meeting	LSEC	31/01/14	31/01/14	Network Operator & ISP	
RSA - EMC CISO debate	LSEC	03/02/14	03/02/14	ict security industry & research	
Innovating botnet mitigation: sharing insights , data, and approaches across different project", joint workshop - project presentation	TU Delft	06/02/14	07/02/14	Security Experts	http://www.tbm.tudelft.nl/en/about-faculty/departments/multi-actor-systems/polg-section/economics-of-cybersecurity/events/
Cybersecurity in Romania Conference- giving a presentation	CARNet	10/02/14	10/03/14	IT security experts, vendors	https://cybersecurity-romania.ro/
Presentation	TID	10/02/14	10/02/14	Telefonica worldwide business units	
Mobile Security – presentation	LSEC	13/02/14	13/02/14	ict security industry & research	together with TNO
ENISA NLO MEETING	CERT-RO	18/02/14	18/02/14	Representants of EU member states	www.enisa.europa.eu
Infosharing – presentation	LSEC	21/02/14	21/02/14	ict security industry & research	
RSA Conference – discussion	LSEC	21/02/14	27/02/14	ict security industry & research	RSA conference US
ACDC Presentation during ETSI ISG ISI meeting	TI-IT	26/02/14	26/02/14	Security experts	
High Level Cyber Security event – discussion	LSEC	28/02/14	28/02/14	ict security industry & research	EC High Level Cybersec event
CERT-RO ANNUAL CONFERENCE - giving presentation	CERT-RO	11/03/14	11/03/14	IT specialists	http://www.cert-ro.eu/articol.php?idarticol=896
Spain Workshop H2020	INCIBE	11/03/14	11/03/14	Private and public cybersecurity companies	

Security Hardening – discussion	LSEC	12/03/14	12/03/14	ict security industry & research	
EUROPOL (EC3) presentation	INCIBE	13/03/14	13/03/14	EUROPOL (EC3) members	
Big Data Security & Privacy – discussion	LSEC	18/03/14	18/03/14	ict security industry & research	
Giving a presentation in conference - IDC Conference "Information Security and evolution of the data centre"	BGPOST	20/03/14	20/03/14	Bulgarian media	http://idc-cema.com/eng/events/56346-idc-it-security-and-datacenter-transformation-roadshow-2014
Industrial Automation Security – ICS	LSEC	20/03/14	20/03/14	ict security industry & research	http://www.industrialautomationsecurity.com
2nd Annual Cyber Security Forum	LSEC	24/03/14	25/03/14	ict security industry & research	
ACDC Presentation during ETSI NTECH meeting	TI-IT	25/03/14	27/03/14	Standardization Experts	
Security Innovations Pavillion at Infosecurity.be	LSEC	26/03/14	27/03/14	ict security industry & research	http://www.infosecurity.be/nl-NL/Bezoeker/Activiteiten/Seminarieprogramma.aspx
APWG eCrime Sync-Up Conference – presentation	XLAB	31/03/14	03/04/14	Security Experts	http://ecrimeresearch.org/events/eCRSyncup2014/
APWG – presentation	LSEC	01/04/14	03/04/14	ict security industry & research	Oberammergrau NATO educational facilities
eCrime Sync-up presentation	MI	01/04/14	03/04/14	industry, research, government	http://www.ucd.ie/cci/news_and_events/events/ecr_sync-up_2014.html
Datafocus 2014 conference	CARNet	08/04/14	08/04/14	LEA,prosecutors	http://www.insig2.hr/datafocus2014-f22?lang=hr
Giving a presentation in International conference RIPE - SEE3 conference	BGPOST	14/04/14	15/04/14		http://www.ripe.net/
BeCommerce	LSEC	24/04/14	24/04/14	ecommerce cyber security	http://awards.becommerce.be/nl/awards/uitreiking-awards
RSA Security Summit NL	LSEC	24/04/14	24/04/14	ict security industry & research	http://netherlands.emc.com/campaign/global/rsa-summit/index.htm
Infosecurity.co.uk	LSEC	29/04/14	01/05/14	ict security industry & research	http://www.infosec.co.uk/
NIS Platform WG3 – discussion	LSEC	29/04/14	29/04/14	ict security industry & research	
Nebucom bootcamp SaaS	LSEC	30/04/14	30/04/14	ict security industry & research	
Vlaams Innovatienetwerk	LSEC	06/05/14	06/05/14	innovation networks	
Racviac SEE security conference	CARNet	07/05/14	07/05/14	CERTs in SEE, ENISA	www.racviac.org
Racviac SEE security conference - giving presentation	CERT-RO	07/05/14	07/05/14	CERTs	www.racviac.org
BOF meeting about Black-Holing: RIPE 68	DE-CIX	12/05/14	16/05/14	Internet infrastructure operators	http://ripe68.ripe.net

private political debate cyber security	LSEC	12/05/14	12/05/14	ict security industry & research	https://www.eventbrite.com/e/cyber-security-belgium-state-of-affairs-political-debate-tickets-11327632253
Trusted Digital Identity	LSEC	13/05/14	13/05/14	ict security industry & research	http://trusteddigitalidentity.com/event-page-BE.html
German ETSI RGI - R2GS – presentation	LSEC	14/05/14	15/05/14	ict security industry	http://rg-berlin-brandenburg.gi.de/fileadmin/user_upload/GIRGB-140514-Steinhoefel-Planung-Call_engl_G2C_comments_24Jan2014_V4.01.pdf
NCSC & LSEC analytics & information sharing – presentation	LSEC	16/05/14	16/05/14	ict security industry & research	https://www.eventbrite.com/e/information-sharing-security-monitoring-16-may-2014-national-cyber-security-center-ncsc-den-haag-tickets-10655389557
Giving a presentation to a conference	DFN-CERT	20/05/14	20/05/14	European NRENs	https://tnc2014.terena.org/core/presentation/89
Annual Privacy Forum ENISA & EC	LSEC	20/05/14	21/05/14	ict security industry & research	http://privacyforum.eu/
giving presentation during meeting	CARNet	22/05/14	23/05/14	EU regulators	n/a
CSP Forum – dissemination	EII	22/05/14	23/05/14	ict security industry & research	https://www.cspforum.eu/2014
CSP Forum – Presentation	LSEC	22/05/14	23/05/14	ict security industry & research	https://www.cspforum.eu/2014
Mipro 2014 conference- giving presentation	CARNet	28/05/14	29/05/14	Scientific & ICT community	www.mipro.hr
NCSRA IIPV cyber security – Presentation	LSEC	02/06/14	02/06/14	ict security industry & research	https://www.iipvv.nl/en/content/register-ncsra-symposium-june-2nd-2014-hague
NCSC One Forum	LSEC	03/06/14	04/06/14	ict security industry & research	https://www.ncsc.nl/conference
Banking & Finance Big Data & Finance luncheon	LSEC	05/06/14	05/06/14	banking & finance	public relation - publication
vrijdag visdag - innovation network flanders	LSEC	06/06/14	06/06/14	innovation networks	http://www.innovatienetwerk.be/calendar_events/4244
AWS conference	LSEC	10/06/14	10/06/14	ict industry	
Panel discussion: Kompetenzgruppe Infrastruktursicherheit,	DE-CIX	12/06/14	12/06/14	Internet infrastructure operators	http://de-cix.eco.de/2014/events/ddos-angriffe-und-

Eco/DE-CIX					gegenmassnahmen.html
Nebucom conference dissemination - Agoria, Sirris	LSEC	12/06/14	12/06/14	ict industry	http://agcpartners.com/events/agc-partners-second-annual-european-tech-growth-conference/
AGC Europe Conference	LSEC	16/06/14	16/06/14	ict industry	
IOT Europe conference	LSEC	16/06/14	16/06/14	ict industry	
AGM LSEC – presentation	LSEC	18/06/14	18/06/14	ict security industry & research	
workshop mobile security	LSEC	18/06/14	18/06/14	ict security industry & research	
end point security – presentation	LSEC	23/06/14	23/06/14	ict security industry & research	
meetings: attendance at CSA CEE Summit in Ljubljana	XLAB	02/07/14	02/07/14	Security experts	http://csa-cee-summit.eu/
Symantec partner event	LSEC	03/07/14	03/07/14	ict security industry & research	
Presentation of ACDC at University of National and World Economy(UNWE)	BGPOST	04/07/14	09/07/14	Bulgarian University	
STIX - TAXI training	LSEC	14/07/14	15/07/14	ict industry	http://www.leadersinsecurity.org/events/icalrepeat.detail/2014/07/14/100/-/-.html
Discussion about Route-Server-BDF (Transparency of Route-Server)	DE-CIX	20/07/14	25/07/14	Internet infrastructure operators	http://www.ietf.org/meeting/90
IDaaS - multifactor authentication workshop	LSEC	07/08/14	07/08/14	ict security industry & research	
cybersecurity innovation bootcamp	LSEC	01/09/14	01/09/14	ict security industry & research	
Poster on Ljubljana Algorithms and Data Structures Summer School	XLAB	01/09/14	05/09/14	ict industry	http://lusy.fri.uni-lj.si/en/lads2014
Presentation of accepted paper "Fighting Botnets with Cyber-Security Analytics" in conference ARES-IND 2014	ATOS	10/09/14	10/09/14	Security research and industry	http://www.ares-conference.eu/conference/conference-2/program/ares-industrial-track/
Cyber Risks in Financial Services - giving a presentation	CERT-RO	10/09/14	10/09/14	IT specialists	http://cybersecuritymonth.eu/ecsm-countries/romania/cyber-risks-in-financial-services
Cyber Physical workshop	LSEC	11/09/14	11/09/14	ict security industry & research	
TDI Future of Digital	LSEC	11/09/14	11/09/14	ict security industry & research	
Poster Presentation at the Future Security Conference	B-CCENTRE-	16/09/14	18/09/14	Academia, Government, Industry	http://www.en.future-security2014.de/

2014 in Berlin	KUL				
NATO NIAS 2014	LSEC	16/09/14	19/09/14	ict security industry & research	
FSEC 2014 - vendor neutral security conference	CARNet	17/09/14	19/09/14	IT security experts	fsec.foi.hr
ISD 2014 - Giving a presentation	EII	23/09/14	24/09/14	Internet infrastructure security group	http://isd.eco.de/
Brucon 2014 – discussion	LSEC	23/09/14	26/09/14	ict security industry & research	
Giving a presentation: Internet Security Days 2014	DE-CIX	24/09/14	25/09/14	Internet infrastructure security group	http://isd.eco.de
Internet Security Days 2014	ECO	24/09/14	25/09/14	ict security industry & research	http://isd.eco.de/en/agenda
Presentation at ISD2014	XLAB	24/09/14	25/09/14	ICT Security Industry & Research	http://isd.eco.de/en/agenda/agenda-2014-wednesday/
Giving a presentation: Workshop on Critical Information Infrastructures and Internet Infrastructure	DE-CIX	26/09/14	26/09/14	Internet infrastructure security group	http://www.enisa.eu
CSA Belux Kick Off Activitiy – Presentation	LSEC	29/09/14	29/09/14	ict security industry & research	
Nebucom conference dissemination - Agoria, Sirris	LSEC	30/09/14	30/09/14	ict security industry & research	
ENISA High Level - ECSM kickoff	LSEC	01/10/14	01/10/14	ict security industry & research	
Cybersecurity in Romania - giving a presentation about CERT-RO in ACDC	CERT-RO	03/10/14	04/10/14	IT specialists	http://cybersecuritymonth.eu/ecsm-countries/romania/cybersecurity-in-romania
Cyberthreats conference-giving a presentation	CERT-RO	16/10/14	16/10/14	IT specialists	http://cybersecuritymonth.eu/ecsm-countries/romania/cyberthreats-conference-1
European Banking Forum 2014	ECO	16/10/14		banking & finance	http://www.arena-international.com/ebf-future-banking-security/programme/
Giving a presentation - 14th Broadband Word Forum 2014	TID	21/10/14	21/10/14	industry, network operators	http://broadbandworldforum.com/agenda/day-1/
IPACSO Innovation Awards 2014	XLAB	23/10/14	23/10/14	ICT Security Industry & Research	http://ipacso.eu/
Giving a presentation and being part of a panel discussion: 25th Euro-IX Forum	DE-CIX	25/10/14	28/10/14	Internet infrastructure security group	http://www.euro-ix.net
Giving a presentation - ENISE 2014	INCIBE	28/10/14		General public	http://www.8enise.webcastlive.es/webcast.htm?video=04
Giving a presentation - MalCon 2014	FKIE	29/10/14	29/10/14	ICT Security Industry & Research	http://malwareconference.org/index.php/en/
Giving a presentation: Internet Infrastructure Security and Resilience Reference Group	DE-CIX	03/11/14	03/11/14	Internet infrastructure security group	http://www.enisa.eu

Discussions: RIPE 69	DE-CIX	03/11/14	07/11/14	Internet infrastructure operators	http://ripe69.ripe.net
Discussion about Route-Server-BDF (Transparency of Route-Server)	DE-CIX	09/11/14	14/11/14	Internet infrastructure operators	http://www.ietf.org/meeting/91/
Project presentation - CARNet User Conference 2014	CARNet	20/11/14	20/11/14	CARNet user conference	http://cuc.carnet.hr/2014
Project presentation - KOM 2014	CARNet	24/11/14	25/11/14	IT experts	http://www.case.hr/konferencije/kom2014
ADVICE Liaison Workshop on social acceptability of smart surveillance – giving a presentation	EII	24/11/14	26/11/14	ICT Security Industry & Research	https://advice-project.eu/events
Presentation at Botconf 2014	B-CCENTRE-KUL	03/12/14	05/10/14	Academia, Law Enforcement, Industry	https://www.botconf.eu/
CPDP Conference – dissemination	EII	21/01/15	23/01/15	ICT Security Industry & Research	http://www.cpdpconferences.org/
Giving a presentation at 44th TF-CSIRT Meeting	DFN-CERT	25/01/2015	28/01/2015	European CERTs	
Discussion on the ACDC at ICSS 2015	B-CCENTRE-KUL	04/02/15	05/02/15	Academia, Government, Industry	https://www.icss2015.eu/
Discussion on ACDC at ICSS 2015	B-CCENTRE-KUL	04/02/15	05/02/15	Academia, Government, Industry	https://www.icss2015.eu/
Presentation ACDC at Workshop	ECO	19/02/15	19/02/15	Security experts	https://de-cix.eco.de/2015/news/its-all-about-the-people-and-processes.html
Giving a presentation at CSA CEE Summit 2015	XLAB	11/03/15	11/03/15	Security professionals	https://csa-cee-summit.eu/
Giving a presentation at Bsides Ljubljana Conference	XLAB	12/03/15	12/03/15	Security professionals	http://bsidesljubljana.si/
Giving a presentation at ITrisk Conference	CARNet	17/03/15	17/03/15	IT experts from financial sector	http://institutzaosiguranje.hr/hr/itrisk/program/
Giving a presentation at NATO ARW Workshop	XLAB	17/03/15	18/03/15	Security professionals	http://www.atlantic-club.org/index.php?advanced-research-workshop-8220encouraging-cyber-defence-awareness-in-the-balkans8221
Panel disucssion at World Hosting Days	ECO	26/03/15	25/03/15	IT security industry	http://www.whd.global/de/whd-2015.php
Discussions on ACDC at Datafocus 2015 conference	CARNet	31/03/15	31/03/15	IT experts, LEA, prosecutors	http://www.insig2.eu/agenda-f22-16
Presentation of ACDC activities and Montimage's	MI	17/04/15	17/04/15	Telecom stakeholders, SMEs	http://www.systematic-paris-

expertise at Info Day Souverainte Telecoms					region.org/fr/evenements/info-day-souverainete-telecoms-5g
Discussions on ACDC at RIPE NCC SEE meeting	CARNet	22/04/15	23/04/15	LIR and Internet experts	https://www.ripe.net/participate/meetings/regional-meetings/see-4
Interview	BGPOST	24/04/15	24/04/15	Bulgarian media	
Discussions at the ACDC booth at CSP Innovation Forum	XLAB	28/04/15	29/04/15	Security professionals	http://cspforum.eu/
Discussions at the ACDC booth at CSP Innovation Forum	EII	28/04/15	29/04/15	Security professionals	http://cspforum.eu/
Giving a presentation at ''Fighting terrorism and the need for Security Culture'' Conference	CERT-RO	28/04/15	28/04/15	security specialists, government officials	http://www.bcub.ro/cataloage/conferinta-internationala-fighting-terrorism-and-the-need-of-security-culture/agenda-eveniment
Giving a presentation at RACVIAC SEE security conference	CARNet	13/05/15	14/05/15	security officers from SEE region	
Giving a presentation at ACDC Bulgarian National Conference	EII	26/05/15	26/05/15	Bulgarian companies	http://www.bgpost.bg/?cid=236
Hosting the ACDC Bulgarian National Conference	BGPOST	26/05/15	26/05/15	Bulgarian companies	http://www.bgpost.bg/?cid=236
ACDC collaborator of APWG.EU E-Crime Forum	CyDef	26/05/15	29/05/15	industry, law enforcement, governmental, experts	http://www.antiphishing.org/apwg-events/ecrime2015/
Giving a presentation at ACDC Bulgarian National Conference	MI	26/05/15	26/05/15	IT experts	http://www.bgpost.bg/?cid=236
Giving a presentation at ACDC Bulgarian National Conference	CARNet	26/05/15	26/05/15	IT experts	http://www.bgpost.bg/?cid=236
Giving a presentation at ACDC Bulgarian National Conference	INCIBE	26/05/15	26/05/15	IT experts	http://www.bgpost.bg/files/custom/Agenda_Conference_Final.pdf
Giving a presentation at eCrimeSync-up Research Collaboration	INCIBE	26/05/15	26/05/15	Cybersecurity	https://apwg.org/apwg-events/ecrime2015/agenda
Giving a presentation at ACDC Bulgarian National Conference	CERT-RO	26/05/15	26/05/15	IT experts	http://www.bgpost.bg/?cid=236

Giving a presentation at ACDC Bulgarian National Conference	ECO	26/05/15	26/05/15	IT experts	http://www.bgpost.bg/?cid=236
Stand at InfoSecurity Days	ECO	02/06/15	04/05/15	ict security industry & research	http://www.infosecurityeurope.com/
ACDC and Spain NSC presentation at AMERIPOL	INCIBE	04/06/15	04/06/15		
Security workshop organized by Telecom Italia Lab	TI-IT	10/06/15	11/06/15	Intrnational Security experts / academic	
National conference CERT-RO activity presentation with focus on ACDC project	CERT-RO	10/06/15	10/06/15	cyber security specialists, government officials	http://www.dataprotection.ro/?page=Eveniment_aniversar_10_ani_de_la_infiintarea_ANSPDCP&lang=ro
Atos Webinar about ACDC model and technologies	ATOS	10/07/15	11/07/15	Atos Research & Innovation group	
Presentation - Rescom SDN Days	MI			Academia and industry	sdndays.loria.fr

Table 9 – Annex Complete list of events