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

Deliverable	**D1.3.1 Specification of Tool Group "Support Centre"**
Work package	WP1 Requirements & Specifications
Due date	M6
Submission date	31.07.2013
Revision	1.0
Status of revision	
Responsible Partner	ECO
Contributors	Peter Meyer (ECO) Michael Weirich (Eco)
Project Number	CIP-ICT PSP-2012-6 / 325188
Project Acronym	ACDC
Project Title	Advanced Cyber Defence Centre
Start Date of Project	01/02/2013

Dissemination Level	
PU: Public	X
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
v.0.1	06/13/2013	Peter Meyer (ECO)	Initial structure of the document / table of content
v.0.2	06/20/2013	Peter Meyer (ECO)	Revised table of content, provided details to bullet points.
v.0.3	07/02/2013	Peter Meyer (ECO)	Updated information to German support centre, included concept for a central support centre
v.1.0	07/30/2013	Peter Meyer (ECO)	
v.1.1	12/09/2013	Peter Meyer (ECO)	Added minimal requirements
V1.2	12/10/2013	Peter Meyer (ECO)	Replaced EII with ISCTI for the Italian Support Centre
V1.3	23.01.2014	Michael Weirich	Minor fixes – responsible Partner, languages of the support chentres

Glossary

ACDC	Advanced Cyber Defence Centre
ABBZ	German Anti Botnet Advisory Centre
OTRS	Customer Support System

Table of contents

1. Executive summary 4
2. Introduction 4
   2.1. National Support Centres 5
      2.1.1. Germany – eco e.V. 5
      2.1.2. Spain – INTECO 5
      2.1.3. France – SignalSpam 5
      2.1.4. Belgium – BCCENTRE / KU Leuven 5
      2.1.5. Portugal – FCCN 5
      2.1.6. Croatia – CARNET 5
      2.1.7. Romania – CERT.ro 5
      2.1.8. Italy – Engineering Italia 5
      2.1.9. Luxembourg – UL / SnT 5
      2.1.10. English – n.A. ..... **Fehler! Textmarke nicht definiert.**
   2.2. Collaboration and Organisation of the European support centres 6
   2.3. The Website botfree.eu 6
3. Common standards for National Support centres 6
   3.1. Standard requirements for a national support centre 6
   3.2. National Awareness 7
   3.3. Support & Service of a national Support Centre 7
      3.3.1. Support by email 7
      3.3.2. Support by telephone 7
      3.3.3. Support through a forum 7
      3.3.4. Free Tools 8
      3.3.5. Online tools 8
      3.3.6. Links to security pages, security tools/vendors and partner sites 8
   3.4. Communication 8
      3.4.1. Awareness Coaching 8
      3.4.2. Presence in Social Media 8
      3.4.3. Blogs 8
   3.5. Data protection and privacy 8
   3.6. Special Landing Pages 9
4. Example for a National Support Centre: Germany / ECO 9
   4.1. Initiative–S 9
   4.2. Botfrei.de 9
   4.3. The ABBZ (Anti Botnet Advisory Centre) 9
      4.3.1. Support centre process flow 9
      4.3.2. Support centre project website 10
      4.3.3. Telephonic support at the support centre 10
      4.3.4. The ticket system: Generating the ticket number in accordance with data privacy regulations as well as by attack type 10
      4.3.5. Legal aspects 10
   4.4. Special Landing pages – example dns-changer.eu 11
   4.5. Other Services 11
      4.5.1. Forum 11
      4.5.2. Blogs 11
      4.5.3. Social Networks 11
5. References 11

Table of figures

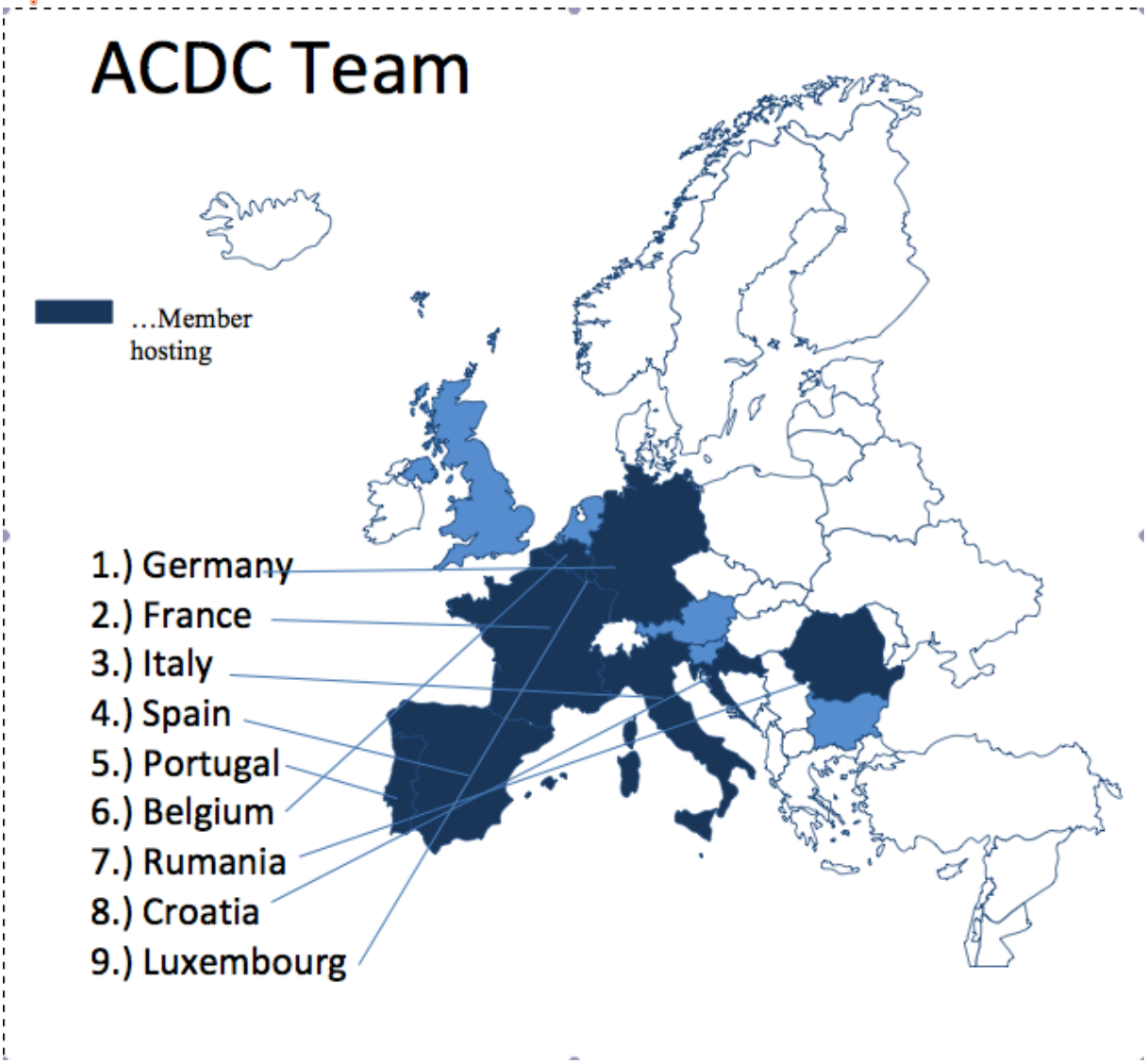
Table of tables

1. Executive summary

This document describes the specifications for a tool group support centre. The support centres are the first point of contact for victims of cyber crime and the main resource of information and knowledge for prevention, awareness and dissemination of infected electronic devices. The support centres represent the initiative to the broad public by interacting directly with end-users and the project has the goal to provide 8 National Support Centres in the participating Member States.

2. Introduction

One of the goals of the ACDC pilot project is a network of 8 National Support Centres being established in the countries participating in ACDC. National Support Centres already exist in Germany Spain, Luxembourg and partially France, five additional Support Centres need to setup in Italy, Portugal, Romania, Belgium and Croatia.



2.1. National Support Centres

The following organisations will setup a national support centre:

2.1.1. Germany – eco e.V.

2.1.2. Spain – INTECO

2.1.3. France – SignalSpam

2.1.4. Belgium – BCCENTRE / KU Leuven

2.1.5. Portugal – FCCN

2.1.6. Croatia – CARNET

2.1.7. Romania – CERT.ro

2.1.8. Italy – ISCTI

2.1.9. Luxembourg – UL / SnT

No partner from the UK/Ireland has committed in establishing an English Support Centre, English Speakers will be directed to the English Version of the German Support Centre botfrei.de

Each of these organisations is responsible to identify an operator for the national support centre and ensure that a national support centre is up and functional as part of the pilot project. Each National Support Centre needs to ensure that it is adequately funded to provide the basic requirements for national support centre as part of the ACDC initiative. It is recommended that the funding and Support Centre get established under the premise of long-term activity going beyond the duration of the ACDC pilot project. It is also recommend that the Support Centres will get operated by a neutral, non-commercial organisation like a CERT, association, independent foundation or government entity.

2.2. Collaboration and Organisation of the European support centres

The national support centres are presenting themselves as part of the ACDC-Initiative. Even though each national support centre will be acting independently, it is necessary that the centres collaborate and sync up on their activities. Therefore, there is a suggestion to establish a "**European Anti-Botnet Support Centre Council"** to coordinate the activities of the European Support Centres even after the end of the pilot project. During the ACDC project, Eco as the project coordinator will lead the cooperation between the national support centres and initialize the founding of an official organisation after the end of the pilot project. This council would coordinate European Wide activities like campaigns; news/press releases and ensure the regular the communication and exchange between the National Support Centres.

2.3. The Website botfree.eu

The website botfree.eu will not be a full operational national support centre. The website is intended as a landing page, pointing users to their national support centres. Providers of a national support centre can either link to their own domain, but it is also possible to host a national support centre directly on a subdomain of botfree.eu, e.g. like italia.botfree.eu
The botfree.eu website may also host dissemination tools that have been developed by the ACDC-consortium or other tools like a joint forum or blog.

3. Common standards for National Support centres

As the national support centre being part of the ACDC-Project, it is necessary that national support centres provide a basic standard of information as defined in the goals of the ACDC project:

- Information
- Dissemination
- Prevention

The exact level of service of a national support centre is based on the available budget and funding of the organisation that is operating the support centre. The support centre itself can range from a simple website up to a service-level exceeding the current functionality of the German Support Centre botfrei.de.

3.1. Standard requirements for a national support centre

- There should be an operator/owner in the country running the support centre.
- The Website must be available in the official language(s) spoken in the hosting country.

- There must be an option to contact the operating organisation.
- The website needs to provide content towards information, dissemination and prevention.
- The operating organisation needs to update the website regularly. This includes security updates, same as news/press releases related to ACDC and updates to internal dissemination tools.
- The operator needs to participate and collaborate with activities driven by the other national Support Centres within ACDC.
- The operator of the support centre is responsible to maintain the highest security standards for its website.
- The operator of the support centre is responsible to translate content related to the ACDC-Initiative into the operating language.
- The National Support Centre needs to display the ACDC Logo
- The Service of the Support Centre needs to be free of charge
- The National Support needs to apply common data privacy standards

3.2. National Awareness

The operator of a national support centre needs to reach out to all national Internet Service Providers to promote and to inform them about their support centre and to indicate how a workflow in regards of customer notification in case of an infection can be established.

3.3. Support & Service of a national Support Centre

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 a recommendation how to extend the service beyond the standard functions.

3.3.1. Support by email

Support by email should be handled by a central help desk system. Privacy needs to be in line with national regulations. Responses should be made in a timely manner. A receipt confirmation for a request with a ticket number always indicates a good service and is recommended. For the support level, it is recommended having templates for standard responses and to provide a knowledge database on the website. ECO has made some good experience with OTRS and it is recommended to utilize this platform across other European support centres. OTRS supports customized queues, ticket numbers, templates and comprehensive search functionalities, basically all functions that are required to run a support system efficiently. An implementation of one standard ticketing system would allow the European Support Centres to benefit from synergies and to standardize their services.

3.3.2. Support by telephone

The costs a phone call should not exceed the costs of a local call, ideally even a toll-free number should be made available. It is open to each support centre to specify their own support time, but it is recommend providing those during common business days and hours only. Based on the experience eco has made, a 24/7 phone support is not necessary.

3.3.3. Support through a forum

In order to keep the direct efforts for phone and email support at a low level, it is recommend to build a support forum and to establish a strong community with a knowledge repository.
The forum needs to be living forum, so it is recommended to recruit and identify volunteers that actively contribute to the forum. The forum should run on an open-source forum system like Vbulletin.

3.3.4. Free Tools

All provided dissemination tools on the website need to be free of charge. The provided tools should also be presented along with a detailed tutorial and screenshots on the website. The available tools need to support all common operating system, especially Microsoft Windows. The portfolio of tools needs to include specific threat-related removals tools, tools for general detection and analysis, same as additional tools for maintenance like for backups. Tools identified as beneficial for the goals of the botfree.eu initiative should be distributed across all national support centres. The Operator of a national Support Centre should also support the localization of tools and manuals being provided as part of the ACDC initiative. Tools can be hosted on a national support centre, on the botfree.eu platform or just linked to the vendor website.

3.3.5. Online tools

The ACDC project will also provide online security checks. This includes testing for up-to-date plugins, browsers, operating systems or other extensions, properly configured firewalls or routers or the detection of other potential security risks. Tools identified as beneficial for the goals of the botfree.eu initiative should be included or linked across all national support centres

3.3.6. Links to security pages, security tools/vendors and partner sites.

A national support centre should provide a strong and comprehensive directory of security websites, covering all areas of Internet security, privacy etc. The links could be marked with affiliate programs to receive funding; 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.

3.4. Communication

3.4.1. Awareness Coaching

One of the main ACDC project goals is the area of prevention. This needs to be raised by regular and detailed security awareness coaching. National support centres should synchronize on their campaigns and especially try to release this coaching on a regular and frequent basis. It is also necessary to use simple language and screenshots etc., as the target of the awareness coaching are mostly non-technical end-users.

3.4.2. Presence in Social Media

The botfree.eu and the national support centres should be actively present in social media, especially on the big three social platforms – Facebook, Twitter and Google Plus. The support centres should use those platforms to reach a broader audience in order to raise security awareness, general information on security and the ACDC project itself.

3.4.3. Blogs

The botfree.eu and the national support centres should be publishing regular blog postings. The posting should cover special threats, provide help on major threats and raise security awareness in general.

3.5. Data protection and privacy

The national support centres need to maintain a common standard on data protection and privacy. The general consensus is that the support centres do not collect or store any personal data. The tickets from the users/ISPs will remain anonymous, as described in the procedures of the German support centre. The support centre websites must explain website visitors

transparently, which type of data they collect or store. Each support centre and the website needs to be in compliance with all participating national privacy laws. No data retrieved by the support centre will be shared with 3rd parties and the data exchange between the individual support centres will be strictly limited by data privacy restrictions as defined and identified within the legal analysis within the ACDC project.

3.6. Special Landing Pages

Special landing pages can be provided, if necessary. Those can either refer to special awareness campaigns or be used for redirecting users with a specific infection as already introduced with the dns-changer.eu website by ECO.

4. Example for a National Support Centre: Germany / ECO

The German national support centre has been launched in 2010. It provides various layers of service and can be seen as a pilot model for other national support centres. ECO provides the following services:

4.1. Initiative–S

The initiative-S is a project run by ECO and supported by the Federal Ministry of Economics and Industry. The initiative provides a service to companies, which scans their websites in regular intervals for potential infections. Should the security experts detect an infection, defacement, or a phishing page, the company receives an email with initial information on cleaning the websites and possibly the company computer system. In addition, the email includes a ticket number and contact information for the Initiative-S experts, who are happy to answer any questions and help analyse the situation and find the appropriate solutions. A renewed check is performed and if the malicious code is still online, the company will be notified again and the Internet Provider will also be informed. Another part of this initiative includes prevention and education to avoid future infections.

4.2. Botfrei.de

Botfrei.de is an initiative from ECO supported by the Federal Office for Information Security (BSI). The goal of this project is to reduce the number of botnet infected computer clients in Germany. Its aims are to inform about botnets, to clean infected computers and to prevent future infections. Spamtraps and honeypots are used to find infected PCs. For this purpose, only attacks from infected PCs are evaluated. In no case does an evaluation of the Internet traffic through deep packet inspection or similar methods take place. User behaviour is not recorded or evaluated.

4.3. The ABBZ (Anti Botnet Advisory Centre)

The ABBZ is the German national support centre consisting of a website and a user help desk with telephonic support. With the help of this help desk, Internet users whose PCs have been taken over by a Trojan and are part of a botnet which has been confirmed by their Internet access providers can as a start begin to disinfect their PCs themselves by using the offered online tools and by getting support from a help desk assistant upon providing a personal ticket number. The ABBZ has established processes to enable affected end users to clean their PCs themselves as much as possible and to offer a help desk service telephone number (at the cost of a local call) provided by the ISPs to their customers for the purpose of removing malicious code.

4.3.1. Support centre process flow

The overall process is mainly as follows:
(a) Providers operate honeypots and Spamtraps. Only the providers can identify their customers from the IP-address at that particular point in time.
(b) Providers inform the particular customers according to the process determined by the providers themselves. In the first phase, the customers are informed that they have been infected with malicious software (bot). The customers are referred to the central help website where disinfection instructions are available.
(c) If the customer does not succeed there, he/she can contact his/her provider. The provider can then decide if the customer needs to be referred to the call centre for further help with removing the malware. In this case, the provider gives the customer a pseudonym created trouble ticket number that contains coded information about the infection.
(d) The process is set up so the affected users are initially informed by their ISPs that they can download certain tools from the project help website and that they can carry out steps described there. If the user does not succeed on his own, the user is given a ticket number that will allow him/her to get help telephonically from the help desk. Should that also fail to lead to the desired success, the caller is forwarded to a specialist, going from a Level 1 to a Level 2 support, who will then give further suggestions on what to do. Moreover, Level 2 Support will work out action suggestions for Level 1 support and as the case may be continually update and improve it.

4.3.2. Support centre project website

The central project website provides the respective tools for downloading as well as instructions, and therefore its quality, functionality as well as security are crucial for managing the volume of calls received by the help desk. The website contains detailed step-by-step instructions as well as the respective tools to enable the end user to disinfect his/her own computer. The website also provides tools available for downloading in collaboration with Anti-Virus companies.

4.3.3. Telephonic support at the support centre

4.3.3.1. Inbound help desk only format

The help desk is as an inbound only help desk. Exclusively customers identified by their ISPs as infected make incoming calls, and who have received a ticket number from their ISPs for this purpose. The phone number is publically not available. The service telephone calls are billed as a local call.

4.3.3.2. Help desk schedule

The telephone availability of the help desk is covered from Mondays through Fridays from 09:00 to 18:00.

4.3.4. The ticket system: Generating the ticket number in accordance with data privacy regulations as well as by attack type

Every referring ISP generates the ticket number to include the individual ISP-ID-code so that only that particular ISP can connect to the personal customer data. If the ISP has information about the type of malware, they include that additional information that would be helpful for the cleaning process on the ticket number.

4.3.5. Legal aspects

Due to the ticket system implemented in this project, participating ISPs do not enter personal customer information into a central database. Help desk employees do not access the customer computer directly or with remote hands but rather walk the customer through the procedure over the phone. The ABBZ does not store, trace or receive any personal data from an infected user or from his computer.

4.4. Special Landing pages – example dns-changer.eu

The DNS-changer botnet hijacked DNS tables of infected machines and redirected legitimate traffic to fake sites in order to steal personal information. This botnet was taken down by the ISC, and eco had been asked to interact as a relay between the ISC and the German ISPS. Besides alerting the German ISPs through a newly created standard notification format, eco also designed a special landing page that directed infected users to the dns-changer.eu website. This website provided a general check to identify infected machines same as an interactive guidance for the disinfection of compromised computers.

4.5. Other Services

4.5.1. Forum

The ABBZ runs a support forum at forum.botfrei.de. This forum provides the first level of support. Besides the regular staff of the ABBZ, several volunteers regularly contribute to the support activities.

4.5.2. Blogs

The blog regularly informs visitors about latest threats and other relevant news from the IT-Security landscape, same as information towards security awareness.

4.5.3. Social Networks

The activity is focussed on Twitter, Facebook and Google Plus. These additional social channels are used to reach a broader audience on latest threats or same as spreading information towards

5. References

http://www.botfrei.de
http://www.botfree.eu
http://cert.inteco.es
http://www.initiave-s.de
http://acdc-project.eu