



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



Deliverable	D5.1.2 – Intermediate dissemination report	
Work package	WP5	
Due date	31/01/2014	
Submission date	31/01/2014	
Revision	1.13	
Status of revision	Final	
Responsible partner	Engineering Ingegneria Informatica	
Contributors	Véronique Pevtschin (EII), Barbara Pirillo (EII), Ioana Cristina Cotoi (EII), Toni Felguera (BDIGITAL), Dan Tofan (CERT-RO), Jochen Schoenfelder (DFN-CERT), Christian Nordlohne (Institute for Internet Security), Ana Belén Santos Pintor (INTECO), Edgardo Montes de Oca (Montimage), Peter Meyer (eco), Goran Skvarc (CARNet), Aleš Černivec (XLAB), Will Rogofsky (CyDef), Jeronimo Nuñez Mendoza (TID), Rumen Dontchev (BGPOST), Ann Mennens (KUL), Tiziano Inzerilli (ISCTI), Kazim Hussain (ATOS), Paolo De Lutiis (Telecom Italia)	
Project Number	CIP-ICT PSP-2012-6 / 325188	
Project Acronym	ACDC	
Project Title	Advanced Cyber Defence Centre	
Start Date	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
1.00	20/12/2013	EII – VéroniquePevtschin	Creation of table of content
1.01	3/1/2014	EII – IoanaCotoi	First draft
1.02	6/1/2014	Eco	Contribution of meetings
1.03	8/1/2014	EII – IoanaCotoi	Update of meetings / contribution from all partners
1.04 – 1.07		EII	Internal reviews
1.08	20/01/2014	EII – IoanaCotoi	Update of list of future opportunities
1.09	24/01/2014	EII – VéroniquePevtschin	Review Addition of link to WP6
1.10 1.11	28/01/2014	EII – Ioana Cotoi	Update of figures
1.12	29/01/2014	EII –Véronique Pevtschin	Submission
1.13	7/2/2014	EII – Véronique Pevtschin	Updated submission version to correct Inteco names of participants

Glossary

ACDC	Advanced Cyber Defence Centre
APT	Advanced Persistent Threat
APWG	Anti-Phishing Working Group
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
EC3	European Cybercrime Centre
ECI	European Critical Infrastructure
EEC	European Economic Community
ENISA	European Network and Information Security Agency
EU	European Union
FS-ISAC	Financial Services - Information Sharing and Analysis Centre
ICST	International Conference on Software Testing, Verification and Validation
ICT	Information and Communication Technologies
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
INTUG	International Telecommunications Users Group
ISAC	Information Sharing and Analysis Centre
ISD	Internet Security Days
ISIC	International Standard Industrial Classification of All Economic Activities
ISP	Internet Service Provider
LAP	London Action Plan
LEA	Law Enforcement Authority
LoI	Letter of interest
MAAWG	Messaging Anti-Abuse Working Group
NSC	National Support Centres (ACDC relay nodes)
RIPE (NCC)	RIPE Network Coordination Centre
RCIS	International Conference on Research Challenges in Information Science
US	Unites States

Table of contents

1. Executive summary	5
2. Overview of the link between WP5 and WP6 deliverables (M12 deadline)	6
3. Introduction	7
4. Dissemination team	7
5. The ACDC logo	8
6. Online visibility	9
6.1. Website	9
6.2. Social media	11
7. Printed materials and publications	11
7.1. Presentations	11
7.2. Posters.....	12
7.3. Press releases	14
8. Events	16
9. Internet Security Days	21
10. ICT 2013	23
11. Octopus Conference 2013	24
12. Botconf 2013	25
13. Updates to the dissemination activities plan	26
14. Future opportunities	31
15. Conclusions.....	32

Table of tables

Table 1 – overview of the WP5 – WP6 deliverables over the first 12 months of operation	6
Table 2 - list of contacts per partner involved in the dissemination task T5.1.....	8
Table 3 - Logo	8
Table 4 – List of Press releases.....	16
Table 5 – List of Events.....	21
Table 6 -List of partners role in dissemination updated	31
Table 7 – list of events for 2014	32

Table of Figures

Figure1 – ACDC Website	10
Figure 2 – Website visibility	10
Figure 3 – ACDC overview presentation.....	12
Figure 4– ACDC Poster	13
Figure 5 – ACDC at the Internet Security Days	22
Figure 6– ACDC at ICT 2013, one of 10 networking sessions	23
Figure 7– ACDC at ICT 2013, the presentation of the project	24
Figure 8 – ACDC at Octopus Conference	25
Figure 9 – ACDC at Bonconf 2013	26

1. Executive summary

The goal of ACDC is to bring together partners from 14 European countries, including public administrations, private sector organizations, law enforcement representatives and academia, in order to detect, prevent and mitigate a cyber threat commonly known as botnet. ACDC integrates the prior knowledge of the consortium and the additional developments done during the project's lifetime into an integrated strategy of providing a full service offer deployed through a network of national support centres supported by a centralised data clearing house. During the project, this deployment is done through a pilot.

The pilot addresses the identification, measurement, and analysis of botnets as well as the prevention, detection, mitigation, recovery, and evaluation of their impact. ACDC introduces an end-to-end approach from detection to protection.

This pilot project is set in a wider context of the European Cyber-Security Strategy and the NIS platform, as well as the operations of European Agencies such as ENISA and EC3 and numerous CERTs across Europe. This provides the ACDC dissemination activity with a context from which to start, as defined in the dissemination plan deliverable D5.1.1.

This deliverable, D5.1.2, reports on the implementation of the dissemination activities over the first 12 months of activities of ACDC, including

- visibility actions set up to create *awareness*
- links to the project exercises to foster *adoption* through best practices as well as *contributions* of data and new solutions to the ACDC clearing house and network of national support centres
- actions to create a community of stakeholders beyond the ACDC partners (WP6)

The dissemination plan detailed in D5.1.1 involves all partners, identifies key stakeholders and how these would be addressed along awareness, participation and adoption directions, while D5.1.2 focuses on the implementation of the dissemination strategy, including the monitoring of its effectiveness.

Therefore the report is divided in two sections: the first section focuses on monitoring the implementation of the dissemination strategy, whilst the second section focuses on the update to the dissemination strategy for the 2nd year and the list of identified opportunities of events.

2. Overview of the link between WP5 and WP6 deliverables (M12 deadline)

As WP6 has a last number of deliverables within the first 12 months, this section provides an overview of which deliverable provides what information. In addition, due to the close link to the dissemination activities of WP5 two deliverables from WP5 are also included in the description below. This section is repeated in all WP6 deliverables.

<i>Deliverables</i>	<i>What is in the deliverable?</i>
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	<p>A list of the activities carried out by ACDC partners over the first 12 months of existence to lead to user involvement. First results are the letters of intent signed by 5% of the stakeholders identified in D6.1.2.</p> <p>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.</p>
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.

Table 1 – overview of the WP5 – WP6 deliverables over the first 12 months of operation

3. Introduction

Deliverable D5.1.2 is the first report on dissemination activities after 12 months of operation of the ACDC project. It builds on D5.1.1 which defined the dissemination plan.

The ACDC dissemination plan is part of a wider community oriented approach in which ACDC aims to deploy a comprehensive interconnected set of tools to help European citizens and organisations to fight the negative impacts of botnets.

In the first reporting year of the project, ACDC's dissemination activity has delivered the following results:

- The realisation of the Web site
- The presence on Social Media
- Participations to meetings and events
- Various press releases
- The realisation of flyers, posters, power-point presentations

The dissemination activity is complemented by the outreach activity whose first year results are described in D6.3.2.

4. Dissemination team

The dissemination team involves the following partners:

Partner	Contact	Email
ATOS	Pedro Soria	Pedro.soria@atos.net
ATOS	KazimHussain	kazim.hussain@atos.net
BDIGITAL	AntoniFelguera	afelguera@bdigital.org
BGPOST	Rumen Donchev	rdontchev@bgpost.bg
BGPOST	Katia Velikova	k.velikova@bgpost.bg
CARNet	GoranSkvarc	Goran.Skvarc@CARNet.hr
CERT-RO	Daniel Ionita	daniel.ionita@cert-ro.eu
CERT-RO	MihaiRotariu	mihai.rotariu@cert-ro.eu
CERT-RO	Dan Tofan	dan.tofan@cert-ro.eu
CERT-RO	Gabi Ene	gabriel.ene@cert-ro.eu
CyDef	Jart Armin	jart@cyberdefcon.com
CyDef	Will Rogofsky	will@cyberdefcon.com
DFN CERT	Klaus-Peter Kossakowski	acdc@dfn-cert.de
ECO	Thorsten Kraft	Thorsten.kraft@eco.de
ECO	Peter Meyer	Peter.meyer@eco.de
ECO	Michael Weirich	Michael.weirich@eco.de
EII	VéroniquePevtschin	Veronique.pevtschin@eng.it
EII	Barbara Pirillo	Barbara.pirillo@eng.it
EII	Ioana Cotoi	ioana.cotoi@dhitech.it
FCCN	Luis Morais	Luis.morais@fccn.pt
FCCN	Tomás Lima	Tomas.lima@fccn.pt
IF(IS)	Christian Nordlohne	nordlohne@if-is.net
INTECO	Ana Belén Santos Pintor	ana.santos@inteco.es
INTECO	Angela María García Valdés	angela.garcia@inteco.es
ISCTI	TizianoInzerilli, Sandro Mari	tiziano.inzerilli@mise.gov.it , sandro.mari@mise.gov.it

KUL	Ann Mennens	ann.mennens@b-ccentre.be
LSEC	Ulrich Selderslachts	ulrich@leadersinsecurity.org
MontImage	Edgardo Montes de Oca	edgardo.montesdeoca@montimage.com
Telecom Italia	Paolo De Lutiis Sebastiano Di Paola	paolo.delutiis@it.telecomitalia.it Sebastiano.DiPaola@it.telecomitalia.it
Telefónica I+D	JerónimoNúñez Mendoza	jnm@tid.es
Telefónica I+D	Pedro García Parra	pedrogp@tid.es
Telefónica I+D	Diego R. López	diego@tid.es
XLAB	Daniel Vladušić AlešČernivec	daniel.vladusic@xlab.si ales.cernivec@xlab.si

Table 2 - list of contacts per partner involved in the dissemination task T5.1

5. The ACDC logo

The ACDC logo was designed by partner Engineering Ingegneria Informatica to fully reflect the three key aspects of ACDC, namely

- The "end to end approach"
- The "fighting against botnets"
- The "infrastructure" concept of a centre surrounded by national / regional / specialised centres

This is reflected through three components as follows:





	end to end approach	the green line represents the end to end approach, combined with a "defensive" image (against the botnets which in the logo are positioned on the left)
	Fighting botnets	A set of networked devices linked into a bot
	Cyber defence centre surrounded by a set of national centres actions as local relays	A central centre visualised by the inside green point linking to the centres represented by the « C » shape form
	ACDC logo	Bringing the concepts together in a single project ACDC Botnets are figured on the left, with the green line representing « protection » and « end-to-end », while on the right the concept of « centre » appears in the Centre word of the logo

Table 3 - Logo

The elaboration of the logo was done through a number of proposals to the entire consortium and was finalised through exchanges with all partners.

6. Online visibility

In order to facilitate the information and the promotion of the project, a set of channels were chosen and implemented by the consortium, including an online Website and presence on social media.

Having online visibility gave the consortium the opportunity not only to inform the target audience or to promote solutions and initiatives, but also to interact and engage them in the activities carried on by the consortium – for instance at ICT 2013, twitter was successfully to send out a reminder of the networking session of ACDC.

6.1. Website

The ACDC website (www.acdc-project.eu) is used as the main promotional and information channel and is regularly updated with latest news and information.

The website is in line with the ACDC graphic identity and represents the heart of the ACDC dissemination strategy – around which all the other communication tools are deployed and refers back to – centralizing latest news, project's activities and relevant events

The main purpose of the website is to promote ACDC's objectives, messages and activities to all the potential stakeholders.

The website is hosted and managed by ECO, as ACDC project's Coordinator, while its design and content updates are handled by Engineering Ingegneria Informatica as well as the individual WP leaders.

The website presents a home page displaying general information including the main objectives of the project and sub-pages presenting the main action lines of the project as well as all the project partners and the dissemination material (poster, presentations, brochure, newsletters, etc.). An important tool of the Website is the "[Join us](#)" page which gives the possibility for an organisation to express its interest by requesting a Letter of Interest (refer to WP6) to become an ACDC community member.



Advanced Cyber Defence Centre (ACDC)

[Home](#) [About](#) [Infrastructure](#) [Community](#) [Media](#)

ACDC - Advanced Cyber Defence Center

Joining forces to fight botnets

Building on an EU wide sharing of data consolidated in a clearing house, ACDC delivers solutions and creates a pool of knowledge to help organisations across Europe fight botnets.

ACDC is open to new organisations to join its community.

Started in February 2013, the European Advanced Cyber Defence Centre (ACDC) aims to create a community of stakeholders joining forces to fight botnets.

ACDC provides a complete set of solutions accessible online to mitigate on-going attacks and targeted both to end-users and to network operators. It also consolidates the data provided by various stakeholders into a pool of knowledge, accessible through the ACDC central clearing house.

ACDC reaches out to users across Europe through 8 national relay centres.

ACDC currently operates as a 30 months EU-supported pilot project, ending in July 2015 and aims to continue as a self-sustained infrastructure beyond the end of the project.

Initiated by 28 partners from 14 countries, ACDC is open to stakeholders from industry, public authorities and academia across Member States.



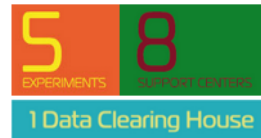
Fighting Botnets



End-to-end Approach



1 Cyber Defense Center



EU-Cleaner Download

By using our EU-Cleaner you will free your computer from malicious threats. At the moment we provide the following EU-Cleaners of your choice to download:



Figure1 – ACDC Website

The ACDC website displays only publicly available information. There is no registration or login needed to access the website. Information displayed is static apart from regular updates about upcoming activities and event related to the project.

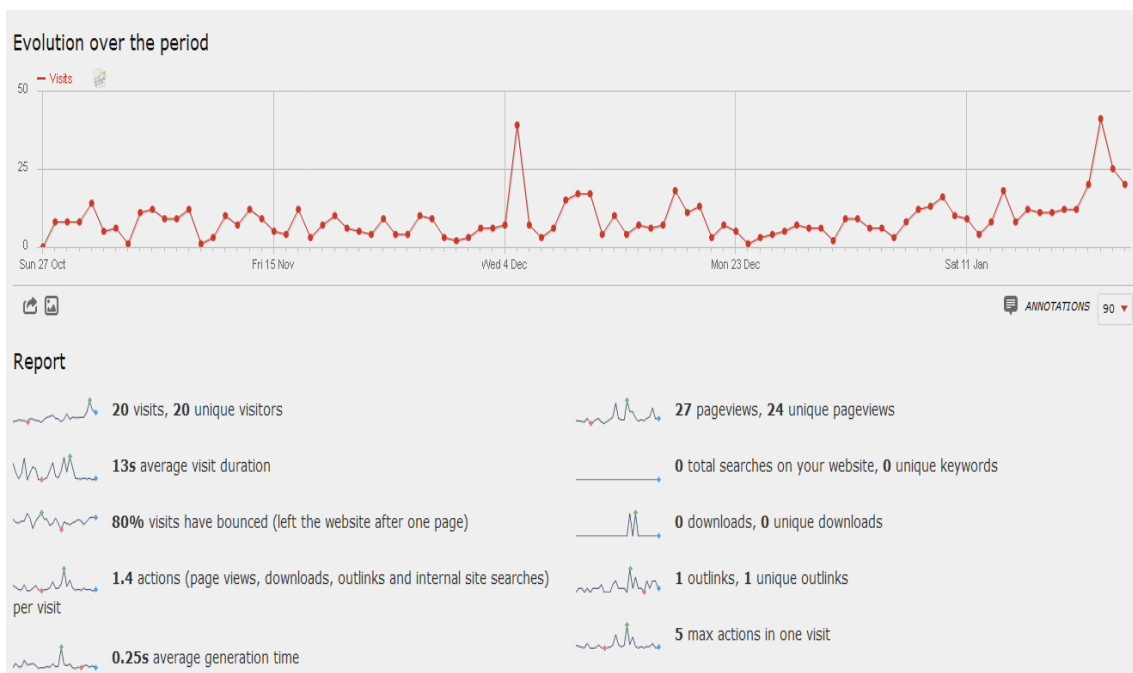


Figure 2 – Website visibility

To determine the progress of the Website in terms of visibility, we are using PIWIK, an open source web analytics platform that gives us, during the last months, valuable insights on the website's visitors in order to optimize the strategy and experience of the users.

The average number of visitors per day was around 9 prior to ICT 2013, and has increased to an average of 15-17 visitors per day since.

6.2. Social media

ACDC is present on social media platforms Facebook and Twitter. The creation of social media accounts allowed the project not only to actively participate and engage with various actors from around Europe but also keeping pace with the on-going discussions and emerging ideas on this topic.

The use of various social media platforms is aligned with the overall dissemination strategy for ACDC. The social media platforms gave the opportunity to ACDC to open another communication channel with stakeholders to promote the project's purpose, messages, activities and events to a wider audience but also maintain a certain visibility to the outcomes and achievements of ACDC during and even after its completion.

ACDC is followed by around 250 users, between Facebook and Twitter, where the users can get involved actively in discussions and activities proposed by the Partners of ACDC.

Other social media platforms, such as Google+ and LinkedIn, will be used in a second phase to have a complete online presence, in order to arrive to a wider audience and to use various ways of communication with the stakeholders.

To improve the online visibility, besides the official Website and the social media platforms, ACDC was also involved in different online awareness campaign, during the European Cyber Security Month, ACDC being promoted by [INTECO](#) Spain and [CERT-RO](#) in Romania.

7. Printed materials and publications

A set of key visuals such as poster, flyers and presentations were designed, printed and distributed during public events and made available on the website.

The look and the feel of the dissemination materials are based on the ACDC project logo.

7.1. Presentations

An ACDC overview presentation was designed, and subsequently updated.



Figure 3 – ACDC overview presentation

In addition to this overview presentation, specific presentations have been designed for events with ACDC participation base on the target and on the nature of the event.

7.2. Posters

This dissemination material contributes to establish the graphic identity of the project as an extension of the website. The main goal was to transmit through the poster a short yet comprehensive overview based around key words and figures describing the purpose of the project, disseminating its message and encouraging all targeted audiences to visit the website and contribute to the project.

The ACDC poster was designed with the overall graphical chart, and its content was elaborated to really focus on the key activities of ACDC as a pilot project. The poster also conveys a graphical overview of the 28 partners involved.

The poster played a key role in the various presentations of the project, facilitating the communication during the events.



ACDC is a European pilot project funded under the CIP-PSP programme.

The ACDC project runs over 30 months from 01/02/2013 to 31/07/2015 and intends **to evolve beyond the end of the project into a sustainable European Advanced Cyber Defence Centre**, building on the networked support centres and clearing house deployed during the project and enlarging the cyber-protection scope beyond botnets.

THE APPROACH

ACDC aims to take down botnets through the elaboration of a European centre proposing a full set of services. The services are relayed through national support centres.

ACDC provides an end-to-end approach from detection to protection. ACDC will build on the data acquired through its European centre to create prevention strategies and improve the awareness and adoption across users.

ACDC will provide tools and sensors to detect botnet related cyber-threats and mitigate cyber attacks on networks, web sites, end user computers and mobile devices.

the Advanced Cyber Defence Centre a European project co-funded through the CIP/PSP programme



30
MONTHS
DURATION



Fighting botnets



End-to-end approach



**1 cyber defence centre
8 national support centres
4 tool groups**

**15,5 M€
TOTAL
COST**

UNITING A COMMUNITY OF Internet Service Providers, CERTs, law enforcement agencies, IT providers, National Research and Education Networks (NRENs), Academia and critical infrastructure operators.

28
PARTNERS

14 COUNTRIES
DEPLOYING
8 SUPPORT CENTRES

Contact point
Coordinator eco - Association of the German Internet Industry

Web sites
ACDC Botnet Services www.botfree.eu
ACDC www.acdc-project.eu



Figure 4– ACDC Poster

7.3. Press releases

In addition to visibility created through the online channels and through the events, ACDC has been visible in the press either through direct activities by ACDC partners or through third party references to ACDC.

The ACDC consortium team regularly prepared and sent out press releases prior to an event or to promote the project's achievements.

The following table lists either the ACDC partners' publications or the press and third party references for ACDC over the first 12 months.

Publication date	Title and Link	Partner(s) involved
13/02/2013	Advanced Cyber Defence Center http://www.eco.de/2013/presse-downloads/advanced-cyber-defence-center-acdc.html	issued by ECO
13/02/2013	Europe bands together to fight against botnets http://www.fccn.pt/fotos/editor2/20130206_pm_kick-off_acdc_eng.pdf	issued by FCCN
13/02/2013	Comienza la andadura del proyecto 'Advanced Cyber Defense Centre' contra lasredeszombi en Internet http://www.inteco.es/pressRoom/Prensa/Actualidad_INTECO/comienzo_ACDC;jsessionid=BD714A3FC321E4A5A046C49820C9E1A3	issued by INTECO
14/02/2013	ecokoordiniert Advanced Cyber Defence Center (ACDC) http://blog.botfrei.de/2013/02/eco-koordiniert-advanced-cyber-defence-center-acdc/	issued by ECO
19/02/2013	Advanced Cyber Defence Center: Neue EU-Zentrale gegen Botnetze http://www.onlinekosten.de/news/artikel/51595/0/Advanced-Cyber-Defence-Center-Neue-EU-Zentrale-gegen-Botnetze	www.onlinekosten.de
19/02/2013	CARNetdioCentrazanaprednuralnuzastituuzpotporu EU-a www.limun.hr	www.limun.hr , Croatia
19/02/2013	CARNet u europskoj borbi protiv botnetata www.rep.hr	www.rep.hr , Croatia
19/02/2013	CARNet s EU-om protiv botnetata www.tportal.hr	www.tportal.hr , Croatia
19/02/2013	CARNet postaodijelomCentrazanaprednuralnuzastituuzpotporu EU-a	issued by CARNet
20/02/2013	CARNet partner protiv botnetata	Novi list, Croatia
20/02/2013	CARNetdioCentrazanaprednuralnuzastituuzpotporu EU-a - Europa protiv botnetata www.racunalo.com	
13/03/2013	CERT-RO se alătură proiectului Advanced Cyber Defence Centre, pentru combaterea amenințărilor cibernetice http://www.cert-ro.eu/articol.php?idarticol=717	issued by CERT-RO

13/03/2013	LSEC plays leading role in Europe's cybersecurity strategy as partner in anti-botnet pilots http://www.lsec.be/index.php/whats_happening/news/lsec_plays_leading_role_in_europes_cybersecurity_strategy_as_partner_in_ant/	issued by LSEC
19/03/2013	LSEC, KULeuven in strijd tegen botnets http://datanews.knack.be/ict/nieuws/lsec-kuleuven-in-strijd-tegen-botnets/article-4000264764771.htm	www.datanews.knack.be
19/03/2013	LSEC, B-CCENTRE et la KU Leuven joignent leurs forces contre les réseaux de zombies http://www.informaticien.be/articles_item-13690.html	www.informaticien.be issued by LSEC and B-CCENTRE
20/03/2013	Europa gaat de strijd aan met botnets http://www.smartbiz.be/nieuws/148240/europa-gaat-de-strijd-aan-met-botnets/	www.smartbiz.be
21/03/2013	LSEC, B-CCENTRE en KU Leuven mee in Europese strijd tegen botnets http://www.solutions-magazine.com/nl/nederlands-lsec-b-ccentre-en-ku-leuven-mee-in-europese-strijd-tegen-botnets-2/	www.solutions-magazine.com issued by LSEC and B-CCENTRE
28/03/2013	Advanced Cyber Defense Center (ACDC) Europe takes on the battle against botnets http://www.tbm.tudelft.nl/en/research/projects/research-review/advanced-cyber-defense-center-acdc/	www.tbm.tudelft.nl issued by Michel van Eeten
01/04/2013	Dio ACDC-a	MediaNet, Croatia
08/05/2013	Bulgarian Posts" EAD began working on a European project "Advanced Cyber Defense Center" ACDC http://www.bta.bg/bg/c/OT/id/596313	www.bta.bg
15/05/2013	Bulgarian Posts" are involved in the project: 5. "Trusted e-services and other activities" http://www.bgpost.bg/?cid=227&spid=227	issued by BGPOST
08/06/2013	Botnetz-Bekämpfung: Rufenach globaler Zusammenarbeit http://www.heise.de/newsticker/meldung/Botnetz-Bekaempfung-Rufe-nach-globaler-Zusammenarbeit-1612849.html	www.heise.de
17/06/2013	Advanced Cyber Defence Centre http://www.scoop.it/t/cyber-defence/p/4003377163/2013/06/17/advanced-cyber-defence-centre	www.scoop.it
26/06/2013	Advanced Cyber Defence Center - ACDC http://www.carnet.hr/eu_projects/acdc	issued by CARNet
26/06/2013	Il primo Centro Avanzato di Difesa del Cyberspazio (ACDC) per l'Europa porta anche la firma di Telecom Italia http://www.telecomitalia.com/tit/it/innovation/cybersecurity/ACDC-Advanced-Cyber-Defence-Center.html	issued by Telecom Italia
10/07/2013	ACDC - Advanced Cyber Defence Center http://www.technikon.com/projects/acdc	issued by Technikon
24/09/2013	Na fsecsimpozijupredstavljjen ACDC project	issued by CARNet
25/09/2013	World Hosts Report - September 2013 http://hostexploit.com/blog/14-reports/3543-world-hosts-report-september-2013.html	www.hostexploit.com

17/10/2013	Uspjescozapocelo rani pilot u okviruCentraza naprednura cunalnuzastituuzpotporu EU-a	issued by CARNet
07/11/2013	Radionica Nacionalnog CERT-a za bankarski sektor	issued by CARNet

Table 4 – List of Press releases

Besides the visibility created through the press releases, ACDC was also promoted via radio and TV coverage in different countries including Germany, Croatia and Romania.

8. Events

The events as well as the workshops and the conferences presented in the following sections were organised to meet as many targeted audiences as possible, thereby multiplying the impact of the communication and creating synergies around the objectives and achievements of ACDC.

The following table lists events either organised by ACDC partners or to which ACDC participated with a presentation, a workshop or a poster session.

Event	Main Leader/ACDC Partner	Start date	End date	Type of audience	Web site
Atos Global Customer Conference	ATOS			Customers	
TERENA TF-CSIRT	CARNet	23/05/2013	24/05/2013	European CERT representatives	https://www.terena.org/events/details.php?event_id=2448
FSEC -vendor neutral technical security Symposium	CARNet	18/09/2013	20/09/2013	internet security specialists	http://fsec.foi.hr
15th CARNet Users Conference	CARNet	20/11/2013	22/11/2013	CARNet users, ISPs	cuc.carnet.hr
Annual International CERT-RO Conference	CERT-RO	31/10/2013	31/10/2013	experts (inc. EU Cert, ENISA & Europol)	http://www.cert-ro.eu/articol.php?idarticol=777
APT Incident Handling and Network forensic Workshop	CERT-RO	17/12/2013	17/12/2013	audience of specialist	http://www.cert-ro.eu/articol.php?idarticol=808
CERT-RO Cyber Security technical workshop	CERT-RO	01/10/2013	01/10/2013	audience of specialist	
CERT-RO Cyber Security technical workshop	CERT-RO	01/11/2013	01/11/2013	audience of specialist	
Conference on Cyber Security	CERT-RO	31/10/2013	31/10/2013	audience of specialist	http://cybersecuritymonth.eu/e-csm-countries/romania

Cyberthreats Conference	CERT-RO	16/10/2013	16/10/2013	research, industry, government	http://cybersecuritymonth.eu/e-csm-countries/romania
The protection of critical infrastructure in energy and communication sectors Conference	CERT-RO	10/10/2013	10/10/2013	CERTs, LEA	http://cybersecuritymonth.eu/e-csm-countries/romania
Provision Day Conference	CERT-RO	03/10/2013	03/10/2013	Network Operator & ISP	http://cybersecuritymonth.eu/e-csm-countries/romania
Cyber Crime & Cyber Terrorism Roundtable	CyDef	08/04/2013	09/04/2013	Financial Services	http://www.archimedes-eu.eu/mailings/roundtable3_280213.html
M3AAWG General Meeting	ECO	18/02/2013	21/02/2013	Audience of specialists	http://www.maawg.org/events/upcoming_meetings
CeBIT 2013 Conference	ECO	05/03/2013	06/03/2013	General audience	http://www.cebit.de/home
LAP spring 2013	ECO	16/04/2013	16/04/2013	research, industry, government	icpen.org
ECO Kongress	ECO	17/04/2013	17/04/2013	general audience	Eco.de
Trust in the digital world Conference	ECO	18/04/2013	19/04/2013	Industry, military, public agencies	www.eema.org
MAAWG Conference	ECO/B-CCENTRE-KUL	04/06/2013	06/06/2013	Industry, military, public agencies	http://www.maawg.org
APWG Conference	ECO	14/09/2013	17/09/2013	Audience of specialists	
ISD 2013 Conference	ECO	24/09/2013	25/09/2013	Security experts	
ENISA/EC3 Workshop	ECO	02/10/2013	03/10/2013	Security experts	http://www.enisa.europa.eu/media/news-items/european-cyber-security-month-2013-get-involved
RIPE67	ECO	15/10/2013	17/10/2013	privacy specialists, research, cybersecurity	https://ripe67.ripe.net/

M3AAWG General Meeting	ECO	21/10/2013	24/10/2013	Audience of specialist	
BKA Herbsttagung	ECO	12/11/2013	12/11/2013	Police	
FI-ISAC Europe Summit	ECO	02/12/2013	03/12/2013	ICT security specialists	https://www.fsisac.com/
Octopus Conference	ECO	04/12/2013	06/12/2013	Cybercrime experts	http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2013/Octopus2013_en.asp
ICT 2013	ECO/EII/ CARNet/ ATOS / XLab	06/11/2013	08/11/2013	research, industry, government	https://ec.europa.eu/digital-agenda/en/ict-2013-conference
ACDC Roadshow Netherlands	ECO / TU Delft	21/11/2013	21/11/2013	business, policy	
InnoVisions IT Security Day	FKIE	08/10/2013	08/10/2013	research, industry, government	http://innovisions.de/
DWT Forum Cyber Defence	FKIE	20/11/2013	20/11/2013	research, industry, government	https://www.dwt-sgw.de
Innovation Security Day 2013	INTECO	12/12/2013	12/12/2013	research, industry, government	http://grandesempresas.telefonica.es/panorama_tic/el-innovation-security-day-cierra-el-ano-el-dia-12-de-diciembre-en-madrid/
ENISE	INTECO	22/11/2013	23/11/2013	research, industry, government	http://www.enise.inteco.es
“Cooperare per crescere nella sicurezza” Workshop	ISCTI	25/10/2013	25/10/2013	private and public stakeholders	http://www.isticom.it/index.php/archivio-evidenza/2-articoli/313-cooperare-per-crescere-nella-sicurezza
CPDP Conference	LSEC	25/01/2013	27/01/2013	research, industry, government	www.cdpd.org
Computer Privacy and Data Protection Seminar	LSEC	07/02/2013	07/02/2013	Business	www.lsec.be
RSA Conference	LSEC	26/02/2013	01/03/2013	Business	

Cyber Intelligence Workshop	LSEC	29/08/2013	30/08/2013	research, industry, government	http://www.iipvv.nl/nl/content/veldraadpleging-ncsra-ii
LSEC – Agoria ICT eHealth Workshop	LSEC	12/09/2013	12/09/2013	research, industry, government	
NIAS 2013 – Nato Information Assurance symposium	LSEC	12/09/2013	14/09/2013	business& government	
NXP security days	LSEC	23/09/2013	23/09/2013	NWO & Dutch Government	
Brucon 2013 Workshop	LSEC	25/09/2013	27/09/2013	business& government	
Veiligheidsinnovatie Netherlands	LSEC	10/10/2013	10/10/2013	Government	
Belgacom Security Convention	LSEC	15/10/2013	15/10/2013	research, industry, government	
IBM Finance Cyber Security	LSEC	17/10/2013	17/10/2013	business, industry	
ISSE 2013 Conference	LSEC	22/10/2013	23/10/2013	research, industry, government	http://www.isse.eu.com/
RSA Europe 2013	LSEC	27/10/2013	30/10/2013	research, industry, government	
Infosecurity.nl	LSEC	30/10/2013	31/10/2013	business, industry, government	www.infosecurity.nl
Cybersecurity Challenges Seminar	LSEC	14/11/2013	14/11/2013	industry, research	www.lsec.be
SBIR Cyber Security Workshop	LSEC	19/11/2013	19/11/2013	industry, research	
Cyber Security Guide Launch Event	LSEC	28/11/2013	28/11/2013	industry, research, government	
CIP Event	LSEC	28/11/2013	28/11/2013	industry, research, government	www.lsec.be

Botconf 2013	LSEC/ XLAB	05/12/2013	05/12/2013	industry, research, government	
EII R&D strategy day	EII	10/12/2013	10/12/2013	Industry	Internal presentation to the R&D direction team
Future of Mobile Payments	LSEC	10/12/2013	10/12/2013	industry, research, government	
NIS Plenary	LSEC	11/12/2013	11/12/2013	industry, research, government	
CSP Forum	LSEC	12/12/2013	12/12/2013	industry, research, government	
MACCSA meeting	LSEC	13/12/2013	13/12/2013	Engineers and managers from Thales business divisions	
Poste Italiane	EII	13/12/2013	13/12/2013	Industry	Presentation of ACDC
ICS Cyber Security Workshop	LSEC	16/12/2013	16/12/2013	Researchers and industry	
NIS WG2 Workshop	LSEC	08/01/2014	08/01/2014	Academia and industry	
ETSI Security Workshop	LSEC	15/01/2014	16/01/2014	Researchers and industry	http://www.etsi.org/news- events/events/681-2014- securityws
FIC 2014 Forum	LSEC	21/01/2014	22/01/2014	Security experts and stakeholders	http://www.forum- fic.com/2014/fr/
CPDP Conference	LSEC	22/01/2014	25/01/2014	general audience	
SMIG	LSEC	23/01/2014	24/01/2014	ICT Managers	
Cyber Security sharing	LSEC	29/01/2014	29/01/2014	Network Operator & ISP	
BELSPO meeting	LSEC	31/01/2014	31/01/2014	Network Operator & ISP	
Security Innovation	MI	26/02/2013	26/02/2013	IT specialists	

Forum					
ICST 2013 Conference	MI	18/03/2013	21/03/2013	public and private IT specialists	
Rescom SDN Days	MI	26/11/2013	27/11/2013	CERT-RO partners	sdndays.loria.fr
RCIS Conference	MI	31/05/2013	31/05/2013	It specialists	http://rcis-conf.com/rcis2013/document/RCIS2013IndustrialDayProgram.doc
APWG Conference	MI, CyDef	23/04/2013	25/04/2013	It specialists	http://www.apwg.org/apwg-events/cecos2013
European Cyber Security Conference	TEC	16/05/2013	16/05/2013	It specialists	http://www.eu-ems.com/summary.asp?event_id=146&page_id=1219
ICT Compliance & Security workshop	TI	06/06/2013	06/06/2013	It specialists	http://www.osservatori.net/home
GORE 12 Conference	TID	12/11/2013	12/11/2013	It specialists	http://www.esnog.net/gore12.html
CSA CEE Summit	XLAB	23/10/2013	23/10/2013	Security experts	

Table 5 – List of Events

9. Internet Security Days

ACDC was presented at the Internet Security Days, an event with international speakers and audience from the Internet security field that took place from 23rd to 24th September 2013, in Bruehl (Germany).

Internet Security Days gather pioneers of Internet security, and fosters their interaction and collaboration with one another. The goal was to create promising synergies and facilitate discussions around current topics, in the hope that this could eventually lead to new solutions.

Composed of a fair, talks and social events Internet Security Days offered many opportunities for networking and learning the latest developments and trends.

Security Sessions			
	Room 1:	Room 2:	Room 3:
	Advanced threats on the Application Level Moderated by Markus Schaffrin	Protecting your networks Moderated by Cornelia Schildt	European Cooperation Moderated by Peter Meyer
14:30 – 15:00	Security across all layers for internet facing applications Frank Thias, <i>F5 Networks</i>	DDoS & Modern Threat Motives Darren Anstee, <i>Arbor Networks</i>	ACDC Overview and Statistics Ulrich Seldeslachts, <i>LSEC</i> / Michel van Eeten, <i>TU Delft</i>
15:00 – 15:30	Doing well by doing good - Family Freedom as a serv Sascha Beyer, <i>GateSecure</i>	Disguised attacks are a big challenge for it security systems Motasem Al Amour, <i>Stonesoft</i>	ACDC Standards and Experiments Jochen Schönfelder, <i>DFN-CERT</i> / Ignacio Cano Luna, <i>INTECO</i>
15:30 – 16:00	Confidence Interval Measurements Daniel Busch, <i>NSS Labs</i>	European law and botnets: A Dutch Lesson (Or how to make a dishonest living in three simple steps) Hein Dries-Ziekenheiner, <i>Vigilo Consult</i>	ACDC Outreach and User Commitment Kazim Hussain, <i>Atos</i> / Wout de Natris, <i>eco</i>
16:00 – 16:30	Coffee break		

Figure 5 – ACDC at the Internet Security Days

The event was introduced two modes of interaction: general presentations and bilateral meetings.

In the first mode of interaction, the ACDC team gave an introduction to the project. The presentation provided background information of ACDC, an overview about the current threat landscape and especially the goals of the project, focusing on mitigation and long-term plans.

The presentation also included technical insights into the entire ACDC project were provided, addressing topics such as the Centralized Data Clearing House, technical standards, workflow and data handling. The team provided an overview on experiments that were held on detecting Malware and Botnets, giving also an overview about other research and scientific activities within the ACDC project.

An overview about the activities was also provided by different stakeholders involved in the ACDC project. Their presentation also outlined the efforts and the partnerships that were needed to achieve the project goals like botnet mitigation, supporting organizations in raising their cyber-protection level and the activities or creating a European wide network of cyber-defence centres.

In the second mode of interaction, ACDC was presented during one hour face-to-face meetings with each stakeholder interested in the project. The team had the opportunity to have specific and concrete discussions based on the interest of the stakeholders.

During the two days conference the ACDC team presented and promoted the project and also linked with targeted organizations. Several national agencies, national centres on cyber-security/defence or CERTs expressed their interest in the ACDC project willing to join the external consultative board. As a result, 4 of them have signed the Letters of Interest (as of 31/01/2014).

10. ICT 2013

The ACDC project was presented at ICT 2013, Europe's biggest event on digital technology organised by the European Commission that took place from 6th to 8th November, 2013 in Vilnius (Lithuania) attracting more than 4.000 researchers, innovators, entrepreneurs, industry representative, students, public authorities and politicians.

The ACDC team had the opportunity to present and promote the project using two different approaches: on the one hand there was a project stand dedicated to ACDC over the full three days of the conference and on the other hand the project delivered a 90 minutes networking session.

The project stand had 3 different rolling presentations, one more general and two presenting experiments from WP2.

The ACDC networking session took place on the third day of the ICT Conference and the presentation was given by the team, focusing on the introduction to ACDC, its objectives and possible outcomes.

Agenda: [45 minutes sessions] [90 minutes sessions]

Networking sessions

10 Networking sessions

- ▶ Personal Data Management in the Digital Age
- ▶ Better Society: empowering Horizon 2020 with trustable social media
- ▶ Manage your cyber-risks ! Take 20 minutes to visit Cyspa !
- ▶ Engineering a Secure Cyber Space for Europe by 2020
- ▶ ACDC, the European Advanced Cyber Defence Centre addressing the EU2020 priority on Cyber Security
- ▶ A Trustworthy ICT FIREplace – igniting the European research activities
- ▶ Digital Agenda for Europe - The role of trustworthy and interoperable electronic Identification.
- ▶ Preparing the industry to privacy and security-by-design by supporting its application in research
- ▶ Towards a secure and trusted Europe - Research Challenges for Horizon 2020
- ▶ Secure and privacy-aware mobile devices

ID: 11508

Figure 6– ACDC at ICT 2013, one of 10 networking sessions

The format of the networking session was created by the European organisers of the ICT conference based on the presentation of 12 sessions with different themes during a fixed duration of 90 minutes. Each networking booth had a typical capacity of 15 people.

Given the small size of the networking booth and the other competing 11 booths, it was assumed that people would not dedicate a full 90 minutes to ACDC only and the booths would be an open-space and therefore noisy environments.

This led the team to change the initial approach, therefore the session was provided with a self-running and self-explanatory presentation, understandable without the presentation of the speaker while the team had continuously one-to-one interactions with interested parties. This format helped the team have direct connection with many stakeholders and to identify the right collaboration between each stakeholder and the consortium.

ICT 2013

- Conference
- Exhibition
- Networking
- Work Programme
- Investment Forum
- Students

DAE & U

- My Country
- Advisers
- Digital Agenda Assembly
- ICT 2013**
- Communities
- Consultations
- Futurium
- Funding Opportunities

ACDC, the European Advanced Cyber Defence Centre addressing the EU2020 priority on Cyber Security

Booth 12, 08/11/2013 (11:00-12:30)

ACDC would like to use the networking session at the ICT 2013 Conference to present an early showcase of the different tool groups that will empower users in handling security incidents and in fighting botnets, as well as the approach of interconnected centres across Europe.

During the networking session, stakeholders will increase their awareness on the destructive impact of botnets and will learn how to receive improved support to fight botnets.

The ACDC User Community Platform – which will support the user interactions and will provide the opportunity to get training and information – will be also presented during the session.

Organised by: **Barbara PIRILLO** (Engineering - Ingegneria Informatica S.p.A., Italy)

Topic: **Security & Trust**

Comments

You must [log in](#) to add a comment.

ID: 10488



Welcome, dear **Guest** [\[Log on\]](#)

Travel & Accommodation

[Practical information](#)

Figure 7– ACDC at ICT 2013, the presentation of the project

During the conference, in addition to the presentation, posters and flyers were used to entice the participants and to spread efficiently ACDC.

During the three days conference, around 70 organizations (researchers, internet providers, associations, national agencies etc.) expressed their interest in the ACDC project interested to learn more about it and eventually to join the external consultative board. As of 31st January 2014, 3 of them have signed the Letters of Interest.

11. Octopus Conference 2013

ACDC was presented at Octopus Conference 2013, an event where almost 300 cybercrime experts from more than 80 countries, 17 international organizations and initiatives, and 45 private sector and civil society stakeholders and academia met in Strasbourg from 4th to 6th December, 2013 to enhance cooperation against cybercrime at all levels.

The event was focused on capacity building on cybercrime and on safeguard and data protection (criminal justice versus national security).

Octopus Conference was open to cybercrime experts from public and private sectors and from international and non-governmental organizations, like police agencies, ministries, representatives from the justice system, parliamentarians, regulators and industry.

ACDC was presented in the panel on capacity building. Besides the representative of the project, the panel included a police officer from Ukraine, a private cyber crime firm from Russia and a sub-panel on cross border cooperation between the U.S. Federal Trade Commission and the Nigerian Economic Financial Crime Commission.

To create an efficient presentation it was decided to use posters and presentation, in order to facilitate the exposure of the activities and the solutions proposed by ACDC.

THURSDAY, 5 DECEMBER	
Parallel workshop sessions 9h30 – 13h00	Room 1 (Languages: English, French, Russian, Spanish) Workshop 3: Capacity building on cybercrime Capacity building as an approach to cybercrime is broadly supported by the international community. The aim of this workshop is show how this approach may be applied in practice by sharing good practices, success stories, lessons learnt and information on upcoming capacity building programmes. ► Moderator: Jayantha Fernando (Director, ICTA, Sri Lanka) ► Agenda: <ul style="list-style-type: none"> - Examples of current projects and initiatives <ul style="list-style-type: none"> - Capacity building on cybercrime: the experience of the Council of Europe (Alexander Seger, Head of Data Protection and Cybercrime Division, Council of Europe) - Commonwealth Cybercrime Initiative (Tim Crossland, Chair, Executive Management Committee, CCI and Head of Cyber, Prevention and Information Law, National Crime Agency, United Kingdom) - Advance Cyber Defence Centre (ACDC): fighting botnets (Wout De Natris, Reach Out Officer ACDC at ECO, Netherlands) - Capacity building in Ukraine (Leonid Tymchenko, Deputy Chief, Cybercrime Division, Ukraine) - Group-IB (Dmitry Alexandrovich Volkov, Group IB, Russian Federation)

Figure 8 – ACDC at Octopus Conference

The Octopus Conference provided the team the opportunity to reach out to 10 representatives from sectors like justice system, policy makers, security services etc.

Furthermore, ACDC was seen as a very interesting experiment by several relevant representatives at the Octopus meeting; great interest was expressed by organisations from outside the EU.

12. Botconf 2013

ACDC was presented at Botconf 2013, an international scientific conference aiming at bringing together academic, industrial, law enforcement and independent researchers working on issues related to the fight against botnets. The conference was held in Nantes, France from 5th to 6th December, 2013.

The conference focused on topics like the functioning of botnets and of methods used to distribute malware related to botnets, in particular the functioning of malware and command & control mechanisms related to botnets, the understanding of the organisation of groups involved in the development or the management of botnets, methods to monitor, localize and identify botnets and distribution of malware related to botnets and technical, legal and other methods used to mitigate, investigate, dismantle or disrupt botnets.

Thursday Dec 5th






Time	Title Authors	Prez	Paper
08:30	Welcome and registration Coffee and pastries		
09:30	Opening speech <i>Eric Freyssinet, Chairman</i>		
09:40 30'	01 – Invited talk: Preliminary results from the European antibotnet pilot action ACDC. Integrating industry, research and operational networks into detecting and mitigating botnets <i>Ulrich Seldeslachts</i>		
10:10 40'	02 – Advanced Techniques in Modern Banking Trojans <i>Thomas Siebert</i>		
10:50 40'	03 – Spam and All Things Salty: Spambot v2013 <i>Jessa dela Torre</i>		
11:30 40'	04 – Distributed Malware Proxy Networks <i>Brad Porter and Nick Summerlin</i>		
12:10 50'	Lunch		
13:00 20'	05 – Legal limits of proactive actions: Coreflood botnet example <i>Oğuz Kaan Pehlivan</i>		
		SHORT TALK	

Figure 9 – ACDC at Bonconf 2013

For the presentation of the project, the team focused on the following topics:

- extensive sharing of information across network and member states;
- provision of complete set of solutions, accessible online for mitigating on-going attacks;
- use of the pool of knowledge to create best practices and to support affected end users and organizations in raising their cyber-protection level;
- creation of a European wide network of cyber-defence centres.

During the two days conference 8 organisations from different sectors, especially Internet Service Providers, expressed their interest in the ACDC project.

13. Updates to the dissemination activities plan

The following table updates for each partner involved in task T5.1 the dissemination activities plan. This table is based on the one included in D5.1.1. which was submitted in May 2013.

Partner	Contribution to dissemination
ATOS	<ul style="list-style-type: none"> • Inform the different areas in Atos involved in IT security solutions of the ACDC initiative and address ACDC in our yearly international Atos Defence and Security workshop • Include ACDC in our Atos Marketing e-boletín, in Axia magazine, in the Lookout Report, in ARI 2013 Handbook and in next issues of AscentJourney

	<ul style="list-style-type: none"> • Raise awareness of ACDC in presentation to customers, roundtables, seminars, workshops, etc.
BDIGITAL	<p>BDIGITAL develops several technological dissemination activities through the year, being on-line security a topic which, due to its societal relevance, it is always under the scope. The proposed contribution to ACDC dissemination will be by hosting a session on ACDC in the BDigital Global Congress 2014 edition. In addition the BDIGITAL's ACDC team will also attempt to disseminate the project along the following lines:</p> <ul style="list-style-type: none"> • Participating in the Antiphising Working Group (APWG) • Dissemination within the Dorothy Project organization • Dissemination within the Cloud Security Alliance (Spanish chapter and internationally) • Dissemination within the ISMS Forum –Spain and participating in the Spanish Cyber Security Institute (SCSI) events <p>BDIGITAL will also disseminate the project through the companies and organizations that belong to the ICT Cluster as well as through the project Be.Wiser, a Coordinated and Support Action within the Regions of Knowledge (ROK) program, on wireless and Internet Security in European regions.</p>
BGPOST	<ul style="list-style-type: none"> • In the very beginning ACDC will be deployed and tested in BGPOST network • ACDC dissemination inside network infrastructure the Ministry of Transport, IT and Communications and to some government agencies and organizations • The next step is to involve some bank institutions and private companies. • Building awareness in Universal Postal Union (UPU) and in other bodies in which Bulgarian posts participate. • Meetings with the Cyber defence and antivirus laboratory of Bulgarian Academy of Sciences (BAS) • Participation in International Telecommunication Union' (ITU) Cyber defence conferences, International Data Corporation's (IDC) IT Security Roadshow 2014/5 in Bulgaria • Meetings with the Chief Directorate "Combating Organized Crime" (CDCOC) focused on investigating cyber threats and anti-botnet • Advertising relevant ACDC services in BGPOST' website. • Explain and examine the ACDC' role at a minimum of 2 national Cyber security conferences
CARNet	<p>Croatian Academic and Research Network – CARNet (national NREN) together with its Department for National CERT will conduct a nationwide dissemination campaign about the ACDC project and anti-botnet platform to all Internet users and service providers in Croatia. This will include CARNet contribution to preparation of the dissemination plan and its implementation on a national level with all PR means at our disposal.</p>
CERT-RO	<ul style="list-style-type: none"> • At least 1 international conference in 2013 on cyber security threats, ("New Global Challenge in Cyber Security 2013"); the ACDC project will also be addressed. • 3 or more technological seminars (with closed audience) on the subject of efficiently handling cyber security threats; the ACDC

	<p>solutions will also be addressed.</p> <ul style="list-style-type: none"> • Providing a strong connection to the Romanian community of users through our site, www.cert-ro.eu and our social media channels (Facebook, Twitter, LinkedIn etc.). • Press releases for the national press regarding the message and solutions of the project. • TV spots on the Romanian national public television network (TVR) meant to promote the ACDC project & message and the struggle against botnet activity (if the video-clips are provided within the project). • Providing a strong link to the Romanian Internet service providers, and a lobby for the adoption of the solutions provided in the project. • National support centre, which we are about to implement in the next steps of the project, designed to offer tools, tutorials and all the necessary information for both normal and experimented user to utilize in the fight against cyber security threats such as botnet.
CyDef	<ul style="list-style-type: none"> • Advertise relevant ACDC services in public reports (World Hosts Report and White Papers). • Explain and examine the role of ACDC at a minimum of 3 conferences (these are dependent on invitations, but as examples, conferences recently spoken at include APWG, Clusit, MAAWG, NATO and OSCE). • Refer clients to ACDC services where relevant and appropriate. • Provide a detailed dossier on UK stakeholders (as listed in <i>The European and national contexts</i>) where required.
DFN CERT	Link to the European CERT community through the means of TF-CSIRT cooperation. Presentations and tutorials for DFN-CERT's constituency which forms of universities and research institutions throughout Germany and Europe.
ECO	<ul style="list-style-type: none"> • Link to the German community of users and providers • eco will provide a (locally) centralized reporting infrastructure, distributing all relevant data to the necessary stakeholders. (all relevant industry partners, like ISPs or anti-virus vendors, national authorities, like law enforcement agencies or national CERTs) • Publications • Infrastructure for public and project website • Active promotion in social network platforms (like Google+ and Facebook)
EII	<p>Link to Italian community of users and providers</p> <p>Coordination of dissemination implementation</p> <p>Dissemination monitoring</p> <p>Public Web site: structure, content update and content definition (in collaboration with eco)</p> <p>Presentations preparation</p> <p>ACDC Graphical chart definition</p> <p>Publications and events coordination</p>

FCCN	<p>Dissemination inside the “National Network of CSIRTs”, reaching ISPs, banks, CI etc.</p> <p>Interaction with the Portuguese Safer Internet project to find common ground and dissemination opportunities.</p> <p>Enrolment of the Portuguese Telecom Regulator in the project, to establish a partnership for, among other tasks, disseminate the ACDC project on national level.</p>
IF(IS)	Select security conferences and scientific journals to present the ACDC results to an academic audience
INTECO	<p>Provide information about ACDC project in awareness posts about botnets through INTECO blog:</p> <ul style="list-style-type: none"> • http://www.inteco.es/blogs/inteco/Seguridad/BlogSeguridad • The Security Helpdesk for Internet Users (OSI) blog: http://www.osi.es/actualidad/blog <p>Dissemination of the ACDC project in different events related to cyber security threats in which exists the participation of INTECO, like seminars, conferences, workshops etc.</p> <p>Own events, organized by INTECO as ENISE.</p> <p>In the ENISE 2014 edition is planed to dedicate a time slot to make known the ACDC project.</p> <p>Awareness of the fight against botnets through the INTECO and OSI media channels; Twitter, Facebook, Tuenti, Youtube, LinkedIn.</p> <p>Generating awareness actions with Spanish internet service providers in the working group established for this purpose and to support the ACDC project.</p> <p>Creation and start-up the Spanish National Support Centre with the main objective of botnets mitigation, providing the user with cleaning tools and prevention information.</p>
ISCTI	<p>ISCTI will contribute to the consolidation of relevant project results within the following bodies where it participates as active member:</p> <ul style="list-style-type: none"> - ENISA (European Network and Information Security Agency) <p>Italian national support centre web site might be used as a means for implementing awareness campaign by ISCTI in collaboration with the other Italian partners.</p> <p>ISCTI plans to organize a workshop at the Ministry site at the end of the project to disseminate project results.</p> <p>Relevant events in the field of cyber security with national and international scope will be considered for participation of ISCTI in order to disseminate the project results.</p>
KUL	<p>KUL will actively contribute to the implementation of the dissemination strategy as the coordinator of the Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE), a platform for cooperation between academic, governmental and private partners in the fight against cybercrime in Belgium and beyond. The B-CCENTRE has a large multi-disciplinary network of experts dealing with cybercrime, including different target categories for dissemination. KU Leuven will provide content for the central ACDC website and will disseminate the results of its tasks through participation in conferences and workshops and publication of results in Journals and conference proceedings with a high impact, e.g., USENIX.</p> <p>The B-CCENTRE will use its network of expertise and contacts in Belgium, as well as in the rest of Europe to spread the word on the project and its activities and results to a target audience, including by means of the B-CCENTRE website and awareness raising initiatives.</p> <p>The B-CCENTRE website (www.b-ccentre.be) will be hosting the Belgian</p>

	localised section of the ACDC portal.
LSEC	<p>Partner LSEC will integrate activities of the Pilot Network and the Thematic Network into its day to day dissemination operations. These include weekly mailing to more than 25.000 IT professionals and risk officers of government and enterprises. LSEC has a bi-weekly publication called "Information Security Industry Report", an electronic periodical that informs different communities, business, industry, law enforcement, operator and government IT security responsible persons about on-going IT security developments, threats and challenges and innovative solutions.</p> <p>LSEC runs a number of public websites that collectively reach out to over 5000 users on a weekly basis, providing documentation, business cases, in depth cases, market overviews and other similar types of documentation. These platforms will be used to distribute project information and gather additional interest to the project website, by linking them as active themes.</p> <p>Interesting results coming out of the pilot project or activities from the thematic network will be published by partner LSEC.</p> <p>During the project, partner LSEC will be involved in the development of a professional communication plan, outlining all media and target segments, indicating media use, planning, tools in line with the overall project development and working groups. Development of branding and communication templates for localized distribution and local adaptation.</p> <p>Development of standard communication materials, communication guidelines per country and per target group.</p> <p>LSEC will be able to contribute to the set up and run of the Pilot project website, with regular updates to reflect progress, to support and promote the project. This will include partner profiles, project deliverable reports and presentations, and details of workshops and events including invitations for others to become involved. Other media including press releases, newsletters, high quality project brochure, articles in business publications and scientific and social media will be used.</p> <p>LSEC will also be involved to ensure the distribution of the developed pilot results and mitigation results. LSEC can provide input to the final report which includes project results and policy/program recommendations will be presented to key stakeholders in Brussels in a high-level workshop. This will stimulate further actions to take forward the recommendations identified in the final report.</p>
MontImage	<ul style="list-style-type: none"> • Create general awareness about project objectives and expected results • Establish links with related initiatives and projects. • Increasing the market potential involving the presentation of the tangible/exploitable results • Publications presentation in relevant exhibitions and events • Organisation of an international workshop • Define a open source strategy for our tool <p>Examples of activities done or about to be done:</p> <ul style="list-style-type: none"> • Contribution to the System@tic's (regional competitiveness pole's) R&D Book • Presentation of project to the French DGA (meeting in Rennes) and in Thales' PME Security Day • Presentation of project in the APWG (CeCOS VII)
Microsoft EMEA	

Telecom Italia	<ul style="list-style-type: none"> • Link to Italian community of users and providers • participation to the dissemination actions (event presentation, paper, articles publications, etc.) • Public Web site (Italian “localization”): structure, content update and content definition (in collaboration with other Italian ACDC partners) • Advertise the ACDC Pilot resources (Public Web site, Pilot events, etc.) through Public Telecom Italia Web Sites and corporate magazines. • Advertise the ACDC Pilot resources through TI corporate strategic accounts on Social Networks (e.g. LinkedIn)
Telefónica I+D	<ul style="list-style-type: none"> • ACDC dissemination inside different areas and companies of Telefónica Group. • Participation in standard bodies such as IETF, 3GPP, ITU-T and ETSI. • Building awareness in ISOC and in other bodies in which Telefónica participates. • Attempted participation in relevant events like Campus Party. • Meetings with the university cluster on Security Technologies hosted by Telefonica. • Participation in conferences of the Spanish Network Operators Group (ESNOG/GORE). http://www.esnog.net/
XLAB	dissemination on local conferences in Slovenia and Croatia, dissemination activities of the Consortium as a whole: <ul style="list-style-type: none"> • co-authoring papers, • providing materials for the ACDC web page, webinars, demonstrators

Table 6 -List of partners role in dissemination updated

14. Future opportunities

The following table provides a list of events for the second reporting year of the project; this list will be managed dynamically by the ACDC partners, therefore the table below is a static view for the deliverable purpose.

Event	Start date	End date	Website	Relevance to ACDC
Faculty of electrical engineering and computing (Safer internet presentations)	January 24, 2014	January 24, 2014	http://www.fer.hr	Invited presentation about incidents in Croatia, botnets and ACDC project
Mipro 2014	May 26, 2014	May 30, 2014	http://www.mipro.hr/MI PRO2014/	International conference on ICT, electronics and microelectronics

IDC IT Security roadshow	May 20, 2014	May 20, 2014	http://idc-cema.com/eng/events/56963-idc-it-security-virtualization-and-it-infrastructure-efficiency-roadshow-2014	Conference covering many aspects of information security
fsec 2014 - Vendor-neutral technical symposium	September - TBA		http://fsec.foi.hr/	The Symposium is covering a broad area of information security topics. Additional Activities include OWASP round table discussion and OWASP Croatia membership meeting with plenty of informal networking events.
SoftCOM 2014	September 19, 2014	September 20, 2014.	http://marjan.fesb.hr/SoftCOM/2014/index.html	22nd International Conference on software, Telecommunications and Computer Networks, great place to present ACDC project to expert community
ENISE	October, 2014	October, 2014	http://www.enise.inteco.es	The Information Security International Meeting (ENISE) organized by INTECO and can be used to disseminate the ACDC project
16th CARNet Users Conference CUC2014	November 19, 2014	November 21, 2014	cuc.carnet.hr	CARNet national conference that unites all academic IT staff in one place, usually includes industry partners as well.

Table 7 – list of events for 2014

15. Conclusions

The ACDC intermediate dissemination reports on the first 12 months of activity of the project. The ACDC partners have, together, disseminated ACDC in a consistent manner towards different audiences. The dissemination activities are fully aligned with the initial strategy and with the positioning of ACDC as a pilot project.

The intermediate dissemination report has gathered all the instruments and the activities already done in order to deploy successfully the project. This deliverable has laid out in detail the set of communication and dissemination tools used during the first year:

- Website
- Social media
- Printed and online dissemination material such as presentations, flyers and posters
- Press releases

- Conferences and meetings

D5.1.2 has also presented a clear overview of the effectiveness of the actions envisaged in this deliverable based on the metrics for monitoring introduced in D5.1.1. Further quantitative information can be found in D6.3.2 and D6.1.2.